S. Hrg. 110–291

UNDERSTANDING THE REALITIES OF REAL ID: A REVIEW OF EFFORTS TO SECURE DRIVERS' LICENSES AND IDENTIFICATION CARDS

HEARING

BEFORE THE

OVERSIGHT OF GOVERNMENT MANAGEMENT, THE FEDERAL WORKFORCE, AND THE DISTRICT OF COLUMBIA SUBCOMMITTEE

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

MARCH 26, 2007

Available via http://www.access.gpo.gov/congress/senate

Printed for the use of the Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

34–415 PDF WASHINGTON : 2008

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan	SUSAN M. COLLINS, Maine
DANIEL K. AKAKA, Hawaii	TED STEVENS, Alaska
THOMAS R. CARPER, Delaware	GEORGE V. VOINOVICH, Ohio
MARK L. PRYOR, Arkansas	NORM COLEMAN, Minnesota
MARY L. LANDRIEU, Louisiana	TOM COBURN, Oklahoma
BARACK OBAMA, Illinois	PETE V. DOMENICI, New Mexico
CLAIRE McCASKILL, Missouri	JOHN WARNER, Virginia
JON TESTER, Montana	JOHN E. SUNUNU, New Hampshire

MICHAEL L. ALEXANDER, *Staff Director*
BRANDON L. MILHORN, *Minority Staff Director and Chief Counsel*
TRINA DRIESSNACK TYRER, *Chief Clerk*

OVERSIGHT OF GOVERNMENT MANAGEMENT, THE FEDERAL WORKFORCE, AND THE DISTRICT OF COLUMBIA SUBCOMMITTEE

DANIEL K. AKAKA, Hawaii, *Chairman*

CARL LEVIN, Michigan	GEORGE V. VOINOVICH, Ohio
THOMAS R. CARPER, Delaware	TED STEVENS, Alaska
MARK L. PRYOR, Arkansas	TOM COBURN, Oklahoma
MARY L. LANDRIEU, Louisiana	JOHN WARNER, Virginia

RICHARD J. KESSLER, *Staff Director*
JENNIFER TYREE, *Chief Counsel*
JENNIFER A. HEMINGWAY, *Minority Staff Director*
DAVID COLE, *Minority Professional Staff Member*
EMILY MARTHALER, *Chief Clerk*

CONTENTS

WITNESSES

MONDAY, MARCH 26, 2007

ALPHABETICAL LIST OF WITNESSES

APPENDIX

UNDERSTANDING THE REALITIES OF REAL ID: A REVIEW OF EFFORTS TO SECURE DRIVERS' LICENSES AND IDENTIFICATION CARDS

MONDAY, MARCH 26, 2007

U.S. SENATE,
SUBCOMMITTEE ON OVERSIGHT OF GOVERNMENT MANAGEMENT, THE FEDERAL WORKFORCE, AND THE DISTRICT OF COLUMBIA,
OF THE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:30 p.m., in room 342, Dirksen Senate Office Building, Hon. Daniel Akaka, Chairman of the Subcommittee, presiding.

Present: Senators Akaka, Voinovich, Collins, and Warner.

OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. I call the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia to order.

I want to welcome Senator Collins here. It seems as though our border States are vitally interested in the issue before us today.

Before we begin, I want to extend a warm welcome to all of our witnesses today and especially to Honolulu Mayor Mufi Hannemann, who presented me this lei, and who is accompanied by Dennis Kamimura, the Licensing Administrator for the City and County of Honolulu. I greatly appreciate you coming all the way from Hawaii, Mufi, and I look forward to discussing how REAL ID impacts the State of Hawaii and the County of Honolulu.

Today's hearing, "Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers' Licenses and Identification Cards," will review the REAL ID Act of 2005 and the proposed regulations implementing the Act recently issued by the Department of Homeland Security.

In 2004, the 9/11 Commission reported that all but one of the September 11 hijackers acquired some form of U.S. identification, some by fraudulent means, which assisted them in boarding commercial flights, renting cars, and other activities. As a result, the Commission recommended the Federal Government set standards for issuing sources of identification such as drivers' licenses.

In December 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act to establish a negotiated rulemaking process among the Federal Government, State, and local governments, privacy groups, and other stakeholders to develop standards for drivers' licenses and identification cards. However, the Act provided States with flexibility for complying with Federal requirements and ensured privacy protections.

Without the benefit of Congressional hearings and before the negotiated rulemaking committee held its second meeting, the REAL ID Act was included in the 2005 Emergency Supplemental Conference Report, thus replacing the collective effort to address the 9/11 Commission's recommendation.

From its inception, REAL ID has been controversial and criticized by both ends of the political spectrum. The Act places a significant unfunded mandate on States and poses a real threat to privacy and civil liberties.

In issuing the REAL ID regulations, DHS has acknowledged the implementation problems and the need to address the burdens placed on the States. Secretary Chertoff announced that States could easily apply for a waiver for the compliance deadline and could use up to 20 percent of the States' Homeland Security Grant Program (SHSGP) funds to pay for REAL ID implementation. To me, this proposal does nothing to address the cost of REAL ID which DHS makes estimates to be anywhere from $17.2 billion to $23.1 billion. Moreover, the President's fiscal year 2008 budget proposes to cut SHSGP by 52 percent. On top of this, States have already designated SHSGP funds for particular homeland security projects, such as interoperability equipment, physical security structures, training, and evacuation planning.

My other concern is a serious threat by REAL ID to the privacy of Americans' personal information. The massive amounts of personal information that would be stored in State databases that are to be shared electronically with other States, as well as unencrypted data on the card, could provide one-stop shopping for identity thieves.

In addition, the DHS regulations failed to address redress mechanisms for individuals whose data is lost or stolen in another State or guidance on how States are to secure source documents.

As a result, REAL ID may make us less secure by giving us a false sense of security. Unfunded mandates and the lack of privacy and security requirements are real problems that deserve serious consideration and workable solutions.

Congress has a responsibility to ensure that drivers' licenses and ID cards issued in the United States are affordable, practical, and secure, both from would-be terrorists and identity thieves.

Over half of our Nation's State Legislatures, 28, have acted to introduce or to pass legislation expressing concern or calling for repeal of REAL ID. Two States, Maine and Idaho, have passed legislation to opt out of complying with REAL ID. In Hawaii, a resolution passed the State Senate which calls for repeal of those provisions of REAL ID that violate the rights and liberties guaranteed under the Hawaii State Constitution and the Constitution of the United States and create unfunded mandates for the State without any plan for financial subsidization for implementation.

To address these concerns, I reintroduced the Identity Security Enhancement Act, S. 717, with Senators Sununu, Leahy, and Tester, to repeal REAL ID and replace it with a negotiated rulemaking process and the more reasonable guidelines established in the Intelligence Reform and Terrorism Prevention Act of 2004. It is in the interest of Americans that this hearing shed light on the problems with REAL ID and provide a forum to discuss solutions that both protect the Nation and Americans' privacy and civil liberties.

I now turn to my good friend and partner on so many issues to improve government programs, Senator Voinovich, for any opening statement he may want to make. Senator Voinovich.

OPENING STATEMENT OF SENATOR VOINOVICH

Senator VOINOVICH. Thank you, Mr. Chairman, for holding this important hearing today to discuss the proposed regulations for implementation of REAL ID. The statutory requirement to issue 245 million—245 million—secure drivers' licenses in 5 years places a significant burden on our States, which bear the bulk of the responsibility for meeting the mandate.

The long-awaited draft regulation to implement REAL ID was released earlier this month. I want to begin by commending the Department of Homeland Security for its outreach process. The draft regulation clearly reflects a number of common sense recommendations that have been made by the States.

I had the opportunity to meet Secretary Chertoff last month to discuss REAL ID and was heartened by his sincere commitment to make full use of the flexibilities provided in the draft regulation. Secretary Chertoff is firmly committed to waiving the May 2008 compliance deadline until the end of 2009 for any State that makes a reasonable request.

However, I am concerned by the number of hurdles that stand in the way, including the cost to States and the lack of availability of electronic verification systems. It is important that we work together to find solutions to these challenges before us. The relationship between the Federal Government, State, and local governments should be one of partnership. Sadly, that is not always the case as the Federal Government has a tendency to force new responsibilities on State and local governments without providing adequate funding to cover the true cost.

As Governor of Ohio, I became particularly concerned with the cost of Federal mandates. During my tenure, I worked tirelessly with State and local government groups to pass the Unfunded Mandates Reform Act. As a matter of fact, the first time in my life that I set foot on the floor of the U.S. Senate was when the unfunded mandates relief legislation passed. I was in the Rose Garden representing State and local governments when President Clinton signed the legislation in 1995 and that pen is proudly displayed in my office today.

DHS estimates that the cost for States to comply with REAL ID will exceed $14 billion, and that most of these costs will be incurred in the first 5 years. Ohio, my State, estimates that it will need $45 million to comply and $11 million annually to run the program. As someone who has been responsible for balancing a

public budget, I can assure you these are significant costs that require tough choices.

This unfunded mandate poses a significant financial burden on States, many of whom are facing tight budgets. Though I am pleased the Department will allow States to use 20 percent of their State Homeland Security Grant Program funds to help implement REAL ID, I worry about the unmet homeland security needs that will be put on the back burner if States select this option.

For example, last month, I was in Cuyahoga County, the largest county in Ohio, to discuss the cost of implementing their interoperability program, which is $114 million. It is ridiculous to ask States to use 20 percent of their State homeland grant programs, which in most cases have already been allocated, to implement REAL ID.

I question whether Congress understands the huge cost burden we are placing on States, and I believe that the Federal Government should provide the necessary funding to aid States as they reconfigure their drivers' license requirements to meet their new Federal responsibility.

Technology will also be a key factor in the successful implementation of REAL ID. States will need functional access to a number of databases for verification of an individual's identity. Given the limited time frame, our Federal Government must move quickly to ensure nationwide access to the required databases. As we ask States to do their part, we must be sure the Federal Government is also meeting its responsibility in a timely manner.

The implementation of REAL ID comes at a time when the Federal Government is developing a number of new identification documents, including the Pass card, biometric passports, the TWIC card, and the Fast card. It seems to me that we ought to take a fresh look at the various identification requirements and consider whether or not some of these documents could be used for multiple purposes. For example, common sense would suggest that residents could use their REAL ID cards to cross our Northern land border instead of having to also apply for either a Pass card or a passport.

My concern should not suggest that I am opposed to REAL ID. Rather, I want to be sure that as we move forward with implementation, we are honest about the true cost of compliance. DHS must also redouble its efforts to work closely with States to help ensure a seamless implementation. This partnership is essential to the success of REAL ID, and more importantly, to securing our homeland from another terrorist attack.

Mr. Chairman, today's hearing marks an important first step in our oversight of REAL ID. As implementation moves forward, I would suggest that we invite some of our witnesses today, including DHS, to report back to us in 3 months on their progress.

Senator AKAKA. Thank you very much, Senator Voinovich.

Now I will ask for the statement from the Senator from Maine, Senator Susan Collins, who has been a great leader in the Senate and especially with the Homeland Security Committee here. As I mentioned earlier, her State has already taken action on REAL ID, so, we are glad to have you here, Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you very much, Mr. Chairman. I must say, I am very envious of the gift that the Honolulu Mayor brought to you. You look quite festive decked out in your lei there.

Mr. Chairman, I am very pleased to join today in the discussion of the REAL ID Act of 2005 and the draft regulations that the Department of Homeland Security has recently issued to implement this program and I very much appreciate the comments that both the Chairman and Senator Voinovich have been making on this issue.

I first became involved in this issue back in 2004 when Senator Lieberman and I were working on legislation to implement the recommendations of the 9/11 Commission, which included recommendations for more secure identity documents, including drivers' licenses. The Commission pointed to the fact that several of the hijackers used drivers' licenses to gain access to airplanes and that they had obtained them in some cases through fraudulent documents.

To respond to that legitimate concern, Senator Lieberman and I drafted negotiated rulemaking provisions that were put into the Intelligence Reform Act of 2004 that called upon the Department of Transportation to convene a group to work with State officials, privacy advocates, and technological experts to come up with a workable, practical solution to the problem identified by the 9/11 Commission.

And indeed, this committee, this rulemaking committee, was appointed. Maine's Secretary of State was one of the members and they were working along, making progress, doing exactly what they were charged with when, unfortunately, the House moved ahead and tacked on the REAL ID Act to an emergency war supplemental bill. This Act repealed the negotiated rulemaking provisions of the Intelligence Reform Act, and proceeded to direct the Department to unilaterally draft regulations.

Well, now we find ourselves 2 years from the passage of the REAL ID Act, which repealed these 2004 provisions before they were given a chance to work, and only a year from the statutory deadline for compliance. I am very pleased that in response to concerns that many of us raised, the Department of Homeland Security has responded by extending the compliance deadline considerably and by trying to put back in place the negotiated rulemaking process, albeit as a response to the preliminary regulations rather than starting from scratch, and those provisions are similar to the bill that Senator Akaka and Senator Sununu have introduced to try to reintroduce negotiated rulemaking. I think that is going to greatly improve the process.

We need to make sure that in the pursuit of more secure drivers' licenses that we are not jeopardizing the fundamental liberties of our citizens and that we are not simply handing the bill, an enormous bill, over to the states that requires them to divert funds from other vital homeland security activities. In that regard, I want to associate myself with the comments made by the Senator from Ohio, who is both a former governor and a former mayor and has a special appreciation for unfunded mandates.

The State of Maine has estimated that the cost of complying with the REAL ID Act would be six times the cost of the entire budget for the Bureau of Motor Vehicles. So the cost of this remains a concern, and while I appreciate the Department trying to introduce flexibility, the fact is that the need for Homeland Security grant monies for a host of other vital and urgent needs remains, and I think it is going to be very difficult for States to use 20 percent of those funds to pay for compliance with the REAL ID Act.

So I think this is an issue that we are going to have to do more work on, on the cost issues, on the privacy issues, and on the technology issues. This is not an easy task to make sure that States can tap into databases of other States and it raises many security concerns.

So, Mr. Chairman, I thank you for holding this hearing, a hearing that had the normal course been followed with the REAL ID Act, we would have held years ago and I think we would have ended up with more reasonable legislation. So thank you.

Senator AKAKA. Thank you very much, Senator Collins.

Now, before we move on, I would like to ask Senator Warner for any statement that he may have.

OPENING STATEMENT OF SENATOR WARNER

Senator WARNER. Thank you, Mr. Chairman. I am pleased to be here because I am quite interested in this whole concept. I really think America needs to explore this particular concept in the national security interest. This is where my primary concern arises.

We have now learned that the duplication and the falsification of drivers' licenses is quite feasible. Our security here at home is highly dependent in certain areas, like when boarding aircraft and otherwise, to have some sense of confidence that the individual that displays the card is, in fact, the rightful owner of it. And this card, because of technical advances, can be produced in such a way as to greatly increase the security as associated with any type of identification individual proffers, whether it is for the airlines or other purposes.

So I approach this with an open mind, leaning hard towards seeing what we can do to help the States facilitate the law as it is now written, and if necessary, to change the law that is written to try to further help our States. But the bottom line is we have got to come to the recognition that the life before us is different than the life behind us and that we are faced with very serious threats from abroad and perhaps, regrettably, some internally, and this type of identification will go a long way to, I think, make us more secure here at home.

I thank the Chairman.

Senator AKAKA. Thank you very much, Senator Warner.

Senator WARNER. I would ask to put the balance of my remarks in the record.

Senator AKAKA. It will be included in the record.

[The prepared statement of Senator Warner follows:]

PREPARED STATEMENT OF SENATOR WARNER

Thank you for calling today's hearing as I feel it is one that deserves greater attention in this Committee and indeed the entire Senate. Since the passage of the

Real ID Act many have criticized the program for reasons of cost, inefficiency, and privacy. It is my hope that we may today explore these concerns and some potential solutions.

I believe that standardized identification criteria among the States will make for a more secure country. We can eliminate fraud, provide a barrier to crime, and ultimately protect the American public better if we can rely on the authenticity of state issued drivers' licenses and identification cards. I believe that the sooner we have Real ID in place, the better. However, I have one significant concern with the program as it has been proposed—the passing of an unfunded mandate onto the States.

It is my firmly held belief that the primary responsibility of the Federal Government is to provide for the national defense. And I also believe that the Real ID program is a part of this responsibility. What I do not understand is why this federal responsibility is not being funded by the Federal Government.

The National Governors Association has estimated that the cost of compliance to the States with Real ID will be approximately $11 billion. The Administration has argued that the costs should simply be passed on to the users in the form of increased fees for drivers licenses. Certainly larger states that issue millions of licenses can absorb these costs much easier than smaller states that may only issue a few hundred thousand.

I am pleased that the Department of Homeland Security has recognized this issue and intends to help the States with some of the costs of compliance by paying for the network build-out but am concerned that this only represents a fraction of the costs to the States.

I look forward to hearing more from our witnesses about their concerns and am hopeful that we may come together on some common ground on this important issue.

Senator AKAKA. I want to welcome the Hon. Richard Barth, Assistant Secretary for the Office of Policy Development at the Department of Homeland Security, to this Subcommittee hearing today.

Mr. Barth, it is the custom of this Subcommittee to swear in all witnesses, so please stand and raise your right hand.

Do you solemnly swear that the testimony you are about to give this Subcommittee is the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. BARTH. I do.

Senator AKAKA. Let the record note that the witness answered in the affirmative.

Thank you. While statements are limited to 5 minutes, I want all of our witnesses to know that their entire statements will be included in the record.

Mr. Barth, will you please proceed with your statement.

TESTIMONY OF HON. RICHARD C. BARTH,[1] ASSISTANT SECRETARY, OFFICE OF POLICY DEVELOPMENT, U.S. DEPARTMENT OF HOMELAND SECURITY

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

I also want to take this opportunity to thank you for introducing S. Res. 94 earlier this month to honor the employees of the Department of Homeland Security on the Department's fourth anniversary. It was gratifying to the employees to receive this recognition by the Senate.

Your subject for this hearing, "Understanding the Realities of REAL ID," is highly appropriate and timely. This is a very chal-

[1] The prepared statement of Mr. Barth with an attachment appears in the Appendix on page 48.

lenging program for both the States and the Federal Government to implement, with many complexities ranging from cost to technically integrating various data links while imposing strong data security and privacy protections.

Let me be clear at the outset. Effectively implementing a REAL ID program is a top priority for DHS. REAL ID is fundamental to our security as a Nation. We can debate the costs. We can fret about the time to implement and time waiting in line to obtain a REAL ID. But the inextricable link to ensuring that people are who they say they are when someone gets on an airplane and sits next to you is of paramount importance to preventing another September 11.

All but one of the September 11 hijackers acquired some form of U.S. identification document. Eighteen hijackers fraudulently obtained 17 drivers' licenses and 13 State-issued identifications and some even possessed duplicate licenses. The pilot who crashed American Airlines Flight 77 into the Pentagon, Hani Hanjour, had ID cards from three States. The drivers' 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, take flying lessons, and board airplanes. The hijackers believed that holding drivers' licenses and ID cards would allow them to operate freely in our country, and they were right.

So again, as I will repeat over and over again today, our security as a people and collectively as a Nation relies on valid identification documents.

Counsel to the 9/11 Commission, Janice Kephart, said the REAL ID 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." Said another way, identity document security is a prerequisite for overall security in the United States. If we cannot verify that people are who they say they are and if we allow loopholes in obtaining drivers' licenses and IDs to exist, DHS's job and that of law enforcement becomes exponentially more difficult. Sadly, four of the hijackers had been stopped for traffic violations in various States while out of legal immigration status, a condition that should have resulted in their drivers' licenses expiring.

Key features of the proposed rule include the following. Individuals seeking drivers' licenses or personal ID cards will need to establish their identity, U.S. nationality or lawful immigration status, date of birth, Social Security number, and principal residence. States would verify the issuance validity and completeness of the document presented. As you can see by the chart,[1] which is also included in my testimony, electronic verification of these documents is a work in progress. But in some areas, we can quickly get the States online. For example, birth certificate information can be brought online for all States for about $4 million, and we hope to be able to use existing DHS grant money to facilitate that over the next year or so.

[1] The chart submitted by Mr. Barth appears in the Appendix on page 56.

Standard information will be required to appear on the cards, including full legal name, date of birth, gender, a unique identification number, a full facial digital photograph, address of principal residence, issuance and expiration dates, and signature. The cards would also have physical security features and a common machine-readable technology.

Each State must prepare a comprehensive security plan for all State DMV offices, storage and production facilities, databases, and systems. Employee background checks would be required to decrease the probability of criminal collusion with DMV employees.

Further details on the floor that we are establishing for more secure IDs is in my written testimony, and it is important to note that the States are not precluded from requiring additional security features.

The September 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. As the Secretary noted when he held his press conference when we published the rule, these new cards will cost less than $20 additional each time you renew your license.

I personally believe that any further delay in implementing REAL ID would significantly increase our vulnerabilities as a Nation, and as long as I have responsibility for this program, I intend to do everything possible to make sure that fake IDs are not part of the scenario in the next terrorist plot successfully carried out in this country.

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. It is a national problem and demands a national solution.

Thank you, Mr. Chairman, for the opportunity to testify today and I look forward to your questions.

Senator AKAKA. Thank you very much, Mr. Barth.

Hawaii is an island State whose residents depend on air travel to travel within the State. If the State decides not to comply with the requirements of the REAL ID or if individuals in Hawaii cannot obtain a REAL ID-compliant driver's license, will DHS grant a waiver for inter-island travel so that our residents will be able to travel within the State to visit family and friends on other islands?

Mr. BARTH. That is a very good question, Mr. Chairman, and we are looking at various solutions for that question that would not prevent the residents of Hawaii from getting around the islands. One of the obvious solutions is that a passport, for those who hold a passport, is an easy alternative for getting on an airplane even if Hawaii decides to opt out of REAL ID.

In addition, we are looking at alternative documentation like a Federal Government-issued ID out of the Department of Homeland Security to deal with citizens of States who want to be able to travel freely and easily on airplanes and provide an alternative to the REAL ID that would be equally validated and equally difficult to make fraudulent cards from.

And finally, I would note that in virtually all cases where DHS has security, whether it is Customs coming into the country or TSA and airports for controlling security in airports, there is a secondary referral process that you can go to and present other kinds of documentation that will help inform the inspector to make a decision as to whether or not to let you onto the airplane without a REAL ID. So there are multiple scenarios that we think will effectively address your concern. Thank you.

Senator AKAKA. As you know, Mr. Barth, many people are worried about the REAL ID's impact on privacy and civil liberties. Because of this, did the White House Privacy and Civil Liberties Board review the regulations, and did DHS make any changes to the regulations based on their comments? If so, would you please describe those changes?

Mr. BARTH. Thank you, sir. I am not aware that the White House Privacy Board looked at the regulation before it went out. There is a White House circulation process and I am not aware of all the details of it. However, we were very concerned with the privacy issue. I think the regulation and the preamble to it goes into it at great length about our concerns to make sure the databases are secure. Certainly the background checks on DMV employees are a big part of protecting privacy.

But we also issued at the time that the regulation came out or shortly thereafter a 25-page privacy impact analysis that our own Privacy Office did for DHS and it clearly addresses a lot of the different concerns, even beyond the regulation itself. We are looking forward to receiving comments from the privacy civil rights and civil liberties communities on the regulation during this 60-day comment period and we will do everything within our ability to try to make sure that their concerns are fully taken care of.

No one wants to be a subject of identity theft, and so we want this document to be as secure as possible to become an added advantage in a world where identity theft is becoming a multi-billion-dollar problem for citizens across the country.

Senator AKAKA. As you know, Mr. Barth, REAL ID is going to cost State and local governments billions of dollars. Although DHS has approximately $40 million in grant funding to provide States and has authorized the use of State Homeland Security Grants, this is not enough. What are DHS's plans for helping States pay for REAL ID?

Mr. BARTH. Mr. Chairman, I think that the $40 million is something that we are looking at to become a keystone of doing one particular factor or technology link that needs to be accomplished to make REAL ID work and we are working with our grants and training folks in the Department and consulting with States on trying to find a way of funding the interconnectivity of all of those databases that you see up there while paying close attention to privacy and data security issues. So we are working to try to get the most significant impact out of that $40 million that has already been appropriated.

Beyond that, I have expressed to our friends at the National Governors Association, National Council of State Legislatures, that they have significant lobbying powers and that we will not in any way, shape, or form try to object to them acquiring other money

through appropriations and authorization by the Congress, but we just don't feel like that is necessarily our role at this time.

The finalization of interoperable, interconnected networks of networks, which is what that chart represents, is something that we believe will cost probably more than $40 million and we are right now working with our various technology groups in the Department of Homeland Security, the CIO's Office, for example, to identify the way to link up these databases securely and with due process for identity theft and other problems, and when we conclude the preliminary work-up of that, we will be submitting to Congress, hopefully for the 2009 fiscal year budget, a proposal to have the Federal Government take on the responsibility of networking those networks effectively and securely.

Senator AKAKA. Mr. Barth, you have repeatedly said that the States will use a pointer system, which is based on the Commercial Driver's License Information System, to verify information from other States. However, the regulations do not state this and instead leave open how States are to share information with each other. This may be one reason why Americans fear this is becoming a national ID card. Why didn't DHS just require the use of CDLIS for REAL ID?

Mr. BARTH. Mr. Chairman, that is a very good question and there is a ready answer for it. The CDLIS system handles in the tens of millions of commercial drivers' licenses each year and it does so very effectively, and I might point out that to the Department of Transportation's knowledge, which has been managing the funding and the establishment of the Commercial Driver's License System since, I think, 1986 when they started the roll-out of that system, there have been no Privacy Act violations, so there is an additional reason, perhaps, to use that system, as you have suggested.

At the time when we wanted to bring the regulation to closure and get it published, we were in intense dialogue with AAMVA, which manages the CDLIS system for the Transportation Department, as to their system and particularly whether it had the ability to scale up in time to handle the 240 million non-commercial drivers' licenses that need to be renewed over a 5-year period as part of this program.

So we are getting closer and closer to having the kind of assurance for that exact pointer system, which has not had privacy problems since 1986, might be exactly the solution that we want. We are not ready to say that yet. It may be several more months. But to the extent we can possibly put that in the final regulation as our pathway forward, I will certainly take your comments on board, also, because we are inclined towards that.

Senator AKAKA. While the REAL ID Act requires States to verify information against certain databases, I understand that some databases do not exist and others are only in the pilot phase. Can you provide us specific data on the status of each database and their estimated time of availability on a national basis?

Mr. BARTH. Yes, sir. Mr. Chairman, again, I will refer to the chart that we provided up here. If you look at the far right, it is a column that shows absolutely no check-marks for States being able to access the Passport Office records for your individual pass-

port to confirm that you are who you say you are. Interestingly, that database exists, it is highly accurate and very robust, and the only thing that is missing is the interconnectivity between the State DMV offices and the State Department Passport Office. We, for example, query that passport database all the time as part of the DHS's mission.

So the chart, while it shows significant gaps, as you are suggesting, I think it also, when you dig deeper into explaining each of those links, it is not as bad as it looks.

The next column over, which is the birth certificate confirmation, I am informed by the Department of Health and Human Services that 85 percent of all birth certificates dating back to 1935 have already been digitized. Those checks there show the pilot program that is effectively linking the birth records with DMV offices, and as I said in my oral testimony and the written testimony, for only $4 million, we can have that total column there have checks for that interconnectivity that we require.

So each one is a different story and it would—perhaps in questions for the record we can give you all the details you wish.

Senator AKAKA. Thank you so much for your responses. Let me now call on Senator Voinovich for his questions.

Senator VOINOVICH. Thank you.

Dr. Barth, the proposed regulations state that DHS will require the use of several databases to electronically verify lawful status and Social Security numbers of individuals. They include Social Security Online Verification.

The Department of State's Consolidated Consular Database, Electronic Verification and Vital Events System (EVVE), and the Systematic Alien Verification for Entitlement (SAVE), I understand, all 50 States have Memorandums of Understanding or access to SAVE. However, only 20 are currently using it to verify lawful status. States will also need to access U.S. Immigration and Customs Enforcement Student and Exchange Visitor Information (SEVIS).

The question I have is how far in advance are you going to be able to have all these databases up and working?

Mr. BARTH. Thank you, Senator, for the question. If I could answer with the precise date, I would be thrilled to do so. I can tell you that we have teams working very hard to provide all that connectivity and all that verification capability that we share with you in wanting to provide to the States.

If, for example, the State Department for funding reasons or manpower reasons or priority reasons is unable to provide 50 States plus 7 territories linkage to their passport database, we will look very closely at finding some waiver authority within the Secretary's authority that would allow us to defer bringing the passports online until it is technologically feasible, funded, and has actually been accomplished by the State Department. In making sure that we don't create a loophole for further fraudulent activity, we could significantly increase the training for DMV officials on spotting fraudulent passports.

So we think that there are tradeoffs there between fraudulent document review and actual exceptional digital verification that we can make in the early years of the roll-out of REAL ID.

Senator VOINOVICH. I think you have answered the second question that I was going to ask, and that is if the databases are not up and working by the May 2008 deadline, do you have the authority through regulation to extend that period beyond that date?

Mr. BARTH. My understanding is that we will have the authority to extend beyond that date, yes, and we will be—our hard target, if you will, for filling in that entire chart with check-marks for all 50 States and all five databases would be the December 31, 2009 deadline for which the Secretary has indicated he will issue waivers. But for those states that have indicated to us they want to be early adopters, if you will, we believe we have the authority to give them alternatives to electronic verification of a passport.

Senator VOINOVICH. Is there any effort being made to coordinate the technology that is going to be implemented by the various States?

Mr. BARTH. Yes. We have considered that issue and have actually raised it in the regulation, and at this point in time, the proposed rule would not require the 50 States to use the connectivity that we provide. However, in order to ensure that data passes back and forth through the network efficiently, that is one of the reasons why we believe it should be a Federal responsibility to pay for the build-out of that network of networks to remove the incentive for a State to perhaps go down a different path. If it is paid for, built out faster than anything else, etc., we think that will be a powerful incentive to the States coming online, a single system rather than creating a panoply of systems, as you suggest.

Senator VOINOVICH. You are developing technology that you will share with the States?

Mr. BARTH. We would not develop technology. We would seek a technology solution funded by the Federal Government that the States would have a large stakehold in. We have not yet defined in a high level of granularity what that will look like, but I will draw an analogy to the Department of Transportation, which funds the development of this CDLIS system that the Chairman was referring to, but the States own the system and have funded AAMVA, the American Association of Motor Vehicle Administrators, to build out this CDLIS system.

And if that system proves to be, as I certainly hope it does, the framework for a significantly scaled up civilian driver's license verification network, it will have the advantages that the Chairman mentioned of being a pointer system, not a lot of data flowing. It won't retain a lot of data in a central database, which poses its own risks. And it will give us a platform on which to build without having to invent new technology.

Senator VOINOVICH. Are you going to be able to guarantee that information is going to remain private?

Mr. BARTH. To the extent that we can provide the safeguards, we believe that this system will be vastly an improvement over the current 50-plus-7 territories systems that are built out now. Whether it is the documented cases last week in North Dakota of fraudulent driver's license activity, whether it is the $4,000-per-license cost to collude with an internal DMV person in New Jersey, or some Connecticut similar fraud cases in the past, I think wher-

ever you have human beings involved and the capability to bribe them to do things that are wrong, you can't say there is zero risk.

Senator VOINOVICH. Could somebody break into the system and get the information?

Mr. BARTH. They are likely to be under the age of 20, not to be glib, sir. But I think that we are going to provide the safeguards to do everything possible to prevent that from happening.

Senator VOINOVICH. One concern of the NGA is that 24 States have a driver's license renewal period that is longer than 5 years, many have 10 years. I understand that in the regulations you have ruled out 10 years and have said States have to do it in 5 years. I would like you to explain why DNS has chosen the 5-year renewal date?

Mr. BARTH. In the consultation we did with the States, which have a very wide ranging number of years before renewals are required, we certainly didn't arbitrarily choose, but in consultation with them chose about an 8-year period for renewals as the maximum that we would allow. States that currently have 4-year renewals, they can continue their 4-year renewals. states that have 8-year renewals would have to—the individual applying for the driver's license would have to reappear every 16 years, so every other cycle, in person to revalidate their data, their place of—their documentation——

Senator VOINOVICH. It is not 5 years?

Mr. BARTH. It is not 5 years, sir.

Senator VOINOVICH. I thought that was in the regulation.

Mr. BARTH. I don't believe so. Yes. You are referring to the 5-year implementation period for the very first cycle of everyone in America who has a driver's license who lives in a State that opts into REAL ID, they have to move through that first cycle in 5 years. The second cycle is 8 years, and every cycle after that is a maximum of 8 years, but States can choose a shorter cycle.

Senator VOINOVICH. Ambassador Wilson came in to see me last week and we talked about the Western Hemisphere Travel Initiative. As I mentioned in my opening statement, I want to ensure that DNS is taking into consideration the interoperability between the various screening tools and ID documents?

Mr. BARTH. Yes, it is, sir. Governor Gregoire of Washington State approached us some months ago with a proposal that we partner with Washington State on a dual-use Western Hemisphere Travel Card, WHTC, we call it, and REAL ID, and we fairly quickly sent back from Secretary Chertoff to the governor a letter saying we would definitely like to explore this with you. The "too many cards out there" problem is something we would like to try to get under control.

Senator VOINOVICH. I would suggest that you stay on top of it. DNS should work with what they are doing there and individuals so they don't have to get multiple sources of ID in order to travel back and forth between Canada and the United States. There is real concern about moving people back and forth in the border States.

I know in Ohio, we have many Canadian tourist visiting. We would like to make sure that they continue to visit our great State.

Mr. BARTH. We are piloting this in Washington State, and we expect to roll it out January 1, 2008, which I think is a very efficient way forward, and in many ways, that will show us the way forward for a lot of the border States, but any State, Ohio included, or Florida, if they want a dual-use card for, say, a snowbird from Ontario or somewhere, we would be very happy to try to accommodate that.

Senator VOINOVICH. That would be wonderful. Stay on top of it and do what you can to make sure they get it done on the date that they say they are going to get it done.

Mr. BARTH. Thank you, sir. I will do that.

Senator AKAKA. Thank you very much, Senator Voinovich. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Mr. Barth, in responding to a question from Senator Voinovich, you referred to states that choose to opt in to the REAL ID. But, in fact, States have very little choice but to participate in this new system. If they don't participate, then their citizens cannot board airplanes, they cannot gain access to certain Federal buildings. There are all sorts of practical ramifications. So do you really think that there is an alternative for any State but to opt in?

Mr. BARTH. Senator Collins, the 9/11 Commission was very clear as to the fundamental nature of clarifying this ID thing to prevent a future terrorist attack. I think that legislation reflects exactly what you just said, which was drafted by the Congress and we are trying to implement it.

I think that with the alternative documentation, as I have already explained, a federally-issued other ID, for example, military ID, the military residents of Maine will be able to travel around without a REAL ID, we expect. Passport holders, which is some 30, and growing, percent of the American population, will be able to use that document. And if we, and I am expecting we will come up with a Federal alternative, a Maine farmer who never wants to leave the State or get on an airplane will be happy without his REAL ID and a Maine citizen who wants to travel will have multiple alternative documents to acquire to travel freely like anyone who has opted into the system.

So I believe that there are strong incentives to come into the REAL ID program and opt in, but I believe that the disincentives are relatively low given the potential risk and vulnerability that it presents to the whole country. For states that continue to issue documents that are not as secure as other States—if you are a terrorist, you will very quickly find online that State X is where you go to get your fraudulent document to get on an airplane and drive it into a building.

Senator COLLINS. I guess my point is that we need to face the practical reality that States almost certainly are going to have to participate in this program because of the practical consequences of not doing so for their citizens, which brings me back to the cost issue. The Department, when it issued its draft regulations, estimated that the cost to States of compliance with the REAL ID Act would be $14.6 billion over 10 years. The NGA has estimated $11 billion over 5 years. Really, those are very similar estimates because a lot of the costs would be in the first 5 years, so I think it is fair to say that there is substantial agreement that we are talk-

ing about billions of dollars over a 5- and 10-year period for compliance.

If the Federal Government is imposing this mandate, shouldn't we go beyond the $40 million that you have mentioned that could be used to set up a very useful interstate database that would allow for States to check each other's databases? I mean, isn't that just a drop in the bucket when you are talking about costs of this magnitude?

Mr. BARTH. Yes, that is a drop in the bucket, and even if it costs a couple hundred million—and we don't know the number yet—to fully integrate the databases securely and with data privacy protections installed, it is still a small portion of the cost compared to hiring people, in some cases, building additional lanes, bricks and mortar kinds of facilities, obtaining the equipment necessary.

We are doing everything we can to mitigate those costs. For example, one of the things that we are going to do is work with GSA to have a single contract procurement activity for the cardstock and the card issuance equipment and allow GSA to put up on their procurement site enablement for all States to come in and buy, I presume, at lowest possible cost all the equipment and all the cardstock they need. This would save not only costs on the direct acquisition of those items with just a direct procurement from that list, but it would also save 50 different State procurements. We are seriously looking at the cost issue and doing everything we possibly can to reduce it.

But I think you have to look at it in a way of also evaluating which ones have already made a substantial investment to become, if not REAL ID compliant, but to improve their security. The State of Virginia has put an enormous amount of money into getting there already. The State of Michigan told us that they have spent roughly $30 million and they are a few million dollars from becoming REAL ID compliant. That is a fairly sizeable State with a fairly large population. So the numbers, frankly, are all over the map and we have instructed the economists in DHS to very closely pick apart the numbers that were in our proposed rule economic analysis and see if those costs are really that high. Even with that, though, I agree with you the costs are substantial and I believe, unfortunately, it would be very difficult for us to determine on a State-by–State basis how much they really need for this purpose.

So I would finally note that Alabama, maybe, has provided the ultimate solution. I was talking to their DMV a few weeks ago. They have a zero-cost to the State implementation of REAL ID, or very close to that, depending on a final regulation. They entered into a contract with a service, an equipment provider, whereby that service and equipment provider is tacking on a fee to the issuance of the driver's license, and for no capital investment and I believe no operating investment by the State, they can and will be, when they rewrite the contract in light of REAL ID, compliant.

So there are great models out there for mitigating the costs, for lowering the costs, and we are working with the States to——

Senator COLLINS. I would say to you that paying perhaps double for your driver's license, most people would not consider to be no cost. But we will put that issue aside.

I want to raise just one other issue in the brief time that I have remaining. State officials have repeatedly made the point to me that this system is only as good as the source documents and they are very concerned about training DMV personnel to evaluate the validity of a birth certificate, a baptismal certificate, a visa, or a passport. People working in the DMV offices are excellent public servants. They are very committed to the security of our country. But they are not trained to distinguish whether or not these source documents are valid and should be accepted.

Are you going to assist States with training their personnel to different standards? There must be a huge degree of difference among the various States on birth certificates, for example. Someone coming into Maine who has moved from Virginia or Ohio or Hawaii, I am sure they have a birth certificate that looks different from Maine's. How are you going to deal with this? How are you going to train, to help the States train DMV personnel so that they can accurately assess source documents, because if they can't do that, the whole system on which REAL ID is based falls apart?

Mr. BARTH. Senator, there are several answers to your question, actually, so if you will bear with me, I will try to identify them.

First off, in your passport files, once that data link is connected, and depending on how it is connected, you might be able to pull up the digital photograph of the person and literally match it to the person sitting in front of you. That biometric confirmation of who you are and that you got a passport, maybe all using fraudulent documents, but I hope not, is a very powerful confirmation of who you are.

But more to your point specifically of training for the DMV officials, we have taken that into account. We have forensic document labs in the Department of Homeland Security. We have already been working with them on various aspects of this rule and we expect, I would say, to develop a package, a training package that the States could build on. The rule itself and the $14 billion that we highlight as the cost factors in a $300 training cost for each and every DMV employee across the land. So that cost is factored in. It is not funded by the Federal Government, but it is factored in as one very important item, as you suggest.

Senator COLLINS. Thank you, Mr. Chairman.

Senator AKAKA. Thank you very much, Senator Collins. Senator Warner.

Senator WARNER. Thank you, Mr. Chairman.

This has been a good hearing and I am impressed with the amount of work that you individually and members of your Department have done to try and resolve this. I just hope Congress adopts an attitude that we have got to be a working partner and not get into an adversarial process and also that the States can be working partners.

In the preparation of your regulations, to what extent did the several States participate and come forward with ideas and concepts to improve the regulations?

Mr. BARTH. That is a very good question and the answer, I think, should be very comforting to you, which is that we ran an open phone call with at least four States every Thursday since, I believe, last August to consult with the States on various aspects of this

regulation and the economic analysis. That, in part, is why, as Senator Collins suggested, our costs and their costs line up fairly well. We have been talking extensively.

Four States in particular I want to commend for being on virtually every one of those calls. California, Iowa, New York, and Massachusetts sort of formed a core group that were extremely interested, had the capability within their DMV organizations, and participated weekly, came to Washington for a face-to-face meeting with Deputy Secretary Jackson, really doing everything possible to make exactly what you said, a partnership with the States for this important program.

And I am very pleased to say that my project manager for this, Darrell Williams, just spent the entire last week on a 5-day, four-city tour with the American Association of Motor Vehicle Administrators, pulling in regionally DMV administration people from many different States around the country. So not only has our consultation process been rigorous leading up to the issuance of the NPRM, it is going to continue to be rigorous as we move towards the final rule, and as we build out that network of networks, it is going to continue, sir.

Senator WARNER. Was part of that dialogue to discuss costs to the individual States?

Mr. BARTH. Yes. The States came in towards the end of developing their cost analysis, their $11 billion cost analysis. They came in jointly as the National Governors Association, the National Council of State Legislatures, and AAMVA, and they presented their document and they asked us to help them sort through the funding issue.

Senator WARNER. Is there any standardization of the criteria by which several States did make their estimates?

Mr. BARTH. No, sir, there was not. AAMVA, actually, I believe it was, developed the data from the States on which their figure and much of our figure is based. So each State had a different approach towards the funding and there is no standardization of that.

Senator WARNER. Was the thought given to trying to standardize it, because these estimates which were thrown out here, $23 billion by OMB, that, I understand, even involved the transportation of an individual to and from their home or workplace to the DMV, which strikes me as an odd way to compute things, but anyway DHS was at $14 billion, and $11 billion from the NGA. There is quite a disparity here. And then I also, based on the fragments that I have been able to collect, see where some States came in with a cost estimate, but almost uniformly all of them are coming down in the estimates. Would that be a correct assumption?

Mr. BARTH. Yes, sir, that is a correct assumption, I think in part because while we have been negotiating the regulation and getting it out, States have continued to make good, solid investments in many cases in their existing networks, and we hope that continues as we move toward a final rule, which we hope to announce in August. So I think that as we scrub the costs going forward, which as I have already said our economists are doing, I think that figure could be ultimately viewed as being very high.

Senator WARNER. What figure? I threw three out here. I don't know what figure you are talking about.

Mr. BARTH. The three key ones are the $23 billion includes if you are a disorganized person and it takes you an hour and a half to find your birth certificate, driver's license, passport, to go to the DMV. It even includes the cost of spending time at home finding your documents. That is the highest cost estimate——

Senator WARNER. I don't know which government clerk figured that one out.

Mr. BARTH. Well, required by OMB rules, sir.

Senator WARNER. Oh, is that it? All right. That is extraordinary to me. I can't believe that. Anyway, it took 2 years to put this set of regulations together?

Mr. BARTH. It did, and I think in large part it was due to the extensive consultation, including, as I said, the Deputy Secretary, before he would sign off on the regulation, convened a meeting with AAMVA and the four states that I mentioned before that were our close partners in developing the regulation. So it is regrettable that it took so long, but the consultation process was at least as intense as it would have been under a negotiated rulemaking process.

Senator WARNER. Well, Congress is faced with this and we are getting a lot of understandable pressure. I have always identified myself here in my years as being one who fought against the compulsory mandating of legislation—I mean that then in turn made the States required to come up with the funds. I have always sort of been on the side of protecting the States from being subjected to this by the Congress and I am more than likely to continue in that vein. On the other hand, I am really concerned about the security elements of this.

Where are we, do you think, in this process? Suppose somebody goes out here on an appropriations bill or elsewhere and attaches an amendment to further modify the existing law on this issue? Now, we have got the extension period in there. That is safely ensconced, would that not be correct, Mr. Chairman?

Senator AKAKA. Yes, the initial enrollment period has been extended but not the reenrollment deadline.

Senator WARNER. But I am concerned that others may have reason for further attack, which I want to have a convergence of all the information that should be brought to bear and any further action by the Congress to impede the progress of this program. Where is another time when there is going to be a considerable amount of data out there to try and begin to show the States as to how to alleviate their cost projections today?

Mr. BARTH. Yes. I think that the time frame of August-September is when we are targeting issuing the final regulation, and to the extent we can, renewing our evaluation of the costs. So that is when I think you will find all the stakeholders will have something hard to shoot at rather than something soft, which is a proposed rule.

Senator WARNER. So it would be wise for the Congress now to withhold any further action until that time period?

Mr. BARTH. Except for the funding issue, which the Congress will consider separately——

Senator WARNER. As to whether we are going to step up and fund——

Mr. BARTH. Correct. There is the $40 million that has been appropriated for the grants to the States, but there has been no funding for the DHS or any department of the government for this program, nor, of course, for all the other costs of the State. So to that extent, I think that the cost issue is just a significant one. But until then, we won't be able to tell you even how much it is going to cost to build out that network of networks up there. So there is not a hard target to even fund, in my view, at this point in time.

Senator WARNER. Well, that is, I guess, my point. You really can't begin to ask Congress to give us so much money to try and defer some of the percentages of the State costs when each State is putting together their cost formula by different methods——

Mr. BARTH. And until, sir, they see the final regulation, they are not even——

Senator WARNER. That is correct.

Mr. BARTH [continuing]. Going to be able to put a final-final cost figure per State on it, which I regret that is after some States even go out of legislative session.

Senator WARNER. So it is in the best interest of Congress to ride through this thing until early fall?

Mr. BARTH. With the amount of time and effort I and my team are putting into this, I would greatly appreciate that, sir.

Senator WARNER. Well, I am only one. There are many here, but I certainly would hope that we would proceed on this on a partnership concept of States and the Federal Government working together and the Congress to try and achieve some type of identification that will help America feel a little more secure in our daily requirements to identify ourselves and to otherwise conduct our life here at home. I thank you.

Mr. BARTH. Thank you for your support, Senator.

Senator AKAKA. Thank you very much, Senator Warner.

Just to follow up on Senator Warner's questioning, Mr. Barth, you testified that we shouldn't act to change REAL ID. The proposed regulations state that DHS sought to provide for privacy and security to "the extent of its authority." However, the regulations ask for comments as to whether the privacy protections are adequate. Given that DHS has acted to the extent of its authority, what statutory changes to the REAL ID Act do you believe are necessary to protect privacy?

Mr. BARTH. At some point, Mr. Chairman, I think that the Congress should take seriously a concern that I believe we share with the privacy community, and that is that probably the biggest significant risk for identity theft, for issuing fraudulent cards, for collusion with bad actors in the DMVs, the biggest risk is those bad actors in the DMVs. There is currently law on the books that identifies penalties at the Federal level, penalties for collusion of DMV workers with someone outside the DMV in acquiring a fraudulent document. I would invite the Congress to look carefully as to whether or not those penalties are high enough.

If it only costs $4,000 to get a fake ID and lifetime employment in New Jersey, for example, not even committing bad acts, the penalty must not be stiff enough. If the cost goes up to about $50,000 or $100,000 per fake ID, then you might be getting close. So I make

that sort of in jest, but I think that the penalties there should be looked at closely.

I also think that one of the threats to privacy that has been identified is the lack of encryption of the machine-readable technology that is used on the back of many cards issued today. I think that the technology issues and the encryption issues will be well vetted in the regulation, but the Congress could also consider coming up with substantially higher penalties for fraudulent use of information obtained from drivers' licenses, REAL ID drivers' licenses. That should be a real linchpin of the cost of making an error here, or intentionally stealing data and using it fraudulently from a license is so high that I don't think I am going to do it.

Those are two very specific things that won't slow down our implementation of the rule, but will significantly enhance the effectiveness of whatever privacy protections we put into the rule.

Senator AKAKA. If Congress holds off on legislation, Mr. Barth, until the end of 2007, States will commit more and more funding towards REAL ID only to have the requirements modified if Congress acts on it later. Well, I want to thank you very much, Mr. Barth, for your responses to this Subcommittee and I want to tell you that we may have further questions for you that we will place into the record. Again, I want to thank you so much for being here with us.

Mr. BARTH. Thank you, Mr. Chairman.

Senator AKAKA. Now, I would like to call the second panel forward and welcome you to this Subcommittee.

Testifying on the second panel are: State Senator Leticia Van de Putte, who represents the 26th District of Texas in the State Legislature and is the President of the National Conference of State Legislatures. Welcome.

The Hon. Mufi Hannemann, Mayor of the City and County of Honolulu, who is accompanied by Dennis Kamimura, the Licensing Administrator for the City and County of Honolulu. Aloha and welcome, Mufi.

David Quam is the Director of Federal Relations for the National Governors Association. Welcome, Mr. Quam.

As you know, the custom of this Subcommittee is to swear in all witnesses, so will you please stand and raise your right hand.

Do you swear that the testimony you are about to give this Subcommittee is the truth, the whole truth, and nothing but the truth, so help you, God?

Ms. VAN DE PUTTE. I do.

Mr. HANNEMANN. I do.

Mr. KAMIMURA. I do.

Mr. QUAM. I do.

Senator AKAKA. Thank you. Let the record note that all witnesses answered in the affirmative.

I want to thank you again for your presence and we are looking forward to hearing from you. Senator Van de Putte please proceed with your statement.

TESTIMONY OF HON. LETICIA VAN DE PUTTE,[1] TEXAS STATE SENATOR, AND PRESIDENT, NATIONAL CONFERENCE OF STATE LEGISLATURES

Ms. VAN DE PUTTE. Thank you, Chairman Akaka, Ranking Member Voinovich. I am Leticia Van de Putte, President of the National Conference of State Legislatures and a member of the Texas State Senate. I appear before you today on behalf of the National Conference of State Legislatures (NCSL), a bipartisan organization representing the legislatures of our Nation's 50 States, its Commonwealths, territories, possessions, and the District of Columbia.

Mr. Chairman, thank you very much for your leadership on this important issue, not just today with this hearing, but with your introduction of legislation in both the 109th and 110th Congresses to fix the REAL ID Act. It is imperative that this hearing be the first step toward a successful, cost-effective implementation of the Act.

Legislators across the country share the goal of improving the integrity and the security of drivers' licenses and identification cards, but we want to make sure that it is done right. Mr. Chairman, as you know, NCSL will call for the repeal of the Act if the recommendations made in the September 2006 report,[2] "The Real ID Act: National Impact Analysis," issued by NCSL, the National Governors Association, and the American Association of Motor Vehicle Administrators, are not implemented and the mandate fully funded by December 31, 2007.

Mr. Chairman, I respectfully request that a copy of this report and the NCSL policy,[3] "Funds in the Fiscal Year 2008 Budget Resolution for Implementation of the REAL ID," be submitted for the record with my full testimony.

Senator AKAKA. It will be included in the record.

Ms. VAN DE PUTTE. Thank you, Mr. Chairman. NCSL acknowledges that the draft regulations incorporate a number of our recommendations made in the September 2006 report. However, they do not address several major recommendations, or more accurately stated, solutions needed for the successful cost-effective implementation of the Act. These solutions would ensure that the verification systems are available nationally, allow States to adopt up to a 10-year progressive re-enrollment process, exempt certain populations from the REAL ID process, and provide the necessary Federal funds.

Successful implementation of the Act with such a limited time frame largely depends on the availability of certain electronic systems to verify the validity of the identification documents. It appears that a number of these systems are not likely to be available on May 11, 2008, and given this fact, it is critical that the May 11 deadline be moved to a future date when the verification systems are available on a national level. Without this change, the States will spend billions of dollars to have a real pretty new card, but will have done nothing to actually improve security.

---

[1] The prepared statement of Ms. Van de Putte with an attachment appears in the Appendix on page 57.

[2] The Real ID Act: National Impact Analysis," report submitted by Ms. Van de Putte appears in the Appendix on page 119.

[3] "Funds in the Fiscal Year 2008 Budget Resoulution for Implementation of the REAL ID," submitted by Ms. Van de Putte appears in the Appendix on page 63.

States need to be able to adopt up to a 10-year progressive re-enrollment process. This solution would provide States the ability to manage enrollment over a greater length of time, would meet the objectives of the Act, reduce the fiscal effect on States and, on the Federal Government, and minimize service disruptions for customers. Mr. Chairman, in my State alone, without the 10-year progressive, reenrollment even hiring 900 new FTEs, which we would be required to do, and running our 27 new offices and our offices that are in effect right now 24 hours a day, we could not re-enroll 11.8 million drivers and ID holders. It is impossible to do.

Certain populations should be exempt from the REAL ID process. This exemption could be based on characteristics related to applicable risk, such as the year of birth or duration of the continuous relationship with the State. For example, under our draft regulations, an 82-year-old person who has lived in Texas his or her entire life would still have to make a visit to his or her local DMV. Is this really necessary? The verification requirements should be waived for applicants who have completed an identity verification process conducted by the Federal Government.

Finally, I would like to talk about funding. Whether one uses the NCSL, NGA, and AAMVA estimate for State implementation costs, of at least $11 billion over 5 years or the DHS figure of $10 billion to $14 billion over 10 years, the REAL ID is an enormous unfunded mandate. For Texas, our start-up costs will be $142.6 million for the first year with an ongoing operational expense of $67 million. It is critical that new Federal funds, and I emphasize new, be provided for State implementation of the REAL ID. States should not be required to use their diminishing State Homeland Security grants and should not be required to pay for access to the verification systems.

NCSL also recommends instituting a legislative trigger that would automatically release States from complying in any fiscal year that Congress fails to appropriate these funds.

Mr. Chairman, in closing, NCSL remains steadfast in its resolve to work with Federal policy makers to fix, fund, and implement the REAL ID Act before December 31, 2007, as stated in our policy, and I encourage you to consider legislative action to adopt the solutions I have proposed today. This will provide the States with the necessary certainty to move forward.

Thank you very much for this opportunity to testify.

Senator AKAKA. Thank you for your testimony. Mayor Hannemann.

TESTIMONY OF HON. MUFI HANNEMANN,[1] MAYOR, CITY AND COUNTY OF HONOLULU, HAWAII, ACCOMPANIED BY DENNIS KAMIMURA, LICENSING ADMINISTRATOR, CITY AND COUNTY OF HONOLULU, HAWAII

Mr. HANNEMANN. Good afternoon, Chairman Akaka and Ranking Member Senator Voinovich. Thank you very much for this opportunity to testify on the impact of REAL ID on the City and County of Honolulu, the capital city of the State of Hawaii, where three-fourths of our population resides.

[1] The prepared statement of Mr. Hannemann appears in the Appendix on page 65.

I am here, as you indicated earlier, with Dennis Kamimura, who has over 30 years' experience of running our licensing program, and the City and County of Honolulu licenses 70 percent of the 867,000 drivers in the State of Hawaii. Moreover, all of the State's drivers' computer records are stored in Honolulu's computer system.

We, wholeheartedly, agree that the tragic events of September 11 require the strengthening of our security standards, procedures, and requirements for the issuance of drivers' licenses and identification cards, but we have several major concerns with the implementation of this law and they basically fall in four areas, Mr. Chairman, with respect to funding, the verification process, re-enrollment, and waivers.

It will cost us $25.55 million over a 5-year period if this law were implemented. About 90 percent of this $25.55 million will be incurred by the City and County of Honolulu, and although the Department of Homeland Security announced that 20 percent of the States' Homeland Security Grant Program funds could be made available during the 2007 grant cycle, most of these funds have already been dedicated.

I would also add that we have recently upgraded the status of our Civil Defense Agency now to a full-fledged cabinet-level department called the Department of Emergency Management. That Department will be charged with securing other types of Homeland Security grants into areas that Senator Voinovich had already indicated, like interoperability, the pandemic flu, and other areas there that we would like that department to focus in. So therefore, we would be hard-pressed to tap into this 20 percent for this particular program.

With respect to the verification process, the Act requires that we refuse to issue a driver's license or identification card to a person holding a license or card issued by another jurisdiction. This is similar to a provision of the Commercial Motor Vehicle Safety Act, which requires commercial drivers to have one and only one license at any given time. This requirement is supported by CDLIS.

CDLIS consists of a central site and nodes in each jurisdiction. Access to CDLIS is provided through a secure private network operated by the American Association of Motor Vehicle Administrators and cannot be accessed through the public Internet. Each site connected to the private network has its access controlled by several security mechanisms. Neither the State of Hawaii or AAMVA is aware of any privacy breaches of CDLIS since it went into development in 1989.

In 2005, Congress passed the transportation reauthorization bill, SAFETEA–LU, which authorized $28 million to modernize CDLIS. Our recommendation is that we leverage this project and its Federal funding to expand the scope of the CDLIS modernization effort to support an all-driver pointer system for non-commercial drivers' licenses and identification cards, inasmuch as all jurisdictions are familiar with the CDLIS program, and the all-driver pointer system would use the same principles as CDLIS. Use of this technology would be more efficient than expending public money to create a new system.

The Act would also require us to have access to five additional national databases, SSOLV for Social Security cards, Department of State for passport and consular report of birth abroads, EVVE for birth and marriage certificates, and SAVE for permanent resident status, employment authorization, or U.S. certificate of citizenship or naturalization, and SEVIS to verify the duration of lawful status for student aliens. Obviously, we have challenges with all the aforementioned.

At present, almost all jurisdictions are using the SSOLV, which requires enhancements due to its unreliability. Several States are also using SAVE, but that system requires major improvements to ensure appropriate functionality to operate in real time with accessibility and reliability. Several States are testing EVVE. However, the system will not be fully operational until December 2009. There is no electronic accessibility to SEVIS and/or the Department of State database.

We should not be required to use systems that are unreliable or under development. These systems should be developed and tested before placing the burden on local jurisdictions and the public that we serve. Additionally, we believe that Federal agencies operating these systems should be prohibited from charging jurisdictions transaction fees that only increase our operating cost.

With respect to re-enrollment, the majority of our licensed drivers in the State of Hawaii are issued State identification cards over a 6-year expiration period, so therefore the 5-year re-enrollment as called for in the REAL ID Act will present some challenges there. We recommend that the period be at least 7 years.

Finally, with respect to the waivers, to facilitate the processing of all applicants, we recommend that applicants who are 72 years old or older be granted waivers from the verification requirements of the Act. Similarly, individuals who are required to undergo the same or more stringent verification process for Federal identification be granted waivers. Last, if an applicant has undergone the verification process in one jurisdiction and has been issued a REAL ID-compliant driver's license or identification card, the verification process by the gaining jurisdiction should be waived.

In conclusion, we support the intent of the REAL ID Act, but practical considerations aside, Mr. Chairman, the City and County of Honolulu cannot afford to implement the requirements of the Act without initial and continuing Federal funding. If funding is provided, the time limits for implementation of the program without the required electronic verification systems will place an enormous burden on the driver's licensing staff and be a tremendous inconvenience to the public. To ensure long-term success, a more realistic implementation plan should be developed with input from the jurisdictions who bear the burden of issuing drivers' licenses and identification cards.

Thank you for granting me the opportunity to provide our perspective on this issue, Mr. Chairman.

Senator AKAKA. Thank you very much, Mr. Mayor. Mr. Quam.

TESTIMONY OF DAVID QUAM,[1] DIRECTOR, FEDERAL RELATIONS, NATIONAL GOVERNORS ASSOCIATION

Mr. QUAM. Chairman Akaka, Senator Voinovich, thank you very much for holding this hearing. I note as you did in your opening statement this is one of the first real hearings on REAL ID and that may be the most important thing that is happening today: Congress is taking an honest look at what this law means both to the States and the Federal Government, and probably more importantly, to our citizens.

I do not know of a single governor who is not a homeland security governor. Every one is very concerned about the security and integrity of their driver's license systems. Most States after 9/11 were already in the process of improving their systems when REAL ID came about. NGA supported the negotiated rulemaking process that was put together by this Subcommittee in the Intelligence Reform Act. It is both unfortunate and ironic to note that if that process had been allowed to continue, we probably would be done today.

While several other folks here have noted some of the problems with REAL ID, I am going to focus really on solutions. I will note that NGA and governors have not called for the repeal of REAL ID. What we have done is try to work—governors have tried to work with their States, with motor vehicle association administrators, and also with legislators to find a fix, and that is going to require three things: More time, more flexibility, and additional funds.

The most important message I can give to this Subcommittee and to Congress today is that REAL ID cannot be fixed without Congressional action. It cannot be fixed without legislative action by Congress.

First and foremost, provide adequate time. Certainly, everyone recognized, including DHS, that May of next year was not enough time for States to prepare. NGA recommends that this Subcommittee adopt specific statutory deadlines. Alter the deadlines of REAL ID and set them to the later of December 31, 2009, which is the extension granted under the proposed regulations, or a date that is 2 years after the publication of final regulations, whichever is later. That deadline should be set to when States actually know the rules.

Grant all States a 10-year window in which to re-enroll all of their citizens. Moving the deadline on the front end but not giving a corresponding extension on the back end only means that States have to enroll more people in a shorter amount of time. That maximizes cost, minimizes efficiencies, and hinders States' ability to implement this Act.

And finally, what several other witnesses here have cited, allow us to manage the line. Certain populations can be pushed to the end of the line while we give REAL ID to other folks up front. That allows States to keep some of the efficiencies that are so important to customer service.

Second, the verification systems. I thought Secretary Barth did an excellent job of stating how critical electronic verification is. Without it, REAL ID doesn't work. Until it is online, States should

[1] The prepared statement of Mr. Quam appears in the Appendix on page 69.

not have to comply. It is that simple. Congress should amend REAL ID to specifically allow States to use existing verification practices until all necessary Federal and State systems are fully operational and deployed. The States won't hesitate to put them in place, but they can't be expected to use them until they are in place.

Next, encourage State innovation. I was happy to hear that the Secretary may be willing to use his waiver authority and extension authority if States are making progress towards implementing REAL ID. These are extraordinarily complex systems. It will take time to build these systems and to prepare them and fund them, especially considering some State legislatures are going out of session. Budgeting time and planning time needs to accommodate State schedules.

I will note, however, that even with the extensions of time, the proposed regulations are going to require all States to submit a complete certification package by February 10, 2008. That is ahead of the original statutory deadline. That plan must include milestones, schedules, and estimated resources needed to meet all the requirements of the rule. If we don't finish this rule until August, September, or October of this year, that is a very short turnaround for States to do complete planning and go to DHS and say, this is how we are going to implement. That deadline should be pushed at least 1 year by statute past the time of Federal regulations. That is adequate time for the States to plan. States aren't asking to put it off indefinitely, just give them time to plan.

Finally, sufficient funding, which it has been discussed here repeatedly. It cannot be underscored enough. Congress must provide specific authorization of funds to cover the cost of REAL ID over the next 10 years. Specifically, it should also appropriate at least $1 billion in fiscal year 2008 to fund the initial cost.

One thing I would like to point out, the cost estimates that were done by States were very carefully done. Phone calls were made to make sure that all States were comparing apples to apples, oranges to oranges. Not to contradict the Secretary, but I am going to contradict him. That was a very careful study and the $11 billion that States came up with is a minimum and a hard minimum that it is going to cost States to implement.

Governors are very concerned with REAL ID. Governors want to make it work. If DHS wants to give States the flexibility to run with it, then they should give it to us completely. States can get the job done, but we are going to need time. Thank you.

Senator AKAKA. Thank you very much.

I know Senator Voinovich, being a former governor and mayor, is very anxious to ask some questions here, so I will try to be brief.

My first question is for the entire panel. If the final regulations for the REAL ID Act are issued this fall and remain substantially similar to the proposed regulations, when would your States or a majority of States and localities realistically be able to comply with the Act?

Ms. VAN DE PUTTE. Thank you, Mr. Chairman. Our problem is not the wanting to comply, it is that we are going to have difficulty complying if the verification systems aren't ready. We can't set a date on which we can comply until the Federal Government itself

has those verification systems operational. What we will have is a pretty card with no way to verify a person's identity. So I think that we really need to look at the budget process and the Federal Government and how much it is willing to put into the verification systems because we can't comply unless those systems are in place.

Senator AKAKA. Mayor Hannemann.

Mr. HANNEMANN. Mr. Chairman, as indicated earlier, counties and cities are at the mercy of many of these mandates that come from the Congress or the Federal Government or the State. Right now, our legislative session is due to end in May. There is no vehicle for any type of funding. They recently, as you pointed out in your opening statement, issued a resolution basically expressing their concerns. We will not be able to comply at all for the following reasons that I indicated in my testimony. So not only is the funding not there, but even if we had the funding, there still are some concerns with respect to the verification process, the re-enrollment, and obviously the waivers. So it is very unrealistic for us to even figure out a way in which to comply given the concerns we continue to have.

Senator AKAKA. Mr. Quam.

Mr. QUAM. Just to echo that, REAL ID cannot be solved by any single issue. Money alone will not do it. An extension will not do it. It has got to be a comprehensive solution using both Congressional power and regulatory power at DHS to give States what they need. Until we know that picture, we are basically being handed a Monopoly board without instructions and saying, go play. You have no idea what the objective of the game is or how to play. We need the final rules and then we need the time to implement them and understand them to move forward. So unfortunately, at this time, it is one of the reasons we say REAL ID is unrealistic as planned.

My other concern, Senator, is that the regulations may not look as they currently do. I will give DHS its due. The first time we really understood how much DHS had listened to States was when the draft regulations came out. I was very pleased to hear they had been talking to four States, but there are 50 States and five territories that are going to be involved in this process and it is going to take time for us to move forward and understand exactly what is going to be required of States.

Senator AKAKA. Thank you. As you know, the regulations do not address what someone can do if another State loses or mishandles their personal information. Could each of you address how different States would handle this situation?

Mr. HANNEMANN. Let me defer to Dennis Kamimura, who, as I said, he has 30 years of running this operation for our State. He is also a very active member of AAMVA. And I just wanted to, if I may before I turn it to him, Mr. Chairman, just echo what was said earlier. We want to participate. We want to be able to give our input, and so far, we have been doing it through AAMVA, but we would like to see more of a reaching out process on the part of the Department of Homeland Security as opposed to cities or counties or States petitioning them for input and the like. We think it should be a two-way street. As I said, we have been able to do most of our input through AAMVA, but we really believe that this is

part of our petition here today, is to get a little more of a reaching out process from them.

Senator AKAKA. Mr. Kamimura.

Mr. KAMIMURA. Mr. Chairman, essentially, the REAL ID Act does, in fact, provide for Federal penalties involved in misinformation or handling of information or release of data, personal data, that is not supposed to go out. Speaking for Hawaii, Hawaii does have penalties involved with release of personal information and I think what happens is that under the REAL ID, we would have to comply with whatever the Federal requirements are. But I don't believe that Hawaii would, in fact, loosen its requirements on any penalties for stolen identity, for example.

Senator AKAKA. Mr. Quam.

Mr. QUAM. What we have heard on the privacy front is a great concern for how these databases will be managed, and now that we have a better sense with regard to the regulations, there is some additional comfort in the States. However, I would note that there are several States who have privacy laws that are probably stronger than anything that the Federal Government would actually impose. One of my fears is that the privacy regulations will come out and actually loosen State standards with regard to privacy.

I think addressing privacy may be one of the real critical missing links in moving forward. The negotiated rulemaking would have addressed that. It would have brought a lot of different players to the table. It is unfortunate that was not allowed to finish, but I think addressing the different standards States have and not lessening those standards will be critical moving forward.

Senator AKAKA. Senator Voinovich.

Senator VOINOVICH. Thank you, Mr. Chairman.

This is typical of the Federal Government, REAL ID was put into the emergency supplemental bill in 2005, with no hearings and no consideration about how it is to be implemented. Senator, you are from Texas, as you know first hand, we have a problem with the border, an immigration problem. If the Congress had given money to Customs and Border Patrol to do the job, we wouldn't have the problem today, but we didn't. Finally, Congress has recognized the problem and is funding CBP. This is typical of what we do here in the Congress.

I would like your respective organizations, the National Council of State Legislatures, the NGA, to get back to this Subcommittee on what you are being asked to do with the State Homeland Security Grant Programs. I think it is ridiculous that they are saying to you, take the money and use up to 20 percent of it to offset the costs REAL ID. This money has already been spent or allocated by the States to pay for other programs like interoperability.

I would like to get into some specifics about timing. Now, how much time after the final rule comes out, assuming that you feel that they are decent and proper, would you need to implement REAL ID?

How much time would you think would be reasonable to give people in each State the ability to sign up? Much of the cost is going to happen during the intial phases of REAL ID as States bring people into the program. States are going to have to hire

many more people to handle the registration. Ms. Van de Putte, how many new people did you say Texas would need to hire.

Ms. VAN DE PUTTE. Minimally, our statistics say that we have to hire 741 new FTEs, but we are reshifting close to 200 that are already in the department. So we have achieved some cost savings in other areas, but new hires will be 741 FTES. Senator, that was a very conservative estimate.

Senator VOINOVICH. So you are working harder and smarter and you shifted 200 people over that were doing something else, but you need 700 to get the job done?

Ms. VAN DE PUTTE. Yes, sir.

Senator VOINOVICH. Could I get your opinion on these milestones and how you would set the deadlines?

Mr. QUAM. Senator, I would be happy to, if I may, and starting with final regulations as the key date, and why any of the deadlines were not set from there, I am not sure because that is the time when States know what is expected of them. That is when final regulations actually come out. So let us say that is August.

Senator VOINOVICH. Why don't we just say that it is December 31.

Mr. QUAM. December 31, excellent. DHS has said from a regulatory standpoint that it wants—it is going to use a certification process, which States are familiar with and States actually recommend it. That certification is to present the State plan. We would recommend that should be 1 year from the date of final regulations, that the State submits a plan. That will allow us time to start putting all the different pieces in place.

Senator VOINOVICH. One year to submit a plan of how you are going to comply?

Mr. QUAM. To DHS, correct. We would recommend 2 years from the date of final regulations before the first REAL ID has to be issued, the shorter of that date or the extension that was given under the regulations, which is to the end of 2009, whichever is later, and part of that is to defend against this regulation dragging on. I will note that we only got it this year. We needed this regulation the day the law passed, not 2 weeks ago.

Senator VOINOVICH. So you are talking 3 years actually from, say, December 31 of this year? That is 1 year to submit it and then 2 years thereafter to——

Mr. QUAM. I am actually talking 2 years from final regulations to begin.

Senator VOINOVICH. OK.

Mr. QUAM. I think the States could do that and should recognize the flexibility DHS has given.

Senator VOINOVICH. What about if the verification isn't there?

Mr. QUAM. That goes to a different issue, which is what does it mean to be compliant, and I think a core question is, States can meet that in 2 years if they have the flexibility to use whatever is at their means to verify identities. If the systems are up, running, deployed, working, and populated—that means they have the data in them—then States might be in a position to use them. If they don't exist, States have been verifying this information for several years using best practices. They should be allowed to continue to do that and use those verification processes as we transition. That

way, 2 years from now, States could begin issuing REAL IDs. So you have to change the definition of what it means to comply, and I focus on the verification systems. If they are there, we will use them. If they are not, best practices.

Finally, the end game. When will we finish this process? We have called for a 10-year window from that date, from beginning to end, to bring everybody in. Allowing the States to manage the line so that people can come in, you can use certain efficiencies—there are populations, say, born before 1935, or folks who have been in the State for 20 years——

Senator VOINOVICH. In other words, what you would do as part of your application is you would do some kind of a risk assessment about how States are going to phase-in people based on your experience, like I think you mentioned somebody who is 83 years old. Give me a break.

Ms. VAN DE PUTTE. If a resident had a driver's license for more than 60 years, exempt some sort of population—sorry for the interruption, Mr. Quam.

Mr. QUAM. No, please.

Ms. VAN DE PUTTE. But those are the sort of things, Mr. Chairman, that we are looking at. But the timing issue—this couldn't happen at a worse time because most States will be out of legislative session, and several States are biennial legislatures, like Texas. And so we will hopefully have left to go back to our home cities after Memorial Day, and so there is this time lag. So the quicker that we can get these types of rules and regulations, we want to do it, we want it done right, but our fear is that we are going to have a really pretty card that gives people a false sense of security, but if you don't have the verification systems, if we are not able to have the flexibility, then it is really meaningless.

And everyone wants to adhere to the goals. I think what you have heard from us today is no one doubts the goals and we are all in agreement with that. It is the "how to," and we have had real problems with the "how to" and it is ironic, in fact, that had we continued with the negotiated rulemaking, we would have probably had this solved by now.

Senator VOINOVICH. Thank you.

Mr. HANNEMANN. Mr. Chairman, if I just might, just to add a few comments there. Normally, I would defer to our governor to make a statement on behalf of our State, but in this particular case there, as you know, Senator Akaka, in Hawaii, the counties issue the State drivers' licenses, not only for the County of Honolulu, but for Maui, Kawaii, and the big island. We would like as much time as possible. I have heard what our representative of NGA said, and even at that, we would really be pushing it. So we need as much flexibility and time.

I heard Senator Voinovich speak about some of the unique issues he faces with Canadian visitors that come to his State. Well, we are also particularly concerned with many of the foreign visitors. As you know, we are a State that is dominated by tourism. We depend on foreign visitors. Many of them invest in our economy. That would be another major concern, to get as much information out that this is all part of national security, but at the same time, we

want to continue to maintain good relations with our international visitors and the like.

Senator AKAKA. Thank you. We will have a second round.

Senator Van de Putte and Mayor Hannemann, we have all heard of the enormous unfunded mandate and the impact this will have on the States. Could you both describe exactly how the costs will break down in your States or counties to describe what the average American will have to do to get a REAL ID driver's license under the proposed regulations?

Ms. VAN DE PUTTE. Thank you, Mr. Chairman. Our cost estimates were done very conservatively and we were using the same methodologies as all the States and the counties in Hawaii. Very conservatively, for my State, we have a population of about 24 million, about 18.5 million drivers' and identification card holders. We would have to, under the timeline set by this guideline, fit about 13.8 million in that shortened time frame. We just physically can't do it. Our implementation total for first-year costs is $142.6 million and an annual cost of $67 million.

But the real problem in our State, as in a lot of other jurisdictions, is that we wanted to utilize technology and to make it easier for our citizens, particularly those who have had drivers' licenses and identification cards for a long time, and so we allowed the mechanisms of the Internet for Internet renewal and mail renewal, and so, in fact, for efficient government, we closed down lots of offices. We utilize technology. And we know now that because of these regulations, we will have to have about 741 new FTEs, and then we have shifted within the department some that would be able to do this. But we are going to have to open up 18 new offices and retrofit about 28 other new offices.

Part of our cost that we don't know will be what the security requirements are going to be for the physical locations. Under the draft rules and regulations, all of those physical requirements of security are for States and jurisdictions that issue over-the-counter. So, in other words, the application is made, all the verification is made, and then they receive the identification there. Some jurisdictions and States have a central location where they disperse, but Department of Homeland Security rules are going to require all of us to have every single office, and even in our rural areas, you might co-locate in a county clerk's office or in a rural community in the township's city offices. And so we have a lot of this sharing. We will not be able to service our rural citizens because of the security costs that have been mandated by the Department of Homeland Security for the integrity of the building itself.

So our costs break out to the majority of FTE. The other ones are the software and the verification. But many States were going along that pathway anyway. We were putting in millions of dollars for enhancing our security. But I think that what we see is the cost, and with all due respect to our folks at Homeland Security, when we know it is going to be $11 billion, to offer $40 million was almost an insult. And then their action to us when we asked them about the funds is that, oh, it is not our job. Our job is to put out the rules and regulations and that is Congress's job. So in other words, what they are telling you is that they are telling us to come talk to you about the funds. It doesn't make sense that they are

asking us, the Department is asking States and jurisdictions to try to put the heat on Congress to fund it. Their answer is, it is not our job.

Senator AKAKA. Thank you. Mayor Hannemann.

Mr. HANNEMANN. Yes. We give out about 867,000 drivers' licenses, of which 70 percent of that is issued out of the City and County of Honolulu. We estimated that of the $25.55 million, and once again, it is just a very rough estimate given what we know at this time, to implement the program in the first year will be $7.67 million. Over a 5-year period, it would be $17.88 million.

Mr. Kamimura runs his department with about 85 employees just to do drivers' licenses. Obviously, we are going to have to ramp that up. Our satellite city halls and various distribution points throughout the City and County of Honolulu will be challenged enormously. I think we will be facing everything from challenges to over-the-counter type of application processes to the long lines that everyone will experience. But I would expect that this number could increase as we know more about the challenges that we face and the opportunity that we have to leverage what the other programs are.

In fact, I talked about some of the databases that we need to access, the systems that need to be set up, and I know that my Director of the Department of Information Technology, Gordon Bruce, who works very closely with Mr. Kamimura's department on this whole aspect of making sure that we are spending more time online than waiting in line, he has expressed several major concerns about the REAL ID.

So these are just initial costs. It is obviously going to be very complicated, and therefore, if we are going to go forward, again, I hate to sound like a Johnny one-note, but we are going to need enormous Federal help, especially in the area of funding, to be able to even get to first base on this issue.

Senator AKAKA. Thank you very much. Senator Voinovich.

Senator VOINOVICH. Let us talk about Texas again so that everyone understands how difficult this is and how expensive it will be. First of all, you are going to have to get 700 more FTEs.

Ms. VAN DE PUTTE. That is correct.

Senator VOINOVICH. Then you are going to have to open up 18 new offices. Finally you will have to comply with new databases in order to verify the individuals.

So the real issue is how do we help you get the job done? I would be interested in your response to some kind of partnership. What if we paid for the initial, cost all of the software and other things that you would need to do to implement this?

Ms. VAN DE PUTTE. Yes, sir. The cost estimates that I have are based on the verification of documents using those five different systems that were talked about. It is an implementation cost of $3.4 million and an annual cost of $1.5 million. And so I would imagine that is probably about $5 million when our overall costs to implement are $210 million. So I guess if you take a percentage of that, that is just the verification of documents.

I think that what is a bigger cost for us is the minimum document requirements itself. The implementation cost of that, again, $15 million for my State with an annual cost of almost $17 million,

and that is requirements for the document itself. So those two put together might be something that would be workable for us.

But I think that each State is going to be different. There are some states that did not utilize technology in the 1990s, and particularly the late 1990s, and so they may have lots of physical spaces and offices out there and may not have done as some of our states that tried to be more efficient.

Senator VOINOVICH. Could you do me a favor? I would like, and Mr. Chairman, I think that the Subcommittee would agree, I would like the NCSL and NGA to give me the details of the costs. I can tell you that there is no way that the Federal Government is going to pay for all of this. But I think if you came back with a proposal with some kind of partnership it would be easier for this Subcommittee to develop some kind of funding program for REAL ID.

Senator AKAKA. Mayor Hannemann.

Mr. HANNEMANN. Mr. Chairman and Senator Voinovich, I think that is an excellent idea, this idea of a partnership that you are talking about. We would wholeheartedly also recommend the American Association of Motor Vehicles Association that we work very closely with to tweak some of the numbers and so forth.

My concern is always not only the implementation, but the ongoing maintenance costs, so we obviously would be very willing to participate in that, so we could——

Senator VOINOVICH. Mr. Chairman, one other thing, and I am sure this is how OMB works, they figure like even sewer and the water and the rest of it. Let them raise their rates locally and pay for it.

Mr. HANNEMANN. Absolutely. I have risen my sewer rates twice. [Laughter.]

Senator VOINOVICH. You are talking about annual cost. How much more will you have to charge for the new ID? I would like to get some idea of what those annual costs would be.

Mr. QUAM. Senator, if I may, a couple of things that are in the cost impact study that was done by NGA, AAMVA, and NCSL. I am very happy to report when the negotiated rulemaking ended, the three groups came together as the key stakeholders and basically said, we have to continue this good work. We have to make sure that our voice is heard in this context. And so we have worked very cooperatively together and it has been an excellent partnership and we would love to extend it to the Federal Government and Congress.

I will note in that report that $1 billion, the $1 billion I mentioned for an appropriation up front, is one-time cost. That was actually estimated by the States, one time, get the systems, buy them, man them, get the software, get everything up and running, one-time cost was $1 billion. The ongoing cost, then, over 5 years, you get to $11 billion over five years.

You made a very excellent point and one that is often missed. It is not stated in the regulations, but it should be plain to everybody. The Department of Homeland Security sees this as a fee-based system. In other words, we are going to pass the cost along to folks getting a driver's license or identification card.

Senator VOINOVICH. And by the way, they will raise thunder with you——

Mr. QUAM. Absolutely.

Senator VOINOVICH [continuing]. And the Members of Congress will walk away and say, we didn't do it. [Laughter.]

Mr. QUAM. That is exactly right. The number we use is the $11 billion over 5 years divided by 245 million driver's license holders, because we have to bring everybody back in in 5 years. That is pretty easy math. That is about $45 additional per card.

Now, I am a Maryland resident. It costs me $30 to renew. An additional $45 on top of that for my REAL ID. I need to get a new certified copy of my birth certificate. I went online today to see what that would cost me. That is another $43 that it is going to cost me to get Colorado to send me a certified birth certificate. And just to be safe, so I can get on the airplane in the meantime, if I want a passport, well, the passport fee is $96 and you have got to wait 10 weeks to get it. If you want to expedite that, tack on another $60. You add that list up and you are at $274.

Now, our citizens personally want to be secure and will stand in long lines to be secure, but if we don't really add value to this card as we move forward and do it in a responsible way, their resolve is going to end at some point, and you are absolutely right—their patience will run out and it will run out with local officials first and then with Congress.

Senator VOINOVICH. One last point and then I will finish up. I get weekly reports from my constituency office. The passport offices are being overwhelmed today because of WHTI. It is unbelievable, the demand for passports. The passport offices don't have the people to take care of their customers.

Senator AKAKA. I want to thank this panel very much. You have been very helpful and I want to thank you for being here and for your responses. I also want to extend my appreciation to those of you who traveled from out of town to be here today and I hope you have a safe trip back home.

Ms. VAN DE PUTTE. Thank you, Mr. Chairman, and thank you very much for having us here. I did want to note with Senator Voinovich's comments that part of our cost estimate is for new signage. In the Texas statute, we will have signage at each of the new offices that say that this is a Federal law that the State did not pass nor did the State fund and it will have the addresses and phone numbers of our two Senators and the local Member of Congress. [Laughter.]

Senator AKAKA. Thank you very much.

Ms. VAN DE PUTTE. Thank you, Mr. Chairman.

Senator AKAKA. I now call the third panel to come forward.

On our third panel we have Timothy Sparapani, Legislative Counsel for Privacy Rights at the American Civil Liberties Union, and Jim Harper, Director of Information Policy Studies at the Cato Institute.

As you know, it is the custom of this Subcommittee to swear in all witnesses. I would ask for you to stand and raise your right hand.

Do you solemnly swear that the testimony you are about to give this Subcommittee is the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. SPARAPANI. I do.

Mr. HARPER. I do.

Senator AKAKA. Thank you very much. Let the record note that the witnesses answered in the affirmative.

Mr. Sparapani please proceed with your statement.

TESTIMONY OF TIMOTHY D. SPARAPANI,[1] LEGISLATIVE COUNSEL, AMERICAN CIVIL LIBERTIES UNION

Mr. SPARAPANI. Thank you, Mr. Chairman. On behalf of the ACLU and its half-million members, we recommend that this Subcommittee mark up your legislation, S. 717, the Identification Security Enhancement Act, to replace Title II of the unworkable REAL ID Act. Because Senators never considered REAL ID on its merits, they should be free to vote to replace it with a licensing scheme that is both achievable and free of privacy and civil liberties concerns.

As you can see from the map, the REAL ID rebellion is sweeping the country. As of today, 30 States are moving to reject REAL ID and calling for Congress to replace it. Maine and Idaho have enacted legislation to completely opt out. Driven equally by the extraordinary threat the Act poses to privacy and civil liberties and its prohibitively expensive cost, States are telling Congress that no matter the consequences, they will not participate. Drivers and DMV officials are telling Senators to expect lines at every DMV, not just out the door, but around the block, every day. Congress must respond to this outcry, and I believe your legislation does that.

Therefore, the ACLU recommends three things. One, Congress should replace Title II of the REAL ID Act by enacting S. 717, which reestablishes a more workable process for improving drivers' licenses.

Two, members should submit comments calling on DHS to withdraw its Notice of Proposed Rulemaking.

Three, Congress should refrain from appropriating any funds to implement the REAL ID Act. Quite simply, there is no point in throwing good money after bad.

Because time is short, I will just mention that REAL ID raises intractable constitutional problems. It threatens First Amendment rights and arguably violates the constitutional principles of federalism by usurping State authority.

Make no mistake, REAL ID will be the national ID card. Since the Act's passage, legislators have proposed requiring everyone present a REAL ID to vote, get a job, obtain Medicaid, open a bank account, and travel on interstate busses, trains, and planes. In short, no person would be able to function in our society without providing a REAL ID.

Additionally, REAL ID and DHS regulations pose unprecedented threats to privacy in four areas. Those four are data on the face of the ID card, data in the machine-readable zone on the card's back, data in the interlinked national ID database supporting the cards.

And four, regarding transmissions of data between users. I will just mention a few of these privacy problems.

[1] The prepared statement of Mr. Sparapani appears in the Appendix on page 74.

First, data on the face of the ID card. REAL ID wipes out in States what are called address confidentiality laws by requiring that an individual's principal address be stated on the face of the license versus having a post office box. Consequently, police officers, elected officials, judges, and others will have their home address readily available to anyone who would want to see it. More importantly, an actual address endangers people like victims of domestic violence and sexual assault who are trying to flee their abusers.

Unencrypted data in the machine-readable zone creates an enormous threat, a new threat, Senator, of private sector third-party skimming of data and resale of data contained in that machine-readable zone. DHS's proposed regulations failed to close the loophole because they do not require encryption.

Contrary to DHS's assertions, it will become increasingly profitable for private sector retailers to skim each customer's data because the format of data collected will be standardized nationwide. This creates a huge new threat. Retailers will demand that customers provide these licenses for anti-fraud or customer loyalty purposes and then they are going to retain all the data. And then, of course, these companies can then resell it in two different ways. One, they can sell it for highly targeted and highly invasive direct marketing back to the people, or two, they can sell it to what we call data brokers, companies like ChoicePoint or Axciom or Lexis–Nexis, who in turn can sell it to other companies and to the Federal, State, and local governments. In short, Senator, everyone is going to know in the future what we bought and when we bought it, including books, magazines, medications, contraception, anything you can imagine. So, essentially, we have got some significant problems there.

There are also problems with data in the National ID Database. And again, contrary to DHS's assertions, this unprecedented data aggregation imposed by REAL ID will actually make America, I believe, more vulnerable to terrorism and crime, not less vulnerable, and that is because we are going to have, I think, massive identity theft and fraud. That is because the Act is going to require that, at a minimum, a huge new set of data along with biometric information and these documents, the source documents you have heard about, be aggregated in one place. And then, of course, we are going to make this data set available to hundreds of thousands if not millions of Federal, State, and local employees.

In addition, the identity theft and document fraud are going to be far more serious. Instead of obtaining just one password, an ID thief is going to have a treasure trove of data, and that is because DHS failed to build in basic computer security and safeguards.

I will mention one final data privacy problem, and that is that the REAL ID database, I believe, is going to lead to significant new data mining, and that is because, again, DHS refuses to prohibit data mining of this data set, not only by itself, but by any other Federal, State, or local agency. And prior to REAL ID, it was impractical to do this data mining. But when you aggregate and link the data sets, sir, you are going to end up with the easy kind of data mining that I think many of us would want to avoid.

So in closing, I just want to say, Senator, for this Subcommittee, it is your first opportunity to stop these abusive intrusions into America's privacy by DHS, and again, we would like to call on Congress to replace Title II of the REAL ID Act with an achievable licensing plan that does not threaten personal privacy or civil liberties.

Thank you, Senator.

Senator AKAKA. Thank you very much. Mr. Harper.

TESTIMONY OF JIM HARPER,[1] DIRECTOR, INFORMATION POLICY STUDIES, THE CATO INSTITUTE

Mr. HARPER. Thank you, Chairman Akaka. Thank you for inviting me to be here today, and congratulations to you on your leadership on this issue, along with Senator Sununu, introducing legislation to repeal REAL ID and restore the identity provisions in the Intelligence Reform Act that preceded it.

I am Director of Information Policy Studies at the Cato Institute, which is a research foundation dedicated to preserving limited government, individual liberty, free markets, and peace. I also serve as an advisor to the Department of Homeland Security through the Data Privacy and Integrity Advisory Committee, which advises the Privacy Office and the Secretary of Homeland Security on privacy issues. Today, I speak only for myself, not for the committee or for my Institute.

I have written a book on identification and identity issues that includes REAL ID. It is called, "Identity Crisis: How Identification is Overused and Misunderstood," so I think I am well-studied on this issue and hope to share some of my knowledge with you today.

I am going to be a little bit plainspoken at the outset here. We have done a lot of green-eyeshade stuff on previous panels about where the dollars come from and where they go. But I think the best conclusion is that the REAL ID Act is a dead letter and all that remains is for Congress to declare it so.

Let me make three points and then offer one recommendation, if I can, regarding your legislation.

First, on privacy, I think Tim Sparapani and the ACLU have done a great job of articulating the privacy concerns and I join them in their concerns. The Department of Homeland Security's regulation punted on some of REAL ID's most important technology, security, and privacy problems.

I want to emphasize briefly why concerns with the card are so substantial. Economists know that standards create efficiencies and economies of scale. When railroads in the United States moved to a single track width, much more transportation occurred on the railroads because there was a single standard.

I realize that is not a good example to use with a Senator from Hawaii, but understand that standards, a national standard in an ID card, means that ID cards will be used a lot more. You will have economies of scale in building the card readers, in the software and the databases to capture and use the information from the cards. Americans will inevitably be asked more and more often to produce

[1] The prepared statement of Mr. Harper with attachments appears in the Appendix on page 89.

their REAL ID and share the data from it when they engage in every kind of governmental and business transaction.

Others will use the information collected in State databases and harvested from REAL ID cards. Ann Collins, who is the Registrar of Motor Vehicles in the State of Massachusetts, spoke to the DHS Privacy Committee last week and she said, "if you build it, they will come." What she meant is that masses of personal information will be an irresistible attraction to the Department of Homeland Security and to others to dip into for an endless array of different purposes.

For good or bad, an ID card system is a sort of surveillance system and it is becoming increasingly clear that REAL ID is a surveillance system focused on the law-abiding as much as the wrongdoer.

I want to briefly talk about national security issues, because the privacy and dollar costs of REAL ID would be worth it if REAL ID got us any measure of security. If it improved the protections we have now, I think we would all be in favor of REAL ID, but it doesn't. You have heard the cost figures, so I won't belabor them.

I was very concerned about the lack of risk management-oriented discussion I heard even today from Assistant Secretary Barth. Creating a national identification scheme does not just attach a known accurate identity to everyone in the country. It causes the wrongdoers to change their behavior. Sometimes this will control risk. Sometimes this shifts the risk from one place to another. And other times it can create even greater risks.

I want to give you an illustration about how a system like this works from a report that was released just last week in the United Kingdom. The U.K. home secretary's office released a report saying that about .5 percent of all U.K. passports are based on fraud. That means about 10,000 per year are issued based on fraud. Now, what kind of security do you get from that system, if you have a .5 percent fraudulent error rate? That is not a security system for purposes of national security. That is not a security system against committed terrorists. Perhaps the U.K. should have a national ID so we in America don't have to.

In my written testimony, I have submitted a better cost-benefit estimate than DHS did, and I am disappointed that they did not—they have not done better risk analysis up to this point. But all the money that goes into REAL ID is, as Senator Voinovich emphasized, coming away from other programs that are just as important.

Finally and briefly, I want to emphasize an issue that I think is very important that has not been considered yet, one that I realized was quite prominent when I went through the regulations and the specifications in the regulations. The specifications called for by DHS to go on REAL ID-compliant cards has race and ethnicity as one of its key data elements. DHS does not specifically require inclusion of this information, but States are likely to adopt the entire standard when they do get in compliance. Thus, in May 2008, many Americans may start carrying nationally uniform cards that include race or ethnicity in machine-readable formats. This will be available for scanning and collection by anyone with a bar code reader. Government agencies and corporations alike may affiliate

racial and ethnic data more closely than ever before with information about our travels through the economy and society.

On this poster, I have reproduced the design specifications, which indicate race and ethnicity, and here is how they would be indicated on a card. This is an example of what a card may look like, the two–D bar code. And I have included here, because this is such an important issue, an ID card from Rwanda.[1] In Rwanda, a national identification system that included ethnicity was very useful in the unfortunate, horrible genocide that occurred there. I do not believe that this was intentional on the part of DHS or anyone in Congress to have this kind of system. It is a product of error and it is a product of this system and REAL ID not being carefully considered in Congress before the law was passed.

With that, I have taken up quite a bit of your time. I have recommendations in my written testimony that I would refer you to. Thank you very much for hearing me out and taking my testimony.

Senator AKAKA. Thank you very much for your testimony.

Both of you have discussed how the REAL ID Act infringes on Americans' privacy rights and civil liberties and have spoken in support of my legislation which would repeal REAL ID and replace it with the negotiated rulemaking process in the Intelligence Reform Act. Other than a straight repeal and replace, are there any changes that can be made to the REAL ID Act that would specifically address the concerns you both raised today? Mr. Sparapani.

Mr. SPARAPANI. Yes, Senator, I think there are a couple that could be made. I mentioned one, or at least alluded to it in my testimony. I am really quite concerned, and the whole privacy world is concerned about this new threat about third-party skimming of data off the back of the card. Congress really needs to do what it did in part back in 1994 when it passed the Drivers' Privacy Protection Act in closing down privacy loopholes involving this important data. Congress should specifically prohibit the resale of that data, or the sharing of data with an additional third party beyond the party that is collecting it.

Additionally, I would just like to say on the constitutional standpoint, there are some intractable constitutional problems and I think you would have to rewrite large portions of the Act to get to that point and I think your legislation understands that. But clearly, we have got some First Amendment concerns here that won't be addressed unless there is a specific statutory exception created for some of those well-respected Supreme Court-protected rights.

Senator AKAKA. Mr. Harper.

Mr. HARPER. I don't believe that REAL ID can be fixed. I don't believe it can be improved and made to work. The Chairman of the full Committee, Senator Lieberman, said when REAL ID passed that the law was unworkable. It remains unworkable today and the proof of it is borne out on the earlier panels.

I don't think that a national ID system of any stripe or character can provide the security that a lot of people assume it does. So it is important to have a conversation about this, to learn how ID actually works, how it breaks, what it is useful for, and what it is not useful for.

---

[1] The ID card from Rwanda appears in the Appendix on page 107.

In my written testimony, I have suggested considering some of the emerging digital identity management systems that are coming online. There are systems that exist today that can prove, for example, to the TSA that you are a member of the Registered Traveler Program but that don't tell the TSA who you are, and that is an important, narrow anti-surveillance feature. Prove to the TSA that you have been secured by their processes, but don't give them the opportunity to record where you have been and where you have gone and that kind of thing.

These systems are coming online now. They are a little bit future-oriented. We should look down the horizon to these systems. But the last thing we want to do is build a government system, spend these millions and even maybe billions of dollars to build these government systems that ultimately are dead ends, very expensive dead ends. We need to integrate with the systems of the future, and so I think the whole thing needs to be reconsidered and this hearing is a good start.

Senator AKAKA. Mr. Harper, in your testimony, you mentioned how by creating REAL ID the Federal Government and the private sector will find creative uses for the data outside of the reason for which REAL ID was intended. Can you discuss some of these other ways the information on a REAL ID card or in a REAL ID database can be used?

Mr. HARPER. Well, it is interesting to travel in homeland security circles sometimes because you hear lots of talk about different plans that people have for REAL ID once it is in place. Let us do this with it. Let us do that with it. Frankly, the Department of Homeland Security itself has retreated somewhat from the idea that this provides security benefits. Secretary Stuart Baker came and spoke to the DHS Privacy Committee and suggested how strongly it would prevent against identity fraud. I proceeded to go to the regulatory docket and found that the estimate there is that it would prevent $1.6 billion worth of fraud. That is a $17 billion cost to save $1.6 billion. It doesn't quite balance out.

But other proposals, we would use this to prevent underage drinking. We would use it to prevent underage smoking and that kind of thing. A terrific regulatory system, a terrific police state system for controlling all of our personal behavior. But that is inconsistent with the way we are supposed to live in the United States. It is inconsistent with having a free country. We do indulge a little unlawfulness along the margins, and many people who went to college understand that in terms of ID. When you are 20 years old, you really want to hang around with your 21-year-old friends. Do we want to make a $50,000 or $100,000 penalty come down on that kind of person? I think that is going the wrong direction.

So there are lots of different ways to regulate and control the generally law-abiding populace and REAL ID would help with that, but I don't think that is what we want to do.

Senator AKAKA. Mr. Sparapani and Mr. Harper, as you know, the proposed regulations leave open the question of how States are to share drivers' information with each other. However, DHS repeatedly claims that the system will resemble the Commercial Drivers'

License Information System. What is your opinion of CDLIS and the privacy protection that is in place? Mr. Sparapani.

Mr. SPARAPANI. It is a good question, Senator. If you listen to Mr. Barth's statement earlier today, and in your question and answer period with him afterwards, I think he went at great length to talk to you about interconnectivity between systems of systems and networks. I think we are talking about a maximal sharing of data, not a minimal sharing of data. And so, in fact, I am really quite concerned about the volume. I mean, he showed the chart with all of the systems that would come online and that they would all need to talk to each other.

This isn't going to look like CDLIS. This is going to look like CDLIS on steroids, if you will. So we are really talking about a plussed-up maximum sharing of all of our most sensitive personally identifiable information, and that is exactly the information that we don't want to have get in the hands of terrorists, immigrant smugglers, sophisticated criminals, and it will be easy and ripe for the taking and we will put it all in one place and then we will transmit it widely for anyone to intercept. I think it is the worst choice we could have made.

Mr. HARPER. Allow me to speak about CDLIS in terms of data security. Security turns out to be not a function of what you do to protect a thing, it turns out to be a function of how motivated your attacker is. I have got a shoebox at home that has never been breached. It has never been the subject of a breach. If I put information in there, a business card, no one would ever look at it. If I started to store bars of gold in that shoebox, it would be much more likely that that system would be breached.

So if you take the CDLIS model and expand it out to records about politicians, law enforcement officials, Paris Hilton, if you make that system the security that terrorists want to break, well, that is a much more attractive system and it is much more likely to fail than the CDLIS of the past, which has information about 13 million truck drivers.

Senator AKAKA. I have another question for both of you. Although the REAL ID Act replaced the negotiated rulemaking under the Intelligence Reform and Terrorism Prevention Act of 2004, I understand that DHS has been working with the privacy community to protect personal information. Can you tell me how you have been working with DHS and what recommendations you made to the Department that you see reflected in the proposed regulations?

Mr. HARPER. Well, Tim Sparapani was good enough to convene a couple of meetings with the regulators, and they were good to hear from us. It was welcome to have that input. So there is no fault in terms of the process or the people at DHS.

I recommended that these databases, which are created subject to Federal law for Federal purposes, basically using a Federal mandate, should also be subjected to Federal laws like the Privacy Act. Condition compliance with REAL ID for States. Condition their certification of compliance on the fact that they have met Privacy Act standards. Condition that compliance on the fact that they have met FISMA, the information security law.

DHS chose not to do that, citing federalism concerns that I think are a little stretched. Given the fact that the REAL ID Act was de-

signed to eviscerate the distinction between the State and Federal Governments, and I think that is inappropriate, being especially carefully and following Marquise of Queensbury Rules when it comes to privacy and data security is a little bit off.

Senator AKAKA. Thank you.

Mr. SPARAPANI. Senator, if I could respond very briefly, indeed, we were invited in to come and meet with DHS, but what I have heard over and over again over the last 2 years, and it is a remarkably long period of time, is something that is baffling to me. Here is the justification DHS is using for having a minimal approach to privacy in these regulations. They say that because the word "privacy" does not appear in the statute, they don't feel that they have sufficient authority to grant maximal protection to this information that we know, frankly, is more valuable than the gold in your bank account because it can be used for all sorts of other purposes besides just financial fraud.

So with respect to the DHS Office, they have been good about meeting with us, but they have turned a deaf ear to the fact that in the information age, personal information is more valuable than gold and has to be protected at a much higher standard. We have to treat this like a bank vault.

Senator AKAKA. Thank you for that. Mr. Sparapani, you mentioned several constitutional concerns with the REAL ID Act in your testimony. Would you please elaborate on those issues?

Mr. SPARAPANI. Senator, they are really unprecedented, as I said, and as my written statement elaborates on. I see at least four different First Amendment concerns, a Second Amendment concern, a derivative Sixth Amendment concern, and probably a Tenth Amendment concern, as well as significant due process concerns. Let me just touch on one of the due process concerns very briefly.

If the government begins to demand that people produce a REAL ID-compliant driver's license to get all sorts of benefits, to enter a Social Security office, etc., many people in our society, lawful, law-abiding Americans, won't be able to produce the documents they need to get a REAL ID. And then when they need to get certain benefits, whether they be Medicaid or Social Security disability, etc., they won't even be able to get into the room to meet with the government officials to obtain those benefits.

Similarly, if we begin to say that people who don't have a REAL ID license can't enter certain Federal buildings, they will not be able to exercise, I think, their First Amendment-protected right to petition their government for redress. Now, in Washington, everybody knows nothing is more important than having a face-to-face meeting with your elected official so you can actually ask to have your concerns addressed. Again, when ID becomes a barrier to people exercising their constitutionally-protected rights, we have extraordinary problems.

I think it is these kind of constitutional weaknesses in the law which are going to require a complete rewriting of certain sections of the Act. I think that is why S. 717, the bill that you have introduced, is really the appropriate direction to head.

Senator AKAKA. I want to thank you both so much for your responses. This has been a very interesting hearing and your testimony will help the Subcommittee with our work.

Several of the problems with the regulations that have been identified are the direct result of the strict statutory language of the REAL ID Act. Based on our discussion today, it is evident that, at a minimum, Federal funding is needed to help State Governments enhance the security of drivers' licenses and legislative action is required to ensure that Americans' privacy and civil liberties are protected. I look forward to working with my colleagues and stakeholders to address these vital issues and look forward to working with you, also.

The hearing record will be open for 1 week for additional statements or questions from other Members.

Again, this has been an excellent hearing. This hearing is adjourned.

[Whereupon, at 5:05 p.m., the Subcommittee was adjourned.]

APPENDIX

PREPARED STATEMENT OF SENATOR LIEBERMAN

I want to thank Chairman Akaka for convening this hearing today which will provide the Committee an opportunity to finally shine much needed light on the REAL ID Act of 2005 by reviewing the rules that have been proposed for this program in an open forum.

Earlier this month, the Department of Homeland Security (DHS) issued a Notice of Proposed Rulemaking (NPRM) implementing the REAL ID Act. The NPRM, which took the Department almost 2 years to issue, does little to alleviate the concerns that I, and many of my colleagues, expressed 2 years ago when the REAL ID Act was attached to an emergency spending bill and forced through Congress without debate or substantive consideration.

The proposed regulations will cost approximately $23 billion according to the Office of Management and Budget, will bring Department of Motor Vehicle offices across the United States to a stand still, and may actually jeopardize security. We should not cause undue burden to the American public if security can be achieved in a more sensible way.

I remain fully committed to increasing the security of drivers' licenses and identification cards, which should be a top priority for this country. However, I am concerned, as I was 2 years ago, that the REAL ID Act impedes rather than facilitates the achievement of that goal.

In 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act to implement the recommendations of the 9/11 Commission. Senators McCain, Collins and I worked together closely to produce reasonable, bi-partisan solutions based on the Commissioners' recommendations. One recommendation required the Federal Government to set national standards for the issuance of drivers' licenses and identification cards. This was based on the Commission's finding that many of the 9/11 hijackers obtained U.S. identification documents, some by fraud. We took this recommendation seriously and carefully crafted provisions—with input from both sides of the aisle and all interested constituencies—to increase the security and reliability of drivers' licenses and identification cards. Our provisions were endorsed by state and local governments, the Administration, and a range of immigration, privacy, and civil liberties advocacy groups.

Regrettably, the REAL ID Act repealed those balanced provisions and replaced them with an unworkable, burdensome mandate. I opposed the REAL ID Act because I believed it imposed such unrealistic requirements that without substantial time and resources, it would not be implemented, making the Nation less safe as a result. If the original Intelligence Reform Act provisions had not been repealed, States would be well on their way to securing drivers' licenses today. Instead, DHS was saddled with implementing such a controversial and complex law that the Department took 2 years to issue regulations.

After reviewing the NPRM, I remain concerned about REAL ID implementation because it does not appear that DHS has addressed many of the problems and concerns identified 2 years ago.

First, the REAL ID Act requires States to verify all documents used to obtain a REAL ID, such as a birth certificate. To do so, States must rely on a series of electronic systems and federal databases. Yet some of these databases don't exist or are incomplete. Others are known to contain inaccurate data. One of the most egregious examples is the Electronic Verification of Vital Events (EVVE) system, which was developed by the National Association for Public Health Statistics and Information Systems (NAPHSIS) to provide a single interface for verification of birth and death records. EVVE is currently in pilot form, and only seven States have access. Even if all fifty States had access to the EVVE system, it would not allow for credible electronic verification of birth and death records because the database will not con-

tain records from all the States. NAPHSIS issued a report in January 2006 stating that the EVVE system could take as long as 7 years to be fully operational. The report specifically noted that the system must be implemented nationwide before it will be beneficial for REAL ID. A valid, verified birth certificate is at the heart of REAL ID, yet the timelines for these two programs are completely incompatible.

In addition to the EVVE system, REAL ID relies upon a non-existent State Department system to verify U.S. passports and the DHS Systemic Alienation Verification for Entitlements (SAVE) system, which is notorious for containing erroneous, incomplete, or outdated information. Moreover, even though the success of REAL ID depends on these systems, there is no requirement in the REAL ID Act or in the NPRM that the federal agencies provide these systems in a timely or accurate manner. The States will be left holding the bag if the Federal Government fails to deliver.

I am also troubled by the incomplete nature of the proposed regulations. There is virtually no guidance in the NPRM regarding what type of electronic system will be used to share information between States. This detail is critical to understanding the security and privacy vulnerabilities that may be created by REAL ID. Assistant Secretary Barth has said that the Department of Transportation's Commercial Driver's License Information System (CDLIS) will likely be the model used for REAL ID. CDLIS allows information on licensed commercial drivers to be shared between States on a limited basis—commonly referred to as a "pointer system." However, the NPRM does not specify a pointer system will be used for REAL ID, leaving the realization of a de facto national database as a distinct possibility under the regulations.

Given the inevitable incompleteness and inaccuracies of the REAL ID databases, it is shocking to me that the NPRM does not call for a redress system. This is not a function that can be left to the States because REAL ID and the information it relies upon are bigger than the individual States. What happens if one state passes erroneous information about an individual to another state? Chances are there will be cases where both States claim it's the responsibility of the other state to adjudicate the complaint. Where does an individual turn if a state DMV and a federal agency cannot agree on who should correct an incomplete record? DHS needs to mandate a redress process and make it clear where that responsibility lies to ensure errors and oversights are resolved promptly.

Also notably absent from the NPRM is a requirement to encrypt the data held electronically on the actual ID card. Without encryption it will be substantially easier to steal critical personal information, making all Americans more vulnerable to identity theft. Equipment capable of reading the Machine Readable Zone on the back of most drivers' licenses is readily available. If we're going to spend billions of dollars enhancing the security of the rest of the identification system, why leave this gaping hole?

DHS has chosen to pass the responsibility for privacy protection to the States. This is inherently problematic because REAL ID requires States, and more importantly the individual citizen, to provide and share additional personal information in the name of security. Because REAL ID is a federal mandate, the Federal Government has an obligation to ensure the law is implemented appropriately and that information shared under REAL ID is secure. States deserve some flexibility in implementing REAL ID as they are the ones who understand the drivers' licensing process. However, given the security implications of widespread identity theft, the Federal Government cannot remain silent on this issue.

Most troubling is that DHS has elected to hide behind what is not said in the REAL ID Act as a means to avoid addressing privacy. The NPRM States, "DHS has sought to address these privacy concerns within the limits of its authority under the Act. The Act does not include language authorizing DHS to prescribe privacy requirements for state-controlled databases or data exchange necessary to implement the Act." The concept that federal agencies need explicit Congressional authorization to protect Americans' privacy is just plain wrong. In fact, our government is obligated to ensure that programs and regulations do not unduly jeopardize an individual's right to privacy.

Privacy is inherently tied to security. Secretary Chertoff made this argument earlier this month when he told the Northern Virginia Technology Council that "Security and privacy are very much the same type of value. I don't think they're mutually exclusive, they're mutually reinforced." As Secretary Chertoff argued, executed correctly, better standards for drivers' license issuance will strengthen privacy safeguards and help prevent identity theft. However, we must remember that if this process is executed poorly, it will have the opposite effect.

Finally, it should be noted that States across the country are moving to opt out of REAL ID. Because of the program's structure, it is only as strong as its weakest

member. If we create a system so onerous that it precludes full participation, any security benefit is lost.

While I regret the repeal of the common sense provisions in the Intelligence Reform Act, which I believe has made identification security much more difficult, I am committed to ensuring this job is done right. We must find a way to make the driver's license a trusted document, and the road the Department is now on is not the way. Secure identification is at the very heart of our homeland security. I strongly encourage the Department to consider the concerns expressed by Congress and others in formulation of the regulations. And I look forward to working with Chairman Akaka, Senator Collins, the Department of Homeland Security, and others to solve this critical and complex problem.

PREPARED STATEMENT OF SENATOR SUNUNU

Nearly 2 years ago, the REAL ID Act was inserted into an emergency spending bill without holding a single hearing or a substantive debate on the Senate floor. At that time, a number of my Senate colleagues and I sent a letter to then Senate Majority Leader Bill Frist voicing strong opposition to its inclusion. It was and still is my position this legislation was too significant to be included as an extraneous "rider" on a spending bill and it needed to be debated before the Senate over a period of several weeks. For that reason, I commend Senator Akaka for convening this Subcommittee hearing—albeit 2 years too late—to review the REAL ID Act and to carefully consider ways to improve the security and eligibility standards for drivers' licenses in a manner that does not require a National ID or federal data base to track all drivers.

This Committee appropriately and completely addressed the concerns first outlined by the 9/11 Commission's report to Congress regarding terrorists use of falsely obtained forms of identification to access sensitive security areas. The Commission recommended, "The Federal Government should set standards for the issuance of sources of identification, such as drivers' licenses." (pg. 390) During the summer and fall of 2004, I worked with many of the current members of this committee to craft and pass legislation that included a collaborative process for developing minimum standards for drivers' licenses, such as name, address, phone and signature. This bipartisan legislation—The Intelligence Reform and Terrorist Prevention Act of 2004 (IRTPA)—subsequently passed both Houses of Congress and was signed into law by President Bush in December of 2004.

The IRTPA was mindful of States' rights through the inclusion of governors, State legislators and motor vehicle administrators in the negotiated rulemaking process. Equally important, it avoided the creation of a national ID, massive databases and billions of dollars in unfunded mandates. As we all know, this common-sense solution to a legitimate problem was eliminated and replaced by an unnecessary, unfunded, and unlikely to make you safer federal mandate: REAL ID.

States understand this and have started to take action. Across the country, State Legislatures are introducing, debating and, in some cases, passing legislation outlawing the Federal Government implementing REAL ID. In this instance, the Senate needs to follow the example being set by the States.

Most recently, the Department of Homeland Security (DHS) released a notice of proposed rulemaking. Included in these regulations is an agreement to give States a 2 year extension to implement new standards, as well as, the understanding that DHS will bring States, technology experts, and privacy advocates back to the table to ensure these standards are crafted in a way that respects States' rights and minimizes costs. It is important to note this would not have been possible without the efforts of Senator Collins and others who recognize the unreasonable burden REAL ID places on the States. Although this agreement is far superior to immediate implementation of REAL ID, more must be done to protect taxpayers, States' rights, and the privacy of all Americans.

That is why Senator Akaka and I have reintroduced the "Identification Security Enhancement Act." Our legislation would repeal Title II of the REAL ID Act and replace it with the negotiated rulemaking process originally passed as part of the Intelligence Reform and Terrorist Prevention Act of 2004. These provisions would enhance privacy protections by ensuring procedures and requirements are in place to protect civil liberties, as well as, privacy and constitutional rights. I look forward to continuing my efforts to combat this unnecessary, unfunded mandate with Senator Akaka and my fellow colleagues on the Homeland Security and Government Affairs Committee.

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.

System Connectivity by State – March 2007

Jurisdiction	CDLIS & NDR license checks	SSOLV (SSN)	SAVE (lawful presence)	EVVE (Birth certificate)	DOS (Passport)
Alabama	✓	✓	✓		
Alaska	✓	✓			
Arizona	✓	✓			
Arkansas	✓	✓	✓		
California	✓	✓	✓		
Colorado	✓	✓	✓		
Connecticut	✓	✓			
Delaware	✓	✓			
District of Columbia	✓	✓			
Florida	✓	✓	✓		
Georgia	✓	✓	✓		
Hawaii	✓	✓		✓	
Idaho	✓	✓	✓		
Illinois	✓	✓	✓		
Indiana	✓	✓	✓		
Iowa	✓	✓		✓	
Kansas	✓	✓			
Kentucky	✓	✓			
Louisiana	✓	✓			
Maine	✓	✓			
Maryland	✓	✓	✓		
Massachusetts	✓	✓			
Michigan	✓	✓			
Minnesota	✓			✓	
Mississippi	✓	✓			
Missouri	✓	✓	✓	✓	
Montana	✓	✓		✓	
Nebraska	✓	✓			
Nevada	✓	✓	✓		
New Hampshire	✓	✓			
New Jersey	✓	✓	✓		
New Mexico	✓	✓			
New York	✓	✓	✓		
North Carolina	✓	✓			
North Dakota	✓	✓	✓	✓	
Ohio	✓	✓			
Oklahoma	✓				
Oregon	✓	✓			
Pennsylvania	✓	✓	✓		
Rhode Island	✓	✓			
South Carolina	✓	✓			
South Dakota	✓	✓	✓	✓	
Tennessee	✓	✓			
Texas	✓	✓			
Utah	✓	✓			
Vermont	✓	✓	✓		
Virginia	✓	✓	✓		
Washington	✓	✓			
West Virginia	✓	✓			
Wisconsin	✓	✓			
Wyoming	✓	✓	✓		

NATIONAL CONFERENCE *of* STATE LEGISLATURES

The Forum for America's Ideas

TESTIMONY OF

SENATOR LETICIA VAN DE PUTTE
TEXAS LEGISLATURE

ON BEHALF OF THE

NATIONAL CONFERENCE OF STATE LEGISLATURES

REGARDING

Understanding the Realities of Real ID:
A Review of Efforts to Secure Drivers' Licenses and Identification Cards

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT OF GOVERNMENT MANAGEMENT, THE FEDERAL WORKFORCE, AND THE DISTRICT OF COLUMBIA,
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS,
UNITED STATES SENATE

MARCH 26, 2007

444 North Capitol Street, N.W., Suite 515, Washington, D.C. 20001
Tel: 202-624-5400 | Fax: 202-737-1069

Testimony of Senator Leticia Van de Putte
March 26, 2007

Chairman Akaka, Ranking Member Voinovich and distinguished members of the Senate Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, I am Leticia Van de Putte, President of the National Conference of State Legislatures (NCSL) and a member of the Texas State Senate. I appear before you today on behalf of NCSL, a bi-partisan organization representing the 50 state legislatures and the legislatures of our nation's commonwealths, territories, possessions and the District of Columbia.

Mr. Chairman, I would like to take this opportunity to thank you for your leadership on this important issue, not just today with this hearing, but with your introduction of legislation in both the 109th and 110th Congresses to fix the Real ID Act. It is imperative that this hearing be the first step in a process that takes us down the road to successful, cost-effective implementation of the act. Legislators across the country share the goal of improving the integrity and security of driver's licenses and identification cards. We want to make sure it is done right. In order to do this, we need the necessary systems, time, flexibility and funds.

Mr. Chairman, as you know, NCSL will call for the repeal of the act if the recommendations made in the September 2006 report—*The Real ID Act: National Impact Analysis,* issued by NCSL, the National Governors Association and the American Association of Motor Vehicle Administrators—are not implemented and the mandate fully funded by December 31, 2007. Mr. Chairman, I request that a copy of this report and the NCSL policy—*Funds in the FY 2008 Budget Resolution for Implementation of the Real ID*—be submitted for the record to accompany my testimony.

NCSL would like to acknowledge that the draft regulations released earlier this month by the Department of Homeland Security (DHS) incorporate a number of recommendations for implementation made in the September 2006 report. For example, the draft regulations provide states important flexibility through the self-certification process. They allow states to develop waiver and exceptions processes, define which categories of department of motor vehicle (DMV) employees are subject to background checks, and potentially determine the physical security requirements of the DMV facilities. We hope that the final regulations maintain this flexibility.

The draft regulations, however, do not address several of the major recommendations—or, more accurately, solutions—that serve to ensure successful, cost-effective implementation of the act. These solutions would:

- Ensure that verification systems are available nationally;
- Allow states to adopt up to a 10-year progressive reenrollment process;
- Exempt certain populations from the Real ID process; and
- Provide the necessary federal funds.

Solution 1: Verification Systems Must be Available on a National Level

The draft regulations contemplate that states will need to have access to at least five national databases in order to electronically verify the validity of required identification documents. However, it appears that a number of these systems will still not be available nationally by the May 11, 2008 deadline. For example, it was recently reported that because $3 million was not made available by January 2007, the Electronic Verification and Vital Events (EVVE) system will not be ready for all 50 states to electronically verify birth certificates by the May 11, 2008 deadline (CQ Homeland Security, March 15, 2007).

It is critical that states not be required to electronically verify the validity of identification documents with the issuing agency until the necessary verification systems have been developed, tested and made available nationwide. Although the draft regulations provide states the necessary flexibility to adapt should certain systems not be available by the May 11, 2008 deadline, successful implementation of the act, within such a limited timeframe, depends on the availability of all the systems.

I do not believe it would be in line with the spirit of the law for states to begin issuing Real ID compliant cards without actually having electronically verified the validity of the identity documents an individual presents. We will have spent billions of dollars to have a "pretty" new card, but will have done nothing to actually improve identity security.

Because it is unlikely that a number of the systems will be available nationally by May 11, 2008, it is critical that the May 11, 2008 deadline be moved for all states to a future date when the verification systems are available on a national level.

Solution 2: 10-year Progressive Reenrollment Process

The final regulations or legislative modifications need to allow states to adopt up to a 10-year progressive reenrollment process.

Under the draft regulations, states will need to reenroll 245 million driver's licenses and identification cards by 2013. According to the NCSL, NGA and AAMVA document I referenced earlier, a five-year reenrollment period would cost states at least $8.4 billion. This is due to the fact that all 245 million existing card holders will have to return in person to their DMV as if they were first time applicants, thereby increasing transaction times. In addition, under the draft regulations, states that receive an extension of the May 11, 2008 deadline could have less than 3.5 years to reenroll their existing cards, which would increase the cost even further in those states.

A 10-year progressive reenrollment process would provide states the ability to manage enrollment over a greater length of time, meet the objectives of the act, reduce the fiscal effect on states and minimize service disruptions for customers. It also would allow states to make the necessary modifications to any identified impediments that may result from the requirements.

Because 24 states currently have a renewal period longer than five years, extending the reenrollment period beyond the proposed five-year period would negate some costs related to expanding capacity and allow the remaining cost to be spread over a longer period of time. States could allow for alternative renewal processes to continue during the re-enrollment period, provided that certain existing customer data could be validated before issuance.

Solution 3: Exempt Certain Populations from the Real ID Requirements

Another way to reduce the operational and financial burden of the act is to reduce the population subject to the Real ID Act requirements. NCSL believes that certain segments of applicants should be exempt from the Real ID process. This exemption could be based on certain requirements related to applicable risks such as year of birth or duration of continuous relationship with the state of licensure.

For example, if I have an 82-year-old neighbor who has lived in Texas her entire life, the DMV should be able to use its current issuance and renewal process and send her a compliant license when her driver's license comes up for renewal. Although the draft regulations provide states some flexibility in verifying the identity documents of individuals born before 1935, they do not exempt them from other aspects of the act. Under the draft regulations, my 82-year-old neighbor would still have to visit her local DMV. Is this really necessary?

In addition, the final regulations should waive the verification requirements for applicants who already have been through an identity verification process conducted by the federal government, such as individuals with military IDs, U.S. passports, Transportation Worker Identification Credentials, or certain federal employee identification cards. If an individual can walk out of a DMV and get on a plane with an identification card issued by the federal government, shouldn't that be enough for a state to issue a Real ID compliant license or identification card to an individual?

Solution 4: Provide the Necessary Federal Funds

Federal funds must be provided immediately for successful implementation of the Real ID. Whether one uses the NCSL, NGA and AAMVA state implementation cost of $11 billion over five years or the DHS state implementation cost figure of $10 billion to $14 billion over 10 years, the Real ID is an enormous unfunded mandate. For Texas, the startup costs have been estimated at $142.6 million, with ongoing annual operational expenses of $67 million.

NCSL is concerned that Congress and the administration to date have provided only $40 million for state implementation; that was in FY 2006. NCSL is even more concerned that the FY 2008 Senate Budget Resolution fails to provide funds for state implementation of the Real ID. It is critical that new federal funds—and I emphasize new—be provided for state implementation of the Real ID. States should not be required to use current and diminishing State Homeland Security Grant Program funds. This grant program already has been reduced from more than $1 billion to $525 million over the past two years. Under the President's FY 2008 budget, it would be further reduced to $187 million.

The final regulations should prohibit federal agencies from charging states transaction fees for accessing the required electronic verification systems. This also should apply to state use of the necessary Federal Bureau of Investigate databases to conduct background checks on DMV employees.

NCSL recommends instituting a legislative trigger that would automatically release states from complying with any Real ID provision in any fiscal year in which the Congress fails to appropriate funds for these purposes.

Mr. Chairman, in closing I would like to add that NCSL remains steadfast in its resolve to work with federal policymakers to fix, fund and implement the Real ID Act before December 31, 2007, as stated in our policy. I encourage you to consider legislative action to ensure that the solutions I have proposed today are implemented expeditiously. This will provide states the necessary certainty to move forward in implementing the act. NCSL is encouraged that you and other federal lawmakers have recognized the difficulties states face, and we look forward to working with you on this important issue.

I thank you for this opportunity to testify and look forward to questions from members of the subcommittee.

NATIONAL CONFERENCE *of* STATE LEGISLATURES

The Forum for America's Ideas

FUNDS IN THE FY 2008 BUDGET RESOLUTION FOR IMPLEMENTATION OF THE REAL ID

NCSL Executive Committee Task Force on Homeland Security and Emergency Preparedness

NCSL Standing Committee on Budgets and Revenue

WHEREAS, on May 11, 2005, the REAL ID Act (act) was enacted as part of supplemental spending bill (P.L. 109-13); and

WHEREAS, under the act, a state must implement new federal standards for the issuance of drivers licenses (DL) and identification cards (ID) by May 11, 2008 or the federal government will not recognize the state's DL/ID for federal purposes; and

WHEREAS, under the act, states must have access to five national identity document verification systems, of which only one is operational; and

WHEREAS, a comprehensive analysis of the act conducted by the National Conference of State Legislatures (NCSL), National Governors Association and the American Association of Motor Vehicle Administrators determined implementation of the act would cost states more than $11 billion over its first five years of implementation; and

WHEREAS, the same study concluded states face a one-time, up front cost of $1 billion;

WHEREAS, the deadline for the implementation of the act is rapidly approaching; and

WHEREAS, Congress and the Administration have failed to provide adequate funds to implement the act; and

BE IT RESOLVED, that NCSL requests the President to include $1 billion in his FY 2008 Budget for one-time, up front costs to states to implement the Real ID; and

BE IT FURTHER RESOLVED, that NCSL requests Congress to include $1 billion in the FY 2008 Budget Resolution for one-time, up front costs to states to implement the Real ID;

BE IT FURTHER RESOLVED, that NCSL requests the President and Congress to fully fund the federal government's obligations under the act to develop various document verifications systems for states in the President's FY2008 Budget Resolution.

BE IT FURTHER RESOLVED, that NCSL requests Congress to adopt the necessary changes to the Real ID as outlined in the September 2006 report—The Real ID Act: National Impact Analysis—issued by NCSL, the National Governors Association and the American Association of Motor Vehicle Administrators;

BE IT FURTHER RESOLVED, that if, by December 31, 2007, Congress does not provide at least $1 billion in federal FY 2008 for one-time, up front costs to states to implement the Real ID and adopt the necessary changes to the Real ID as outlined in the September 2006 report—The Real ID Act: National Impact Analysis— then NCSL requests that Congress repeal the Real ID Act.

BE IT FURTHER RESOLVED, that a copy of this resolution be sent to the President of the United States and to all the members of Congress.

Expires August 2007

OFFICE OF THE MAYOR
CITY AND COUNTY OF HONOLULU
530 SOUTH KING STREET, ROOM 300 • HONOLULU, HAWAII 96813
TELEPHONE (808) 523-4141 • FAX (808) 527-5552 • INTERNET: www.honolulu.gov

MUFI HANNEMANN
MAYOR

Statement of

Mufi Hannemann
Mayor of Honolulu
State of Hawaii

before the

Subcommittee on Oversight of Government Management,
the Federal Workforce, and the District of Columbia
Committee on Homeland Security and Governmental Affairs
United States Senate

March 26, 2007

Good afternoon, Chairman Akaka, Ranking Member Voinovich, and Senators:

Thank you for the opportunity to testify on the impact of the REAL ID Act on the City and County of Honolulu.

My name is Mufi Hannemann and I am mayor of the City and County of Honolulu. I am pleased to introduce Dennis Kamimura, who is our licensing administrator and the person responsible for overseeing our driver licensing program.

Although the City and County of Honolulu is only one of Hawaii's four counties that will be impacted by the provisions of the REAL ID Act, Honolulu issues licenses to 70 percent of the 867,000 drivers in the State of Hawaii. Moreover, all of the state's driver license computer records are stored in Honolulu's computer system.

We wholeheartedly agree that the tragic events of September 11 require the strengthening of the security, standards, procedures, and requirements for the issuance of driver licenses and identification cards, but we have several major concerns with the implementation of this law, as proposed in the Notice of Proposed Rulemaking that was released by the Department of Homeland Security.

Funding

Our first concern is funding. We estimate that the one-time cost to implement this system will be $7.67 million and the ongoing expenses will total $17.88 million during the first five years of the program. About 90 percent of this $25.55-million expense will be incurred by the City and County of Honolulu. Although the Department of Homeland Security announced that 20 percent of the state's Homeland Security Grant Program funds will be made available during the 2007 grant cycle, most of these funds have already been dedicated. We ask that these costs be borne by the federal government.

Verification Process

The act requires that we refuse to issue a driver license or identification card to a person holding a license or card issued by another jurisdiction. This is similar to a provision of the Commercial Motor Vehicle Safety Act, which requires commercial drivers to have one and only one license at any given time. This requirement is supported by the Commercial Driver's License Information System (CDLIS), which has been operating in all 50 states and the District of Columbia since 1992.

CDLIS consists of a central site and nodes in each jurisdiction. Access to CDLIS is provided through a secure private network operated by the American Association of Motor Vehicle Administrators (AAMVA) and *cannot* be accessed through the public Internet. Each site connected to the private network has its access controlled by several security mechanisms. Neither the State of Hawaii nor the AAMVA is aware of any privacy breaches of CDLIS since it went into development in 1989.

On August 10, 2005, Congress passed the transportation reauthorization bill, the Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU), and authorized $28 million to modernize CDLIS. We recommend leveraging this project and its federal funding to expand the scope of the CDLIS modernization effort to support an all-driver pointer system for non-commercial driver license and identification cards. Inasmuch as all jurisdictions are familiar with the CDLIS program and the all-driver pointer system would use the same principles as CDLIS, use of this technology would be more efficient than expending public money to create a new system.

The act also requires us to verify, with the issuing agency, the validity of identification documents an applicant presents. The act would require us to have access to five additional national databases:

- Social Security On-Line Verification system (SSOLV) for Social Security cards;

- Department of State for passport and consular report of birth abroad;
- Electronic Verification and Vital Events (EVVE) for birth and marriage certificates;
- Systematic Alien Verification for Entitlements (SAVE) for permanent resident status (I-551), employment authorization (I-766), or U.S. certificate of citizenship or naturalization; and
- Student and Exchange Visitor Information System (SEVIS) to verify the duration of lawful status for student aliens.

At present, almost all jurisdictions are using the SSOLV, which requires enhancements due to its unreliability. Several states are using SAVE but that system requires major improvements to ensure appropriate functionality to operate in real time and with accessibility and reliability. Several states are testing EVVE; however, the system will not be fully operational until December 2009. There is no electronic accessibility to SEVIS and or the Department of State database. We should not be required to use systems that are unreliable or under development. These systems should be developed and tested before placing the burden on local jurisdictions and the public that we serve. Additionally, we believe that federal agencies operating these systems should be prohibited from charging jurisdictions transaction fees that only increase our operating costs.

Reenrollment

The proposed rules require that all licensed drivers and individuals issued identification cards be reenrolled within five years. The majority of our licensed drivers and those issued state identification cards have a six-year expiration period. We will face increased costs and tremendous public inconvenience to meet this shortened re-enrollment period. We recommend that the period be at least seven years.

Waiver

To facilitate the processing of all applicants, we recommend that applicants who are 72 years or older be granted waivers from the verification requirements of the act. Similarly, individuals who are required to undergo the same or a more stringent verification process for federal identification be granted waivers. Lastly, if an applicant has undergone the verification process in one jurisdiction and has been issued a REAL ID compliant driver license or identification card, the verification process by the gaining jurisdiction should be waived.

Conclusion

Practical considerations aside, the City and County of Honolulu cannot afford to implement the requirements of the act without initial and continuing federal funding. If funding is provided, the time limits for implementation of the program, without the required electronic verification systems, will place an enormous burden on the driver licensing staff and be a tremendous inconvenience to the public. To ensure long-term success, a more realistic implementation plan should be developed with input from the jurisdictions who bear the burden of issuing driver licenses and identification cards.

Thank you for granting me the opportunity to provide our perspective on this issue.

Statement of David Quam
Director, Federal Relations, National Governors Association

Before the Subcommittee on Oversight of Government Management, the Federal Workforce and the District of Columbia, Committee on Homeland Security and Governmental Affairs

United States Senate

Understanding the Realities of Real ID: A Review of Efforts to Secure Drivers' Licenses and Identification Cards
March 26, 2007

Chairman Akaka, Ranking Member Voinovich and distinguished members of the subcommittee, my name is David Quam and I am the director of federal relations for the National Governors Association (NGA). I appreciate the opportunity to appear before you today on behalf of NGA to discuss the issues surrounding implementation of Real ID.

Congress passed the Real ID Act (Real ID) as part of the Emergency Supplemental Appropriations for Defense, the Global War on Terror, and Tsunami Relief Act (P.L. 109-13). The law replaced section 7212 of the Intelligence Reform Act (P.L. 108-458), which established a negotiated rule making to determine national standards for state driver's license and identification cards (DL/IDs). NGA supported the compromise contained in section 7212 because it allowed stakeholders, including governors, to participate in the process of reforming what traditionally has been a state function.

Although the negotiated rulemaking already had begun, Real ID repealed the provision and replaced it with statutory standards, procedures and requirements that must be met if state-issued DL/IDs are to be accepted as valid identification by the federal government. Real ID's mandates will alter long-standing state laws, regulations and practices governing the qualifications for and the production and issuance of DL/IDs in every state. Complying with these new standards will require significant investments by states and the federal government and test the resolve of citizens who will be directly affected by changes to state systems.

To ensure states, Congress and the federal government understand the fiscal and operational impact of altering these complex and vital state systems, the American Association of Motor Vehicle Administrators (AAMVA), in conjunction with NGA and the National Conference of State Legislatures (NCSL), conducted a nationwide

survey of state motor vehicle agencies (DMVs). Based on the survey results NGA, NCSL and AAMVA issued a report in September 2006 concluding that Real ID will cost states more than $11 billion over five years, have a major effect on services to the public and impose unrealistic burdens on states to comply with the act by the statute's May 2008 deadline. The report also identified key components of Real ID that will have the greatest impact on states and citizens and made specific recommendations for Congress and the Department of Homeland Security (DHS) to follow if Real ID is to succeed. A copy of the report can be found on the NGA website at www.nga.org/Files/pdf/0609REALID.PDF.

Challenges presented by Real ID

DHS formally published its notice of proposed rulemaking on Real ID on March 9, 2007. NGA and state stakeholders are closely reviewing the regulations and intend to participate actively in the rulemaking process. An initial review of the regulations suggests that while DHS incorporated several of the recommendations made by states, four requirements continue to present critical challenges for states: 1) the need to re-enroll all 245 million DL/ID holders over five years; 2) increased verification requirements for identification documents; 3) new document design mandates; and 4) changes to business and support practices that reduce efficiencies and customer service.

1. Five-year re-enrollment. States estimate the cost of re-enrolling all 245 million DL/ID holders into a Real ID system over five years will exceed $8.4 billion. This standard will require an in-person visit by every current DL/ID holder, as well as new applicants, to review and verify all required identification documents and re-document information for the new license, including place of principal residence, new photographs and new signatures. Efficiencies from alternative renewal processes such as Internet and mail will be lost during the re-enrollment period, and states will face increased costs from the need to hire more employees and expand business hours to meet the five year re-enrollment deadline.

2. Enhanced verification. Real ID supplants traditional DMV vetting processes by requiring states to verify each identification document independently with its issuing agency. While the act contemplates the use of five national electronic systems to facilitate verification, currently only one of these systems is available on a nationwide basis. System development, programming, testing and training will require considerable time and resources that far exceed the deadlines or funds provided by the act or Congress.

3. Document design requirements. The act calls for states to incorporate certain information and security features into DL/ID cards. Although most states have

incorporated security features into their card designs, the proposed regulations call for adoption of certain mandatory security features along with establishing a performance standard based on adversarial testing. While preferable to a strict technology mandate, depending on the technology chosen, such a requirement could dictate DMV business practices by effectively requiring DMVs to move away from over-the-counter issuance systems and toward central issuance systems.

4. New business practices. Real ID will reduce efficiencies and increase wait times for citizens. To comply with the requirement that all DL/ID card holders re-verify their identity with the state, individuals must gather and present all their identification documents, which may more than double the length of time they spend at DMVs. Real ID also will effectively reverse state practices designed to ease an applicant's interaction with motor vehicle agencies (e.g., Internet, mail in renewal, over-the-counter issuance).

Recommendations for Congress

Governors are committed to improving the security and integrity of state DL/ID systems, but the timelines and requirements mandated by Real ID and the proposed regulations remain unrealistic. In order to meet the objectives of the act, Congress and DHS should incorporate state recommendations to ensure the regulations and the statute provide adequate time for implementation, workable verification standards that use available technology, recognition of state innovations that meet the objectives of the act and adequate federal funding to implement the law's mandates.

1. Provide adequate time. There is widespread recognition that it will be impossible for states to comply with Real ID by the statutory deadline of May 2008. DHS has proposed granting states five years to enroll all citizens in a Real ID system, and allowing states to request extensions of the deadline by which states must begin issuing Real ID compliant documents. As mentioned above, re-enrollment of the population is a major logistical and financial obstacle for states. While the possibility of an extension on the start date is necessary – especially given the late release of the proposed regulations – failure to extend the end-date for enrollment correspondingly only will serve to maximize costs and hardships on states and citizens.

It also is impracticable for states to issue all 245 million DL/IDs in five years. The proposed regulations call for all applicants for new or renewed DL/IDs to present their original identification credentials in person by 2013. The 24 states with existing renewal periods greater than five years will need to accelerate their renewal process to meet the new timeline and motor vehicle offices will need to process an additional 30 million individuals during that time. The net effect will be an increase in DMV

workloads of 132 percent and a doubling of transaction times for renewals of licenses and identification cards.

Mandating that states re-enroll their entire population in a short time frame maximizes costs and minimizes the likelihood of successful implementation. Congress should alter the deadlines of Real ID to statutorily set the later of December 31, 2009 or the date two years after the publication of final regulations to begin issuing Real ID compliant DL/IDs; grant states a 10 year window in which to complete re-enrollment of all state DL/ID holders; and provide states with statutory flexibility to manage the re-enrollment process, including the ability to delay re-verifying certain populations and rely on certain federal identification documents as proof of verification.

2. Allow for transition to electronic verification. In its proposed regulations, DHS emphasizes that for states "to verify information and documentation provided by applicants, ***each state must have electronic access to multiple databases and systems…Secure and timely access to trusted data sources is a prerequisite for effective verification of applicant data.***" (Emphasis added.)

The proposed regulations identify five systems that will be required to make Real ID work: Social Security On-Line Verification (SSOLV), Electronic Verification of Vital Events Records (EVVER), Systematic Alien Verification for Entitlements (SAVE), an all-drivers system run by the states to ensure an applicant is not licensed in another state and system run by the U.S. State Department to verify foreign passport information. Only SSOLV is fully operational on a national basis and even it will require enhancements to handle the volume anticipated under Real ID. The other systems are either not widely used, in the developmental or pilot phase, or do not exist.

Given the critical nature and uncertain availability of these systems, Congress should amend Real ID to specifically allow states to use existing verification practices until all necessary federal and state systems are fully operational and deployed.

3. Encourage state innovation. Several states have updated their systems to meet objectives similar to those of Real ID. The proposed regulations suggest DHS will rely heavily on state certification – an early recommendation of the states – as a major component for verifying state compliance with the act. What remains undeveloped is clear guidance as to what will be required of states and what milestones or standards DHS will set for certification. While the Secretary has shown a willingness to allow states to request a delay in issuing Real ID compliant documents, the lack of a similar extension to the 2013 end date, and the proposed requirement that all states submit a certification package by February 10, 2008, including "milestones, schedules, and

estimated resources needed to meet all the requirements of the rule," suggests a lack of appreciation for the time required to transform these complex state systems.

Congress should assist states with implementation of Real ID by urging the Secretary to work in close consultation with states to expedite development of certification guidelines, establish a date for submission of state plans that is at least one year after publication of final regulations; and use his authority to offer extensions to states actively working to meet the objectives of the act.

4. Provide sufficient funding. State estimates place the projected cost of Real ID at more than $11 billion over the first five years, including $1 billion in up-front costs to create the systems and processes necessary to implement the law and re-enroll all 245 million DL/ID holders. The proposed regulations verify state projections. According to DHS, the total cost of Real ID will exceed $23 billion over 10 years with more than 63 percent of the total cost being borne by states. These projected costs far exceed the Congressional Budget Office estimate of $100 million or the $40 million appropriated by Congress in 2005. Real ID is an unfunded federal mandate that violates the intent of the Unfunded Mandates Reform Act and should be paid for with federal dollars.

Congress should provide a specific authorization of funds to cover the costs of Real ID over the next 10 years and appropriate at least $1 billion in fiscal year 2008 to fund the initial costs of implementing Real ID.

Conclusion

Mr. Chairman, the nation's governors want to work with Congress and DHS to enhance the security of state DL/ID systems. We all learned a bitter lesson on September 11th, one no one wants to repeat. States responded to those tragic events by beginning to improve their systems and increase the security surrounding their DL/ID process. Governors supported the reforms contained in the Intelligence Reform Act because they are dedicated to the safety and security of their citizens. Unfortunately, Real ID, in its current form, is unworkable. If the law is to serve its intended purpose, DHS should adopt final regulations and Congress should pass legislation and appropriate funds that are consistent with state recommendations. Only by working together will state and federal governments succeed in meeting the challenges presented by Real ID and making our driver's license and identification systems more secure.

WASHINGTON
LEGISLATIVE OFFICE

Testimony of Timothy D. Sparapani
Legislative Counsel

American Civil Liberties Union

AMERICAN CIVIL
LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544 1681
F/202.546 0738
WWW.ACLU.ORG

Caroline Fredrickson
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL
NEW YORK, NY 10004-2400
212 549 2500

OFFICERS AND DIRECTORS
NADINE STROSSEN
PRESIDENT

ANTHONY D ROMERO
EXECUTIVE DIRECTOR

RICHARD ZACKS
TREASURER

The Real ID Act: An Unprecedented Threat to Privacy and Constitutional Rights

U.S. Senate Committee on Homeland Security and Government Affairs
Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia

Hearing Regarding Understanding the Realities of REAL ID: A Review of Efforts to Secure Driver's Licenses and Identification Cards

March 26, 2007
342 Dirksen Senate Office Building

Subcommittee Chairman Akaka, Ranking Member Voinovich, and Subcommittee Members, on behalf of the American Civil Liberties Union ("ACLU"), America's oldest and largest civil liberties union, its 53 affiliates and hundreds of thousands of members, we recommend that this Subcommittee mark up legislation, such as S. 717, the Identification Security Enhancement Act of 2007, to replace Title II of the unworkable, Real ID Act of 2005, Pub. L. 109-13 (hereinafter "Real ID Act" or "Act".

As we approach the two-year anniversary of the Act's enactment on May 11, 2005, and rapidly approach the end of the statutorily mandated three-year-long period given to states to implement the Act, one thing has become clear – states and the public are moving en masse to reject the Real ID Act and calling for Congress to repeal it in toto. Diverse organizations such as the American Association of Retired Persons ("AARP"),[1] the National Network to End Domestic Violence, and firearms owners and enthusiasts, have called for a repeal of the unworkable Real ID Act. In response, state governments are rapidly moving to opt out of this unfunded mandate altogether.

The impending deadline and recent action by the Department of Homeland Security ("DHS") have made three things abundantly clear.

- First, the minor delay offered to states is not sufficient; states will never be able to implement the Act within the timeline provided.
- Second, the entire Real ID Act scheme is collapsing as states recognize the unprecedented burdens on taxpayers' privacy and civil liberties imposed by this unfunded mandate, and as states – such as Maine and Idaho – opt out of participation.
- Third, Congress cannot sit idly by. Rather, Congress must repeal this Act and, if need be, replace it with a workable, achievable statute to improve licensing security devoid of the privacy and civil liberties infirmities that hamstring the Real ID Act, and which is agreed upon by all interested stakeholders.

This testimony will discuss each of these three realizations briefly. Further, it will elaborate on the four types of privacy concerns raised by the Act and the regulations promulgated by DHS to implement the Act, which are concerns regarding:

(i) data on the face of the ID card;
(ii) data in the machine readable zone on the back of the ID card;
(iii) data in the interlinked national ID database supporting the cards; and,
(iv) transmissions of data between users of the data.

Finally, this testimony will identify how the Real ID Act and the regulations promulgated to respond to it[2] suffer from Constitutional infirmities that are intrinsic to the poorly drafted Real ID Act. Specifically, this testimony will briefly discuss how the Real ID Act potentially implicates (i) four separate First Amendment rights; (ii) gun owners' privacy rights, (iii) could cause derivative problems to citizens' Sixth Amendment rights; and

[1] Letter from AARP to Sen. Richard Shelby Apr. 20, 2006, at pp. 4. "We believe that the implementation of the Real ID Act will – if left unmodified – generally make consumers more vulnerable to ID theft."
[2] Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 72 Fed. Reg. 10821 (proposed Mar. 8, 2007).

(iv) threatens Due Process Clause rights in multiple ways. Any of these Constitutional infirmities could cause the Act and/or regulations to be struck down by a court in whole or in part.

For further information, attached to my written testimony is the ACLU's "Real ID Scorecard," in which we systematically analyze the regulations on an issue-by-issue basis. The Scorecard demonstrates that DHS has utterly failed to protect privacy and security. ACLU Real ID Scorecard, available at http://www.realnightmare.org/images/File/Real%20ID%20Scorecard%20-%20Fed%20Reg%20page%20numbers.pdf.

I. ACLU Recommendations: Replace Real ID by Enacting S. 717

Congress must take rapid action to respond to the outcry from the states and citizens. **The ACLU recommends that:**

- **(i) Congress repeal Title II of the Real ID Act, and, enact legislation, such as S. 717, authored by Senator Akaka (D-HI), and co-sponsored by Senators Sununu (R-NH), Leahy (D-VT), and Tester (D-MT), which reestablishes a more sensible and workable process for improving state issued drivers licenses.**
- **(ii) Members of Congress submit comments calling on the Department of Homeland Security ("DHS") to withdraw its Notice of Proposed Rulemaking, published at 72 Fed. Reg. 10819;**
- **(iii) Congress refrain from appropriating any additional funds that could be used to implement the Real ID Act as it is currently constituted.**

Following these recommendations would ensure that Congress leads the states to implement commonsense proposals to more rapidly produce counter- and tamper-resistant licenses. Further, following these recommendations would lead to improved security for the data maintained by departments of motor vehicle administration ("DMVs"). Additionally, these recommendations would allow DMVs to make improvements at a fraction of the DHS-estimated cost of implementing the Real ID Act. More importantly, this recommended course of action would eliminate the constitutional infirmities that will either delay or block implementation of Real ID in whole or in part.

II. The Deadline for Real ID Implementation Will Not be Met

Congress will need to revisit the Real ID Act during the 110th Congress if for no other reason than that no state will likely actually meet the Real ID's statutorily prescribed deadline for implementation. Further, it is likely that the vast majority of states will also be unable to meet even the December 31, 2009 delayed deadline contemplated by DHS. DHS' failures to issue proposed regulations in a timely fashion, coupled with state legislative and budgetary cycles, ensure that states cannot be compliant by these deadlines. Compounding this problem is the fact that several data verification systems contemplated in the Act and proposed regulations do not exist. Congress will need to – at the very least – push back the statutory compliance deadline well into the next decade.

DHS delayed promulgating the Notice of Proposed Rulemaking regulations for far too long, waiting nearly 22 months from the date of enactment. Comments are due by May 8, 2007, just three days short of the two-year anniversary of the Act's enactment. After comments are received, DHS will need time to review those comments, make modifications and finalize its proposed regulations. Thus, states will not receive final guidance on how to comply until well into the summer of 2007. DHS has told states they must confirm with DHS by October 2007 whether they will meet compliance deadlines or seek an extension. Yet, states will lack sufficient time to analyze the regulations once finalized to meet even this October deadline.

Further, some state legislatures meet only once every two years and many have short legislative sessions. The delays caused by DHS' tardy publication of the proposed regulations and the subsequent delays required to produce final regulations ensure that many states will not be able to propose and enact legislation to modify state statutory licensing laws in a timely fashion. Once state laws are modified, states will also need to draft and modify regulatory structures as well before they can begin implementation. In short, even a December 31, 2009 deadline for compliance will never be met and Congress needs to revisit the Real ID Act.

III. The Public and States are Rebelling Against the Real ID Act and Calling for its Repeal

Driven equally by the extraordinary threat the Act poses to personal privacy and civil liberties and its prohibitively expensive cost, now anticipated to be at least $23.1 billion according to DHS' own estimate,[3] states are telling Congress that, no matter the consequences they will not participate.[4] Already two states, Maine and Idaho have

---

[3] 72 Fed. Reg. 10845.

[4] See, e.g., the Model Resolution in Opposition to the REAL ID Act adopted by the conservative American Legislative Exchange Council and circulated to hundreds of State Legislators who are Members, which provides that:

WHEREAS, the implementation of the REAL ID Act intrudes upon the states' sovereign power to determine their own policies for identification, licensure and credentialing of individuals residing therein; and

WHEREAS, one page of the 400-page 9/11 Commission report, that did not give consideration to identification issues, prompted Congress to pass the legislation which created the Real ID Act, ignoring states' sovereignty and their right to self governance; and

WHEREAS, the REAL ID Act converts the state driver licensing function into federal law enforcement and national security functions that are outside the purpose and core competency of driver licensing bureaus; and

WHEREAS, the REAL ID Act thus constitutes an unfunded mandate by the federal government to the states; and

WHEREAS, the REAL ID Act requires states to conform their processes of issuing drivers licenses and identification cards to federal standards by May 2008; and

WHEREAS, the study cited below predicts state compliance with the REAL ID Act's provisions will require all of the estimated 245 million current cardholders in the United States to renew their current identity documents in person by producing three or four identity documents, thereby increasing processing time and doubling wait time at licensing centers; and

enacted legislation expressly stating that they will not implement the Real ID Act's mandates. The legislation Maine adopted states in part that the "Maine State Legislature refuses to implement the REAL ID Act and thereby protests the treatment by Congress and the President of the states as agents of the federal government." S.P. 113, 123 Leg. (Me. 2007)] More significantly, just 7 days after DHS issued its Notice of Proposed Rulemaking that begins to set the contours for how states must implement the Act, the Idaho legislature voted to opt out of the Act with legislation stating that "the Idaho Legislature shall enact no legislation nor authorize an appropriation to implement the

---

WHEREAS, identification-based security provides only limited security benefits because it can be avoided by defrauding or corrupting card issuers, and because it gives no protection against people not already known to be planning or committing wrongful acts; and

WHEREAS, the REAL ID Act will cost the states over $11 billion to implement according to a recent survey of 47 state licensing authorities conducted by the National Governor's Association, the National Conference of State Legislatures, and the American Association of Motor Vehicle Administrators; and

WHEREAS, the use of identification-based security can not be justified as part of a "layered" security system if the costs of the identification "layer" – in dollars, lost privacy, and lost liberty – is greater than the security identification provides; and

WHEREAS, the "common machine-readable technology" required by the REAL ID Act would convert state-issued drivers' licenses and identification cards into tracking devices, allowing computers to note and record people's whereabouts each time they are identified; and

WHEREAS, a more secure and flexible system of verifying identity may be achieved by less-intrusive means to the individual and to states by employing the free market and private-sector ingenuity; and

WHEREAS, the requirement that states maintain databases of information about their citizens and residents and then share this personal information with all other states will expose every state to the information security weaknesses of every other state and threaten the privacy of every American; and

WHEREAS, the REAL ID Act wrongly coerces states into doing the federal government's bidding by threatening to refuse non-complying states' citizens the privileges and immunities enjoyed by other states' citizens; and

WHEREAS, the REAL ID Act threatens the privacy and liberty of those individuals belonging to unpopular or minority groups, including racial and cultural organizations, firearm owners and collectors, faith-based and religious affiliates, political parties, and social movements; and

WHEREAS, the REAL ID Act thus imposes a national identification system through the states premised upon the threat to national security, but without the benefit of public debate and discourse;

THEREFORE, BE IT RESOLVED that the REAL ID Act is determined by the American Legislative Exchange Council (ALEC) to be in opposition to the Jeffersonian principles of individual liberty, free markets and limited government; and

THEREFORE, BE IT FURTHER RESOLVED that ALEC implores the United States Congress and the U.S. Department of Homeland Security to suspend implementation of the REAL ID Act; and

THEREFORE, BE IT FURTHER RESOLVED that the REAL ID Act should be repealed outright by the United States Congress to avoid the significant problems it currently poses to state sovereignty, individual liberty and limited government.

Adopted by the Homeland Security Task Force at the States and Nation Policy Summit on December 9, 2006. Approved by the ALEC Board of Directors January 8. 2007.

provisions of the REAL ID Act in Idaho, unless such appropriation is used exclusively for the purpose of undertaking a comprehensive analysis of the costs of implementing the REAL ID Act or to mount a constitutional challenge to the act by the state Attorney General." H.J.M. 3, 59th Leg. (Idaho 2007).

The Real ID rebellion in the states is spreading rapidly, and its pace is accelerating. Thirty states have introduced legislation opposing the Real ID Act,[5] and 13states – Arizona, Arkansas, Georgia, Hawaii, Missouri, Montana, New Mexico, Oklahoma, Utah, Vermont, Washington, West Virginia and Wyoming – have had legislation passed by at least one of their legislative bodies. More significantly, many of these states have taken significant legislative action since DHS made public its draft Notice of Proposed Rulemaking on March 1, 2007. **Thus, after reviewing DHS' proposed regulations states immediately moved to reject them.** Since publication of the proposed regulations, legislators in Arkansas, Nevada, Pennsylvania and Texas have introduced anti-Real ID legislation, legislative bodies in Arizona, Arkansas (a different bill from the one introduced the same week), Hawaii, Missouri, Oklahoma, and Washington have passed bills rejecting the Real ID Act, and, as mentioned above, the State of Idaho formally opted out of the Real ID scheme altogether and called on Congress to repeal the Act.

The Real ID Act arguably violates the constitutional principles of federalism by usurping state authority. This usurpation, coupled with federal mandates requiring state employees to effectively serve as federal immigration officers, is compounded by the fact Congress has, to date, only appropriated $6 million of the estimated $23.1 billion cost of compliance. States are refusing to be required to raise the $22,994,000,000 for an Act that imposes substantial, rigid mandates on their licensing systems and their licensees.

Attached is a map showing the tidal wave of activity from coast-to-coast. Status of Anti-Real ID Legislation in the States, available at: http://www.realnightmare.org/news/105/.

IV. Senators Never Voted to Support the Real ID Act and Should Repeal the Act

Today is a noteworthy day. One year, 10 months and 15 days after its enactment into law, the Real ID Act of 2005 is receiving its very first actual consideration by the U.S. Senate. Attached to H.R. 1268, in an extra-procedural manner by its House of Representative sponsor, Rep. James Sensenbrenner (R-WI), the Real ID Act never received a single hearing or any floor debate in the U.S. Senate. Rather than being considered by a Senate Committee or moved for consideration on the Senate Floor as a stand-alone measure, or even as an amendment to an authorizing bill, the Act was attached to the "Emergency Supplemental" appropriations bill providing funding for the

[5] States with pending anti-Real ID legislation (does not include states that have already passed legislation): Arizona, Arkansas, Georgia, Hawaii, Illinois, Kentucky, Maryland, Massachusetts, Michigan, Minnesota, Missouri, Montana, Nebraska, Nevada, New Hampshire, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Texas, Vermont, and Washington.

war effort in Afghanistan and Iraq and humanitarian flood aid for the tsunami victims of southeast Asia. As a consequence, Senators were left with an impossible choice of either opposing emergency funding for troops in an active combat theatre and desperately needed humanitarian assistance, or pass H.R. 1268 with the unrelated Real ID Act attached. Because Senators never considered the Real ID Act, they should be free to vote to repeal it and replace it with a statutory licensing scheme that is both achievable and free of privacy and civil liberties concerns.

V. The Act Raises Unprecedented Privacy and Constitutional Threats and DHS' Proposed Regulations Do Not Resolve these Threats

Even if DHS proposed more complete regulations, which answered all the questions, raised by the Real ID Act that DHS was empowered to consider under the Real ID Act, Congress would still need to revisit Title II of that Act because it is a fatally flawed statute and its flaws cannot be addressed through regulations. Compounding this problem is the substantial failure of DHS to either answer central implementation questions or to mitigate some of the privacy and constitutional concerns. Thus, the regulations fail to resolve the glaring privacy and civil liberties problems created by the Real ID Act.

A) Regulations Proposed by DHS Ignore Substantial Threats to Personal Privacy Posed by Real ID

1) The Act and Regulations Establish the First National ID Card System Eroding Personal Privacy

By enacting the REAL ID Act, Congress set in place the first true National ID Card System. The Act mandates a National ID System by requiring the standardization of state license design and minimum data elements to be collected and stored about each licensee. Thus, although we will continue to have 56 state license issuers with 56 cosmetically different designs, the IDs will essentially be the same. More importantly, the National ID System is created by the mandate that all states make their databases of licensee information interoperable and that they engage in unprecedented data sharing about licensees. Finally, and most importantly, the Real ID licenses will become the de facto National ID as the federal, state and local governments and private sector entities begin to require a Real ID license to exercise rights and privileges and obtain goods and services.

Already, since the Act's passage, Members of Congress have proposed legislation requiring that every adult in America present a Real ID-compliant license to vote, receive authorization to obtain every new job, obtain benefits such as Medicaid, and travel on interstate buses, trains and planes. Thus, if the Act and the regulations are implemented, Senators should expect that no person would be able to function in our society without providing a Real ID-compliant license.

In addition to these burdens from ubiquitous future demands, the machine readable zone on each Real ID license will provide a digital trail everywhere it is read.

The Act, therefore, makes possible the mapping of a person's movements throughout our society and eliminates the anonymity that has protected our privacy since the founding of our country.

2) Privacy Concerns Arising from Data on the ID Card's Face

In addition to the fact that the Act and the Regulations establish the first true National ID Card System, threats to personal privacy caused by the Act and the Regulations arise from four areas:

(i) data on the face of the ID card;
(ii) data in the machine readable zone on the back of the ID card;
(iii) data in the interlinked national ID database supporting the cards; and,
(iv) transmissions of data between users of the data.

Data on the face of the ID card raises substantial privacy concerns. First, it threatens the personal security of numerous classes of licensees by requiring that an individual's principal address be stated on the face of the license. Consequently, police officers, elected officials, and judges will have their home address readily available to all who view their licenses. Address confidentiality laws in dozens of states to protect these government employees are completely overridden by this mandate putting these individuals at risk. Perhaps more importantly, victims of domestic violence and sexual assault who flee their abusers will be stripped of the power to list a Post Office Box as their address on the face of the license. They too will be easier to find by stalkers and abusers.

DHS's proposed solution in its regulations does not resolve this concern adequately. It is unclear how people without such an address or who live in different places – such as students, those who live in recreational vehicles ("RVs") and other mobile homes, and the homeless – will solve this issue. The regulations attempt to address this issue by defining principal address as the place where an individual has his "true, fixed and principal home" (72 Fed. Reg. at 10,851), and stating that DMVs can make exemptions for the homeless (72 Fed. Reg. at 10,803 and 10,836). There is still some concern regarding whether all states will be able and willing to create workable methods for utilizing these exemptions.

Second, Congress failed to prohibit states from noting a licensee's citizenship status on the license. Some have suggested pilot projects to denote citizenship on the face of a license. The ACLU believes that such a "reverse scarlet letter" provision could lead to innumerable discriminatory interactions between police and/or bigoted private citizens and individuals who appear or sound foreign and who do not have such a citizenship sticker on their license every time that license is demanded for presentation. Congress should expressly prohibit any such proposal.

3) Privacy Concerns Arising from Data Contained in the Machine Readable Zone

The Real ID Act created an enormous threat of private sector, third-party skimming and resale of data contained in the "machine readable" zone ("MRZ") on each card. DHS's proposed regulations failed to close the loophole because they do not require encryption of the data in the MRZ.

Because both the type of MRZ and the minimum data elements it must contain are standardized under the Real ID Act, it will become increasingly profitable for private sector retailers to skim a copy of that data from each customer. As states add additional data elements to the machine readable zone, such skimming will become even more valuable. Because the Act does not prohibit skimming, in the near future we can expect retailers to demand that customers produce their licenses for "anti-fraud" or "customer loyalty card" purposes and retailers will routinely retain all the data from the MRZ, combined with a record of each licensee's purchases. The retailers will have two ready markets to profit off such skimming:

(i) using the data to engage in highly-targeted direct marketing back to their customers thereby producing significant amounts of unwanted solicitations, and

(ii) reselling the data to data brokers such as Axciom, ChoicePoint and Lexis-Nexis who will share the information with other companies and federal, state and local governments. The result will be that data brokers and the government will know when and what each customer purchased including items such as the books and magazines we read, what types of birth control we use, and the prescriptions we obtain.

The result will be a substantial erosion of personal privacy.

DHS's proposed regulations failed to close this loophole because they refused to mandate encryption for this data and to place meaningful limits on what data can be harvested from the card and how it can be used. While DHS acknowledges the danger of license data being scanned by third parties, it fails to take action to stop the problem, and merely encourages the states to come up with a solution. DHS says it "leans toward" requiring that data be encrypted but opts not to mandate encryption due to "practical concerns." 72 Fed. Reg. 10819, at 10838. This proposed regulation flies in the face of DHS's own Privacy Office, which believes "there is a strong privacy rationale for cryptographic protections to safeguard the personal information stored digitally in the machine-readable zone (MRZ) on the credentials." Privacy Impact Assessment for the Real ID Act, March 1, 2007, pg. 3. Congress must revisit the Act, if for no other reason, than to expressly mandate encryption of the data provided.[6]

This provision undercuts the Congress' earlier effort to protect driver's information, which considered by many to be of higher quality than commercial data amassed from warranty cards and the like. In 1994 the Congress in response to the

[6] The ACLU believes that any concerns from law enforcement regarding the encryption of data in the MRZ can be overcome by technical means that enable only authorized person to gain access to the encrypted information.

murder of Amy Boyer, by a man who obtained her address from the NH DMV, passed the Drivers' Personal Privacy Act ("DPPA"), Pub. L. 103-322, 18 U.S.C. § 2721, et seq., which requires the data to be kept confidentially. Every state has passed legislation to implement the DPPA. Many of these state statutes, like California's go beyond the original act.

The DPPA would be completely undercut if Congress allows for the easy harvesting of data from both the printed information and the MRZ on the license. How long will it be before another Amy Boyer?

4) Privacy Concerns Arising from Data Amassed by the States

The data storage and aggregation requirements imposed by the Act will lead to massive, and more serious cases of identity theft, which could lead to terrorists and sophisticated criminals impersonating innocent Americans, and will permit unlimited data mining by federal government agencies.

Contrary to DHS's assertions, the unprecedented data aggregation imposed by the Act will make us more vulnerable as a nation, not safer, primarily because it will facilitate massive identity theft and identity fraud, and make these cases more significant. The Act requires, at a minimum, that all source documents for licenses be retained either electronically or in storage at the DMV, along with additional biometric information and a driving history. Identity thieves will quickly recognize that the DMVs' records are a central location for obtaining all the documents and personally identifiable information they need to commit fraud.[7] Insider fraud, where state licensing officials sell IDs and information, will be impossible to stop and become even more profitable.

Further, identity theft and document fraud stemming from thefts from the Real ID databases will be far more significant than the troubling but garden variety identity theft that victims are currently experience. Instead of obtaining just one password to a bank account or one unique identifier, data thieves who access the Real ID database system will be able to obtain data on millions of individuals and obtain all at once a rich trove of information because DHS failed to require basic computer network data security be built into these databases. Thus, the data contained within the system will not be segmented or compartmentalized, with the result that any hacking event of the Real ID databases by an ID thief will provide access to all available documents and information. In short, the Real ID databases are destined to be the ID thieves' bank of choice to rob.

Further, the privacy invasion for those unfortunate ID theft victims will be more pronounced than current ID theft. The victims of Real ID database ID theft will encounter tremendous difficulty in obtaining new documents and recovering their identity because the ID thieves will have real copies – easily printed on a standard color printer – of the victim's Social Security Card and birth certificate.

[7] DHS actually exacerbates the identity theft problems in its regulations, suggesting that individuals can prove their principal address with a bank statement. 72 Fed. Reg. 10831.

The seriousness of this ID theft and document fraud will also make it easier for sophisticated criminals, immigrant smugglers and terrorists to obtain the identity of another person and pass themselves off as that person. **The aggregation of the data and the source documents thus opens a substantial security loophole.** This loophole is exactly contrary to the intent of the 9/11 Commission. Because of the rigidity of the Real ID Act's language, DHS had little flexibility to resolve this concern. **As a result, unless Congress revisits this portion of the Real ID Act, we will be weaker, not safer, due to the Real ID Act.**[8]

The Real ID database will also lead to significant privacy invasions by government snooping through data mining. Despite calls to expressly forbid data mining of the information aggregated in the Real ID database, to date, DHS refuses to promise not to data mine this interlinked data set or that to prohibit data mining by other federal anti-crime or anti-terror agencies. Senators should, therefore, expect that DHS would grant unfettered access to untested data mining programs that will search through millions of innocent licensees' most-sensitive personal information. Until these databases were linked under Real ID, such data mining was impractical or impossible. By linking these databases under Real ID, it will become possible for the government to conduct data mining on an unprecedented scale.

Unfortunately, the DPPA will not provide protections against this data mining. While the DPPA does prohibit DMVs from reselling data about licensees, it does not prohibit other agencies from accessing each DMVs databases. Congress should consider closing this loophole.

5) Privacy Concerns Regarding Data Transmissions

Mandated data sharing of licensees' information leads to what is referred to as a "false positive" problem in which the sharing of false or erroneous information leads to significant problems for licensees with the same or similar names as people who have lost their driving privileges, criminals or suspected terrorists. Because many licensees have common names, states will certainly mistakenly confuse licensees with each other. Undoubtedly, this "false positive" problem will lead to innocent Americans being improperly labeled as criminals or worse because the data from one state database transmitted to another state is erroneous. No easy fix exists for this false positive problem. If states send too little personally identifiable information to each other, innocent people will not be distinguishable from similarly named problem drivers, criminals or terrorists.

[8] For example, see the statement by the Privacy Rights Clearinghouse, a nationally recognized resource center for the victims of ID theft, which states that "[i]f you think identity theft is bad now, wait until something called the Real ID Act goes into effect." http://www.privacyrights.org/ar/real_id_act.htm.

VI. DHS Proposed Regulations Fail to Resolve Significant Constitutional and Civil Liberties Problems Caused by the Real ID Act

The Constitutional and civil liberties infirmities caused by the Real ID Act are unprecedented and are not resolved by DHS' Proposed Regulations. The Act could burden individuals' privacy rights and rights provided by the First and Sixth Amendments to the Constitution and its Due Process Clause. The Act arguable burdens the states in violation of the Tenth Amendment to the Constitution.

The Act unquestionably burdens the First Amendment guarantees of Freedom of Religion. The Act requires that all licensees be photographed and that all licenses contain on their face a digital photograph. As a result, Amish and Mennonite Christians whose religious beliefs forbid their images from being photographed face a clear burden on the practice of their religion. See, Alan Scher Zegeir, Mennonites Leaving Mo. Over Photo Law, Associated Press, Mar. 21, 2007 ("members of a [Missouri town's] Mennonite community are planning to move to Arkansas over a Missouri requirement that all drivers be photographed if they want a license. . . .because the law conflicts with the Biblical prohibition against the making of 'graven images.'") Still other evangelical Christians believe the Real ID Act will enumerate them in a manner contrary to their religious beliefs. Most states currently grant practitioners of these faiths and others license exceptions and states issue more than 260,000 licenses without pictures every year. DHS Real ID Impacts, Survey One. The Real ID Act's rigid mandates eliminate such state flexibility. Therefore, Congress must revisit the Act to provide for exceptions for First Amendment-protected religious practice.

Should an individual be unable to obtain a Real ID-compliant license for any number of reasons, or should DHS follow through on its threat to prohibit the citizens of states that are not complying with the Act from using their licenses for any "federal purpose" or to travel on planes, additional First Amendment and Sixth Amendment protected rights would be implicated. For example, if individuals from those states do not have the proper IDs to enter a federal agency, their ability to petition their government for redress of their grievances is compromised, as is their right to peaceably assemble in a public venue or meeting place. Both such applications of DHS' authority would impermissibly burden First Amendment protected rights. Similarly, if a federal criminal defendant lacked proper ID, the defendant might not be able to enter a federal court house to confront his accusers. Should DHS block residents of non-Real ID compliant states from flying on planes, those residents First Amendment-protected, U.S. Supreme Court-confirmed, Right to Travel would be impermissibly burdened. See, e.g., Saenz v. Roe, 526 U.S. 489 (1999). For residents of Hawaii, Alaska and Puerto Rico, a burden on the Right to Travel would have substantial economic and practical consequences. Congress must revisit the Real ID Act because these burdens are written into the statute and may only be resolved through legislative amendments.

Firearms owners are also concerned that the information sharing mandated by the Real ID Act could lead to a backdoor creation of a federal gun owners' registry. Many believe this would burden the gun owners' privacy interests. Although federal statutes contain two prohibitions on the creation of such a registry, many states do not have

similar registry prohibitions. Thus, if a state were to begin to encode gun ownership information in the machine readable zone and/or in the database supporting the ID card, other states would rapidly gain access to a list of the firearm owners of other states. The Real ID Act and the proposed regulations could, therefore, circumvent these two statutory prohibitions.

The Real ID Act and the DHS proposed regulations also raise certain Due Process Clause burdens. First, as noted above, if people cannot obtain Real ID-compliant licenses – because they lack proper documentation, they cannot afford vastly more expensive licenses, or due to bureaucratic bungling – similar burdens, will certainly arise for those unable to obtain licenses who need to visit a Social Security Administration office, federal prison, court house or any other federal agency. Congress must ask, because DHS did not: how will these people gain access to basic federal government services? If these burdens become substantial, Due Process Clause violations could result. Already, similar ID requirements have wrongly forced tens of thousands of individuals off the Medicaid roles. Robert Pear, Lacking Papers, Citizens are Cut from Medicaid, N.Y. Times, Mar. 12, 2007, at A1. Senators should expect to see their constituent case work rise exponentially with the implementation of the Act and corresponding license requirements to obtain government services and benefits.

Second, Due Process Clause concerns could arise for lawfully present immigrants. The Real ID Act's drafters failed to list numerous categories of lawful immigrants in the statutory list of those who could obtain a Real ID license or temporary license, such as parolees, persons under order of supervision, applicants for victim or witness visas, and applicants for cancellation of removal. Additionally, many lawfully present immigrants will be unable to prove their identity or immigration status. The proposed regulations unwisely limited the list of documents that immigrants could provide to prove identity and immigration status to a green card, employment authorization document, or current passport accompanied by a valid visa. Unfortunately, all too many lawfully present immigrants, such as many asylum applicants, will not likely possess these documents.

Third, Due Process Clause concerns will arise for the mass of citizens and lawfully present immigrants who find they need to challenge erroneous or incomplete information contained in state databases that wrongly prevents them from obtaining a license. The proposed regulations fail to provide an administrative or judicial process accessible as of right for would-be licensees to efficiently resolve data problems. Similarly, all too many lawfully present immigrants will suffer from an inability to see or correct immigration records. The proposed regulations do not provide a process for those immigrants whose status cannot be verified through DHS's Systematic Alien Verification for Entitlements ("SAVE") system. Nor do the regulations provide a process for those whose status was incorrectly reported to obtain their immigration records and correct them. DHS's only suggestion in its proposed regulations is for burdened immigrants to make an appointment with DHS or visit a local Citizenship and Immigration Service office. To obtain the documents, DHS recommends that immigrants file a Freedom of Information Act request, which could take years to be answered given current backlogs. For all aggrieved citizens and immigrants, DHS's failure to provide a

process to challenge and correct such errors efficiently and speedily condemns them to a second-class existence. Congress should revisit the Act to create true due process safeguards.

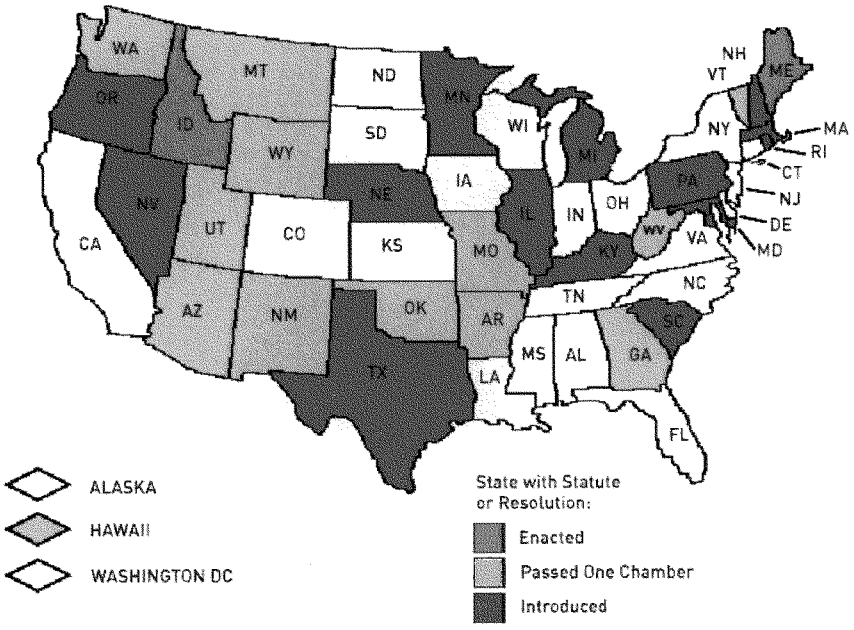
If Congress fails to revisit the Real ID Act and eliminate these Constitutional infirmities, the implementation of the Act and the proposed regulations could be delayed years as provisions are tied up in litigation.

VII. Conclusion: Congress Should Repeal Title II of the Real ID Act and Replace it with an Achievable Licensing Scheme that Does Not Threaten Personal Privacy and Civil Liberties

Congress cannot fix Title II of the Real ID Act; therefore, Congress must repeal the Act. And, if Congress wishes to move forward with a federal standardization of state-based licensing, Congress should replace Title II with legislation – such as S. 717 – creating a flexible, negotiated rulemaking as provided for in the Administrative Procedures Act 5 U.S.C. § 561, et. seq. (2007) that brings all interested parties to the negotiating table and grants them equal bargaining power.

S. 717, would eliminate the inflexible sections of the Real ID Act that drive up costs and do not allow for regulatory flexibility to protect privacy and constitutional rights. Without sufficient flexibility, DMVs will struggle to implement any licensing scheme. Further, S. 717 would put in place a negotiated rulemaking comprised of interested stakeholders and experts in various field, including privacy protection and civil liberties, to ensure that the final licensing scheme is workable while also respectful of our norms and values. The ACLU urges Congress to rapidly enact S. 717 to more rapidly produce counter- and tamper-resistant licenses in a statutory and regulatory framework devoid of privacy and civil liberties detriments.

Status of Anti-Real ID Legislation in the States



Testimony of Jim Harper
Director of Information Policy Studies, The Cato Institute
to the
Senate Committee on Homeland Security and Governmental Affairs
Subcommittee on Oversight of Government Management,
the Federal Workforce, and the District of Columbia
at a hearing entitled
Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers' Licenses and Identification Cards

March 26, 2007

Chairman Akaka, Ranking Member Voinovich, and Members of the Committee:

It is a pleasure to speak with you today. I am director of information policy studies at the Cato Institute, a non-profit research foundation dedicated to preserving the traditional American principles of limited government, individual liberty, free markets, and peace. In that role, I study the unique problems in adapting law and policy to the information age. I also serve as a member of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee, which advises the DHS Privacy Office and the Secretary of Homeland Security.

My most recent book is entitled *Identity Crisis: How Identification Is Overused and Misunderstood.* I am also editor of Privacilla.org, a Web-based think tank devoted exclusively to privacy, and I maintain an online resource about federal legislation and spending called WashingtonWatch.com. I speak only for myself today and not for any of the organizations with which I am affiliated or for any colleague.

* * * *

Mr. Chairman, the REAL ID Act is a dead letter. All that remains is for Congress to declare it so.

The proposed regulations issued by the Department of Homeland Security on March 9th "punted" on REAL ID's most important technology, security, and privacy problems. At the same time, the Department's own analysis helps reveal that REAL ID is a loser — it would cost more to implement than it would add to our country's protections.

Of utmost importance, the DHS proposal lays the groundwork for systematic tracking of Americans ***based on their race.*** The bar code system standard that DHS calls for in the regulation includes machine-readable information about race and ethnicity. This is deeply concerning and unwise. Federal law and regulation should not promote a national

ID system that can track people by race. History has too many devastating examples of identification systems used to divide people based on religion, tribe, and race.

Though the Department of Homeland Security failed to "fix it in the regs," this is not the agency's fault. Regulations cannot make this law work, and neither can delay. The real problem is the REAL ID law itself.

There are highly meritorious bills pending in the Senate and House to repeal the REAL ID Act. They would restore the identification security provisions that were passed in the 9/11-Commission-inspired Intelligence Reform and Terrorism Prevention Act. Congratulations, Mr. Chairman — and I salute Senator Sununu as well — for leading the way on this issue.

These bills would be improved if they were to chart a path to government use of emerging digital identity and credentialing systems that are diverse, competitive, and privacy protective. We can have identification and credentialing systems that maximize security and minimize surveillance. REAL ID is the ugly alternative to getting it right.

DHS Punted on the Hard Issues

Though many states have already voted to refuse the REAL ID Act, some have been waiting to see what they would find in the regulations issued by the Department of Homeland Security. Now that the regulations are out, it is clear that the states have been left holding the bag.

Were they to comply with the REAL ID Act, states would have to cross a mine-field of complicated and expensive technology decisions. They would face enormous, possibly insurmountable privacy and data security challenges. But the Department of Homeland Security avoided these issues by carefully observing the constraints of federalism even though the REAL ID law was crafted specifically to destroy the distinctions between state and federal responsibilities.

The Federalism Issue

The Constitution established a federal government with limited, enumerated powers, leaving the powers not delegated to the federal government to the states and people.[1] Because direct regulation of the states would be unconstitutional,[2] the REAL ID Act conditions federal acceptance of state-issued identification cards and drivers' licenses on their meeting certain federal standards.

This statutory structure — using state machinery to implement a federal program — is unfortunate. It blurs the lines of authority and obscures the workings of

[1] U.S. Const. amend. X.
[2] New York v. United States, 505 U.S. 144 (1992).

government from citizens and taxpayers. But it does draw federalism into play as a potential limit on the Department's ability to regulate.

As the Notice of Proposed Rulemaking ("NPRM") notes,[3] Executive Order 13132 says that "issues that are not national in scope or significance are most appropriately addressed by the level of government closest to the people."[4] Laying out the criteria for policymaking when federalism is implicated, the Executive Order says, "National action limiting the policymaking discretion of the States shall be taken only where there is constitutional and statutory authority for the action and the national activity is appropriate in light of the presence of a problem of national significance."[5]

In support of a federal function — national security — the REAL ID Act conditions federal acceptance of state identification cards and drivers' licenses on their meeting federal standards for documentation, issuance, evidence of lawful status, verification of documents, security practices, and maintenance of driver databases. The federal government has equal power — and the Department of Homeland Security had discretion in this rule — to condition acceptance of identification cards and drivers' licenses on closely related priorities, including meeting standards for privacy and data security.

The decision not to do this is a policy question that, according to the federalism Executive Order, turns on whether there is constitutional and statutory authority and whether national action is appropriate. The Department's decision to abandon these issues to the states is an implicit finding that privacy and data security are not problems of national significance. That finding is wrong. Privacy is a problem of national significance.

Many different federal laws and policies seek to foster privacy and data security, even in the context of national security programs. The Executive Order establishing the President's board on safeguarding Americans' civil liberties, for example, states in its very first section:

> The United States Government has a solemn obligation, and shall continue fully, to protect the legal rights of all Americans, including freedoms, civil liberties, and information privacy guaranteed by Federal law, in the effective performance of national security and homeland security functions.[6]

---

[3] 72 Fed. Reg. 10,820 (Mar. 9, 2007).
[4] E.O. 13132, Federalism (Aug. 4, 1999).
[5] *Id.*
[6] E.O. 13353, Establishing the President's Board on Safeguarding Americans' Civil Liberties (Aug 27, 2004).

Among the many federal laws that are relevant is the Privacy Act of 1974.[7] The Privacy Act requires federal agencies to undertake a variety of information practices, and it accords individuals a number of rights intended to protect privacy and similar interests. The law requires agencies to extend these protections to systems of records operated "by or on behalf of the agency . . . to accomplish an agency function" when that is done by contract.[8]

The Privacy Act apparently did not contemplate that states would maintain systems of records in furtherance of federal functions. However, Office of Management and Budget guidelines issued after the Privacy Act's passage say that the Act is intended to cover "de facto as well as de jure Federal agency systems."[9]

Another relevant law is FISMA, the Federal Information Security Management Act of 2002.[10] FISMA seeks to bolster information security within the federal government and for federal government functions by mandating yearly security audits. FISMA makes the head of each agency responsible for information security protections with regard to information systems and "information collected or maintained by or on behalf of the agency."[11]

REAL ID's Legislative History

The legislative history of the REAL ID Act suggests Congress' intention that the Department should implement REAL ID consistent with federal government policies on privacy. The Department of Homeland Security's Privacy Impact Assessment reviews relevant portions of that history:

> The House Conference Report for the REAL ID Act includes several key statements of Congressional intent regarding privacy. For example, in its discussion of section 202(d)(12) of the Act, which requires each state to provide electronic access to the information in its motor vehicle databases to all of the other states, the Conference Report makes clear that Congress recognized the need for the regulations to address privacy and security and that those protections should be at least the equivalent of existing federal protections. The Conference Report reads in relevant part:
>
> > DHS will be expected to establish regulations which adequately protect the privacy of the holders of licenses and ID cards which meet the standards for federal identification and federal purposes.

---

[7] 5 U.S.C. §552a.
[8] Id. at §552a(m).
[9] Office of Management and Budget, Privacy Act Implementation: Guidelines and Responsibilities,
[10] 44 U.S.C. § 3541 et seq. (enacted as Title III of the E-Government Act of 2002, Pub.L. 107-347).
[11] 44 U.S.C. § 3544(a)(1)(A).

> In addition, the Conference Report discussion of Section 202(b)(9) of the Act, which calls for using "a common machine-readable technology, with defined minimum data elements," clearly indicates that Congress wanted privacy to be a consideration in implementing the technology. The Conference Report states:
>
> > There has been little research on methods to secure the privacy of the data contained on the machine readable strip. Improvements in the machine readable technology would allow for less data being present on the face of the card in the future, with other data stored securely and only able to be read by law enforcement officials.[12]

REAL ID has Formidable Privacy and Data Security Problems

The privacy and data security consequences arising from REAL ID are immense, increasingly well understood, and probably insurmountable.

The increased data collection and data retention required of states is concerning. Requiring states to maintain databases of foundational identity documents will create an incredibly attractive target to criminal organizations, hackers, and other wrongdoers. The breach of a state's entire database, containing copies of birth certificates and various other documents and information, could topple the identity system we use in the United States today. The best data security is not creating large databases of sensitive and valuable information in the first place.

The requirement that states transfer information from their databases to each other is concerning. This exposes the security weaknesses of each state to the security weaknesses of all the others. There are ways to limit the consequences of having a logical national database of driver information, but there is no way to ameliorate all the consequences of the REAL ID Act requirement that information about every American driver be made available to every other state.

There are serious concerns with the creation of a nationally uniform identity system. Converting from a system of many similar cards to a system of uniform cards is a major change. It is not just another in a series of small steps.

Economists know well that standards create efficiencies and economies of scale. When all the railroad tracks in the United States were converted to the same gauge, for example rail became a more efficient method of transportation. Because the same train car could travel on tracks anywhere in the country, more goods and people traveled by rail. Uniform ID cards would have the same influence on the uses of ID cards.

There are machine-readable components like magnetic strips and bar codes on many licenses today. Their types, locations, designs, and the information they carry differs

---

[12] U.S. Department of Homeland Security, Privacy Impact Assessment for the REAL ID Act (Mar. 1, 2007) (footnotes and italics omitted) <http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_realid.pdf>.

from state to state. For this reason, they are not used very often. If all identification cards and licenses were the same, there would be economies of scale in producing card readers, software, and databases to capture and use this information. Americans would inevitably be asked more and more often to produce a REAL ID card, and share the data from it, when they engaged in various governmental and commercial transactions.

In turn, others will capitalize on the information collected in state databases and harvested using REAL ID cards. Speaking to the Department of Homeland Security's Data Privacy and Integrity Advisory Committee last week, Anne Collins, the Registrar of Motor Vehicles for the Commonwealth of Massachusetts said, "If you build it they will come." Massed personal information will be an irresistible attraction to the Department of Homeland Security and many other governmental entities, who will dip into data about us for an endless variety of purposes.

Sure enough, the NPRM cites some other uses that governments are likely to make of REAL ID, including controlling "unlawful employment," gun ownership, drinking, and smoking. Uniform ID systems are a powerful tool. If we build it, they will come. REAL ID will be used for many purposes beyond what are contemplated today.

But the NPRM "punts" on even small steps to control these privacy concerns. It says for example that it "does not create a national database, because it leaves the decision of how to conduct the exchanges in the hands of the States."[13] My car didn't hit you — the bumper did!

As to security and privacy of the information in state databases, the NPRM proposes paperwork. Under the proposed rules, states must prepare a "comprehensive security plan" covering information collected, disseminated, or stored in connection with the issuance of REAL ID licenses from unauthorized access, misuse, fraud, and identity theft. Requiring production of a plan is not nothing, and the NPRM refers to various "fair information practices." However, preparing a plan is not a standard. The NPRM does not even condition federal acceptance of state cards on meeting the low standards of the federal Privacy Act or FISMA.

The REAL ID Act provided the Department of Homeland Security with very little opportunity to "fix it in the regs." And DHS did not fix it in the regs.

REAL ID *Fails* Cost-Benefit Analysis

The privacy and dollar costs of REAL ID would be easy to bear if this national ID system would add significantly to our country's protections. But the cost-benefit analysis provided in the NPRM helps show that it does not. Implementation of REAL ID would impose more costs on our society than it would provide in security or other benefits.

[13] 72 Fed. Reg. 10,825 (Mar. 9, 2007).

Executive Order 12866[14] requires agencies to assess the costs and benefits of the requirements they propose. The Department found that implementing REAL ID would cost over $17 billion.[15] This is 50% higher than the $11 billion estimate put forward by the National Conference of State Legislators. Again, these costs would be worth it — if the REAL ID Act had net benefits. It does not.

On the question of benefits, the regulatory analysis in the NPRM essentially punts:[16]

> It is impossible to quantify or monetize the benefits of REAL ID using standard economic accounting techniques. However, though difficult to quantify, everyone understands the benefits of secure and trusted identification. The proposed minimum standards seek to improve the security and trustworthiness of a key enabler of public and commercial life – state-used driver's licenses and identification cards. As detailed below, these standards will impose additional burdens on individuals, States, and even the Federal government. These costs, however, must be weighed against the intangible but no less real benefits to both public and commercial activities achieved by secure and trustworthy identification.

This is not analysis, of course. It is surmise. A few paragraphs later:

> The proposed REAL ID regulation would strengthen the security of personal identification. Though difficult to quantify, nearly all people understand the benefits of secure and trusted identification and the economic, social, and personal costs of stolen or fictitious identities. The proposed REAL ID NPRM seeks to improve the security and trustworthiness of a key enabler of public and commercial life – state-issued driver's licenses and identification cards.
>
> The primary benefit of REAL ID is to improve the security and lessen the vulnerability of federal buildings, nuclear facilities, and aircraft to terrorist attack. The rule would give states, local governments, or private sector entities an option to choose to require the use of REAL IDs for activities beyond the official purposes defined in this regulation. To the extent that states, local governments, and private sector entities make this choice, the rule may facilitate processes which depend on licenses and cards for identification and may benefit from the enhanced security procedures and characteristics put in place as a result of this proposed rule.

The assessment goes on to imagine what protection-rates would cost-justify the REAL ID Act regulations.[17] According to the assessment, if REAL ID lowers by 3.6% per year the

---

[14] Executive Order 12866, Regulatory Planning and Review (Sept. 30, 1993), requires "significant regulatory actions," such as those costing over $100 million annually, to be assessed in terms of benefits, costs, and alternatives.
[15] *Id.* at 10,845 (2006 dollars discounted at 7%).
[16] *See* 72 Fed. Reg. 10844-46 (Mar. 9, 2007).

annual probability of a terrorist attack causing immediate impacts of $63.9 billion, the rules would have net benefits. If REAL ID lowers by 0.61% per year the annual probability of a terrorist attack causing both immediate and longer run impacts of $374.7 billion, the rules would have net benefits.

This is an unsound way of judging the anti-terrorism benefits of REAL ID, and it reflects almost no thinking about how REAL ID might work as a security tool. I have attached as Appendix A a rudimentary analysis of the REAL ID Act in terms of risk management, using the framework put forward by the Department of Homeland Security's Data Privacy and Integrity Advisory Committee.[18]

Creating a national identification scheme does not just attach a known, accurate identity to everyone. It causes wrongdoers to change their behavior. Sometimes this controls risks, sometimes this shifts risks from one place to another, and sometimes this creates even greater risks. Rather than being evaluated on its ability to prevent attacks outright, as the NPRM did, the REAL ID Act should be assessed in terms of its ability to delay attacks or change their character.

Assuming, for example, that a future attack would be on the scale of a 9/11 — probably an exaggerated assumption — REAL ID might be assumed (generously) to delay such an attack by six months. The value of delaying such an attack, and thus the security value of REAL ID, ranges from $2.24 billion to $13.1 billion.[19] REAL ID offers less in benefits than it does at costs — even using very generous assumptions.

The information published NPRM concludes with this:

> The potential ancillary benefits of REAL ID are numerous, as it would be more difficult to fraudulently obtain a legitimate license and would be substantially more costly to create a false license. These other benefits include reducing identity theft, unqualified driving, and fraudulent activities facilitated by less secure driver's licenses such as fraudulent access to government subsidies and welfare programs, illegal immigration, unlawful employment, unlawful access to firearms, voter fraud, and possibly underage drinking and smoking. DHS assumes that REAL ID would bring about changes on the margin that would potentially increase security and reduce illegal behavior. Because the size of the economic costs that REAL ID serves to reduce on the margin are so large, however, a relatively small impact of REAL ID may lead to significant benefits.

---

[17] This is permitted by OMB Circular A-4 when it is difficult to quantify and monetize the benefits of a rulemaking.

[18] Data Privacy and Integrity Advisory Committee, U.S. Department of Homeland Security, *Framework for Privacy Analysis of Programs, Technologies, and Applications*, Report No. 2006-01 (Mar. 1, 2006) <http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_03-2006_framework.pdf>.

[19] Assumed delay from today until 6 months into the future. (Net present value at 3.5%/6 months interest.)

The actual economic analysis produced by DHS and placed in the rulemaking docket has some more specific information about "ancillary benefits." It estimates that REAL ID could reduce the costs of identity theft by merely $1.6 billion during 2007-16. No other benefits are estimated.

In summary, implementation of REAL ID would cost over $17 billion dollars. Its security benefits, under generous assumptions, might reach about $15 billion. REAL ID promises 88 cents worth of national security for every national security dollar we spend. These dollars would be taken from children's health care, from American families' food budgets, and from security programs that actually work. Implementing REAL ID would harm the country.

These practical considerations are very important, but there are long-term, principled reasons why Congress should reconsider the REAL ID Act immediately.

REAL ID: The Race Card

The "machine-readable technology" required for every REAL ID-compliant card has been a subject of much worry and speculation. This is not without reason. A nationally uniform ID card will make it very likely that cards will be requested, and the data on them collected and used, by governments and corporations alike. DHS was wise to resist the use of radio frequency identification tags in REAL ID.[20]

But even more significant issues have been created by the DHS's choice of technical standards. The standard for the 2D barcode selected by the Department includes the cardholder's race as one of the data elements.

If the REAL ID card is implemented, Americans transacting business using the REAL ID card may well be filling government and corporate databases with information that ties their race to records of their transactions and movements. Students of history should find the prospect sickening.

For the machine readable portion of the card, the technology standard proposed by DHS in the NPRM is the PDF-417 two-dimensional bar code. According to DHS, the PDF-

---

[20]The NPRM left the door for putting RFID chips in our identification cards in the future. *See* 72 Fed. Reg. 10,841-2 (Mar. 9, 2007). The DHS Data Privacy and Integrity Advisory Committee concluded recently that RFID is not well suited to the task of identifying people, at least at this stage in the technology's development. Department of Homeland Security, Data Privacy & Integrity Advisory Committee, *The Use of RFID for Human Identify Verification*, Report No. 2006-02 (Dec. 6, 2006) <http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf>. The Department has recently cancelled RFID-related projects. *See* Alice Lipowicz, *DHS Tunes Out RFID*, Washington Technology (Feb. 12, 2007) <http://www.washingtontechnology.com/online/1_1/30131-1.html>.

417 barcode can be read by a standard 2D barcode scanner.[21] This is a more highly developed version of the barcode scanning that is done in grocery stores across the country.

The version selected by DHS is the 2005 AAMVA Driver's License/Identification Card Design Specifications, Annex D. This is a standardized format for putting information in the bar code.

A summary of the data elements from the standard is attached as Appendix B, but briefly, white people would carry the designation "W"; black people would carry the designation "BK"; people of Hispanic origin would be designated "H"; Asian or Pacific Islanders would be "AP"; and Alaskan or American Indians would be "AI."

DHS does not require all the data elements from the standard, and it does not require the "race/ethnicity" data element, but the standard it has chosen will likely be adopted in its entirety by state driver licensing bureaus. The DHS has done nothing to prevent or even discourage the placement of race and ethnicity in the machine readable zones of this national ID card.

Avoiding race- and ethnicity-based identification systems is an essential bulwark of protection for civil liberties, given our always-uncertain future. In Nazi Germany, in apartheid South Africa, and in the recent genocide in Rwanda, horrible deeds were administered using identification cards that included information about religion, about tribe, and about race. Implementation of the REAL ID Act, which would permit race to be a part of the national identification card scheme, would be a grave error.

Akaka-Sununu is Essential — and it Needs a Vision of the Future

Congratulations again, Mr. Chairman — and I salute Senator Sununu, as well — on your leadership in introducing, for the second Congress in a row, legislation to repeal REAL ID and restore the ID security provisions from the 9/11-Commission-inspired Intelligence Reform and Terrorism Prevention Act.

REAL ID is often touted as a direct response to a strong recommendation of the 9/11 Commission. This is untrue on a number of levels.

The recent push for national ID cards is in reaction to the terrorist attacks of September 11, 2001, of course. An appendix to a report by the Markle Foundation Task Force on National Security in the Information Age recommended various governmental measures to make identification "more reliable."[22] This report was cited by the 9/11 Commission

---

[21] 72 Fed. Reg. 10,837-8 (Mar. 9, 2007).

[22] Markle Foundation Task Force on National Security in the Information Age, Creating a Trusted Network for Homeland Security (Dec. 2, 2003) < http://www.markletaskforce.org/>. The main body of the report endorsed the finding of the Appendix unconditionally. *See id.* at 36.

as it recommended "federal government . . . standards for the issuance of birth certificates and forms of identification, such as drivers licenses."[23] But it is important to know that the 9/11 Commission devoted about ¾ of a page in its 400-page report to identification issues. Identification security was not a "key finding" of the Commission.

Nonetheless, a provision of the Intelligence Reform and Terrorism Prevention Act of 2004, passed in response to the 9/11 Commission Report, established a negotiated rulemaking process for determining minimum standards for federally acceptable driver's licenses and identification cards.[24] This provision — the result of the 9/11 Commission report — was repealed and replaced by the REAL ID Act. Restoring the earlier, more careful provisions would be a step in the right direction.

But the Congress should examine our country's identification policies and practices even more carefully. Identification systems have many benefits but, as we know from REAL ID, they also carry many threats. We should have a much more careful national discussion about the design of the identity systems we will use in the future.

There are identification systems being devised today by the countries' brightest technologists that would provide all the security that identification can provide, but that would resist tracking and surveillance. Meanwhile, hundreds of millions — if not billions — of taxpayer dollars are already being spent on ID systems with little regard for their interoperability with emerging open standards, to say nothing of privacy.

It would be unfortunate of the federal government spent so much time and money to build systems that lead in a few decades to very costly dead end. Even worse would be for government systems to predominate, making it a practical requirement that Americans do have to carry a national ID card in order to function.

As it moves forward, I recommend that the Akaka-Sununu legislation include consideration of emerging open standards for government IDs and credentials. Rather than being locked into the unwieldy federal systems now being created, federal agencies should have the flexibility to accept any identification card or credential that meets or exceeds government standards for data accuracy, security, and verifiability.

In Akaka-Sununu, Congress should recognize the emergence of identity and credentialing systems that are diverse, competitive, and — most importantly — privacy protective. These systems can maximize security while minimizing surveillance. REAL ID is the ugly alternative to getting it right.

---

[23] National Commission on Terrorist Attacks Upon the United States (9-11 Commission), The 9/11 Commission Report (2004) at 390.
[24] Intelligence Reform and Terrorism Prevention Act, Pub. L. No. 108-458, §7212.

APPENDIX A

Rudimentary Analysis of REAL ID Act in Terms of Risk Management

Assessing how, and how well, the REAL ID Act regulations benefit the homeland security mission in terms of risk management requires answers to the following questions. Answers available in the NPRM are critiqued here, and sensible or assumed answers are supplied:

- *What are you trying to protect?* The NPRM identifies federal buildings, nuclear facilities, and aircraft as the primary beneficiaries of the REAL ID rules, as well as other infrastructure should access to it be conditioned on showing ID. "Ancillary" beneficiaries would be the many segments of the public who would benefit from various types of fraud reduction, public safety law enforcement, and various forms of personal regulation.

- *What are you trying to protect it from?* The primary threat articulated by the rule's brief benefit statement is "terrorist attack," which can take any number of forms. The assessment does not describe with particularity any vulnerability or the way any of these assets may be harmed, much less how REAL ID would prevent or diminish such harm. As to ancillary beneficiaries, it is well known that fraud, unsafe behavior, and unwise personal choices have a variety of costs. The assessment does not describe how the REAL ID regulations would prevent these ills, though as part of an expanded police and regulatory state, they undoubtedly would.

- *What is the likelihood of each threat occurring and the consequence if it does?* The rule's benefit statement makes no attempt at terrorism risk assessment, positing instead two different "9/11" scenarios, the avoidance of which would cost-justify the rules. The ancillary harms the assessment claims to effect vary widely across the landscape of human action, and have a variety of likelihoods and consequences.

- *What kind of action does the program take in response to the threat — acceptance, prevention, interdiction, or mitigation?* The NPRM does not go into this kind of detail, but the REAL ID rules are best characterized as interdiction: a form of confrontation with, or influence exerted on, an attacker to eliminate or limit its movement toward causing harm. A more accurate and secure identification system may interfere with terrorists in a variety of ways.

  Requiring REAL ID-compliant identification cards for access to secured areas would limit the field of potential attackers on those areas to only those people that are able to prove their identity and lawful presence in the United States. This would inconvenience foreign terrorist organizations, likely changing their

behavior in a number of ways. The REAL ID Act might cause foreign terrorist organizations to target infrastructure that is not secured by identification requirements. It might cause them to select individual attackers who can lawfully enter the U.S. and acquire identification.[25] It might cause them to ally with domestic criminals or criminal organizations.

They may attack the REAL ID system in various ways. The REAL ID regulations might induce foreign terrorist organizations to procure REAL ID-compliant cards through corrupt Department of Motor Vehicles employees. It might cause them to seek counterfeit documents that can fool DMV employees into issuing REAL ID-compliant cards. It might cause them to seek counterfeit REAL ID-compliant cards good enough to fool verifiers at checkpoints. It might cause them to corrupt verifiers at checkpoints.

Whatever the case, the REAL ID regulations would cause some inconvenience to foreign terrorist organizations seeking to mount an attack on infrastructure secured behind checkpoints.

A second form of interdiction, also not discussed in the NPRM, is the use of REAL ID in conjunction with watch lists. Again putting aside attacks on the REAL ID system, requiring REAL ID-compliant identification cards for access to secured areas would limit the field of potential attackers on those areas to only those people that are not known to be terrorists by the authorities. Coupled with watch lists, the REAL ID regulations might cause terrorist organizations, foreign and domestic, to target infrastructure that is not secured by identification requirements. It might cause them to select attackers who are not known to have contacts with terrorists.[26] It also might cause them to attack the REAL ID system in the ways discussed above.

Similar to the joining of REAL ID to watch lists in terrorism interdiction, REAL ID may be joined to a variety of commercial, law enforcement, and regulatory programs aimed at reducing fraud, promoting public safety, law enforcement, and various forms of personal regulation. Each of these multitudinous potential uses of REAL ID would alter the behavior of "attackers" in various ways. It would improve their behavior in some cases, inspire avoidance in others, and also in some cases prompt attacks on the REAL ID system like those discussed above, such as by college students seeking a good fake ID.

---

[25] In general, this was the modus operandi of al Qaeda in the 9/11 attacks.

[26] As demonstrated by the "Carnival Booth" study, relevant information from watch lists is relatively easy to reverse-engineer. One must simply send an attacker through a checkpoint on a few "dry runs" to determine whether he or she is subject to different treatment. *See* Samidh Chakrabarti and Aaron Strauss, *Carnival Booth: An Algorithm for Defeating the Computer-Assisted Passenger Screening System*, 6.806: Law and Ethics on the Electronic Frontier (May 16, 2002) < http://www-swiss.ai.mit.edu/6095/student-papers/spring02-papers/caps.htm>.

- *Does the response create new risks to the asset or others?* Some of the avoidance behaviors listed above would transfer risks or create new risks. Terrorists may shift from REAL-ID-secured targets to non-REAL-ID-secured targets.[27] Foreign terrorist organizations allying themselves with domestic criminal organizations to avoid REAL ID-based security might form more dangerous hybrid organizations. As noted above, there would certainly be attacks on the REAL ID system, in terms of technical security, corruption, fraud, and so on. The techniques developed by "casual" attackers such as college students would accrue to the benefit of the serious threats such as criminal or terrorist organizations. These are just some of the risk transfers and new risks that would result from implementing the REAL ID regulations.

[27] Assuming terrorists aim to sap the economy and vitality of the United States, they could do very well by serially attacking non-ID-controlled targets if that would induce the U.S. to secure them through ID checks. If each of the 240 million licensed drivers in the U.S. were inconvenienced by just one minute per week to show ID at malls, subway stations, bus depots, office buildings, and other public infrastructure, the cost to society in lost time alone (assumed value: $20/hr.) would be over $4 billion per year – a net present cost of $57 billion (assumed 7% interest).

APPENDIX B

From: Personal Identification — AAMVA International Specification — DL/ID Card Design, Annex D: "Mandatory PDF417 Bar Code"

MINIMUM MANDATORY DATA ELEMENTS

Jurisdiction-Specific Vehicle Class
Jurisdiction-specific vehicle class / group code, designating the type of vehicle the cardholder has privilege to drive.

Jurisdiction-Specific Restriction Codes
Jurisdiction-specific codes that represent restrictions to driving privileges (such as airbrakes, automatic transmission, daylight only, etc.).

Jurisdiction-Specific Endorsement Codes
Jurisdiction-specific codes that represent additional privileges granted to the cardholder beyond the vehicle class (such as transportation of passengers, hazardous materials, operation of motorcycles, etc.).

Document Expiration Date Date on which the driving and identification privileges granted by the document are no longer valid. (MMDDCCYY for U.S., CCYYMMDD for Canada)

Customer Family Name Family name of the cardholder. (Family name is sometimes also called "last name" or "surname.") Collect full name for record, print as many characters as possible on front of DL/ID.

Customer Given Names Given names of the cardholder. (Given names include all names other than the Family Name. This includes all those names sometimes also called "first" and "middle" names.) Collect full name for record, print as many characters as possible on front of DL/ID.

Document Issue Date Date on which the document was first issued. (MMDDCCYY for U.S., CCYYMMDD for Canada)

Date of Birth Date on which the cardholder was born. (MMDDCCYY for U.S., CCYYMMDD for Canada)

Physical Description – Sex Gender of the cardholder. 1 = male, 2 =female.

Physical Description – Eye Color
Color of cardholder's eyes. (ANSI D-20 codes)

Physical Description – Height
Height of cardholder. Inches (in): number of inches followed by " in" ex. 6'1" = " 73 in" Centimeters (cm): number of centimeters followed by " cm" ex. 181 centimeters="181 cm"

Address – Street 1 Street portion of the cardholder address.

Address – City City portion of the cardholder address.

Address – Jurisdiction Code
State portion of the cardholder address.

Address – Postal Code Postal code portion of the cardholder address in the U.S. and Canada. If the trailing portion of the postal code in the U.S. is not known, zeros will be used to fill the trailing set of numbers.

Customer ID Number The number assigned or calculated by the issuing authority.

Document Discriminator Number must uniquely identify a particular document issued to that customer from others that may have been issued in the past. This number may serve multiple purposes of document discrimination, audit information number, and/or inventory control.

Country Identification Country in which DL/ID is issued. U.S. = USA, Canada = CAN.

Federal Commercial Vehicle Codes
Federally established codes for vehicle categories, endorsements, and restrictions that are generally applicable to commercial motor vehicles. If the vehicle is not a commercial vehicle, "NONE" is to be entered.

OPTIONAL DATA ELEMENTS

Address – Street 2 Second line of street portion of the cardholder address.

Hair color	Brown, black, blonde, gray, red/auburn, sandy, white
Place of birth	Country and municipality and/or state/province
Audit information	A string of letters and/or numbers that identifies when, where, and by whom a driver license/ID card was made. If audit information is not used on the card or the MRT, it must be included in the driver record.
Inventory control number	A string of letters and/or numbers that is affixed to the raw materials (card stock, laminate, etc.) used in producing driver licenses and ID cards.
Alias / AKA Family Name	Other family name by which cardholder is known.
Alias / AKA Given Name	Other given name by which cardholder is known
Alias / AKA Suffix Name	Other suffix by which cardholder is known
Name Suffix	Name Suffix (If jurisdiction participates in systems requiring name suffix (PDPS, CDLIS, etc.), the suffix must be collected and displayed on the DL/ID and in the MRT). Collect full name for record, print as many characters as possible on front of DL/ID.
Physical Description – Weight Range	Indicates the approximate weight range of the cardholder: 0 = up to 31 kg (up to 70 lbs) 1 = 32 – 45 kg (71 – 100 lbs) 2 = 46 - 59 kg (101 – 130 lbs) 3 = 60 - 70 kg (131 – 160 lbs) 4 = 71 - 86 kg (161 – 190 lbs) 5 = 87 - 100 kg (191 – 220 lbs) 6 = 101 - 113 kg (221 – 250 lbs) 7 = 114 - 127 kg (251 – 280 lbs) 8 = 128 – 145 kg (281 – 320 lbs) 9 = 146+ kg (321+ lbs)
Race / ethnicity	Codes for race or ethnicity of the cardholder, as defined in ANSI D20.
Standard vehicle classification	

Standard vehicle classification code(s) for cardholder. This data element is a placeholder for future efforts to standardize vehicle classifications.

Standard endorsement code

Standard endorsement code(s) for cardholder. This data element is a placeholder for future efforts to standardize endorsement codes.

Standard restriction code Standard restriction code(s) for cardholder. This data element is a placeholder for future efforts to standardize restriction codes.

Jurisdiction specific vehicle classification description

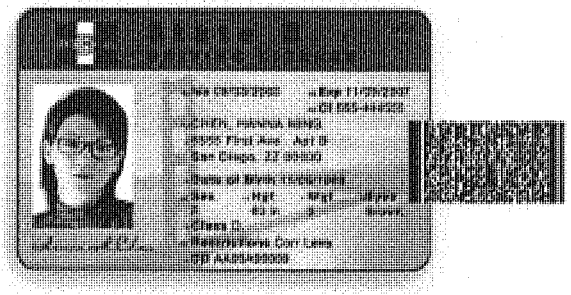
Text that explains the jurisdiction-specific code(s) for types of vehicles cardholder is authorized to drive.

Jurisdiction specific endorsement code description

Text that explains the jurisdiction-specific code(s) that indicates additional driving privileges granted to the cardholder beyond the vehicle class.

Jurisdiction specific restriction code description

Text describing the jurisdiction-specific restriction code(s) that curtail driving privileges.



Data Ref.	Element ID	Data Element	Definition	Card type	Length / type
			5 = 87 - 100 kg (191 – 220 lbs) 6 = 101 7 = 114 8 = 128 9 = 140		
k.	DCL	Race / ethnicity	Codes		
l.	DCM	Standard vehicle classification	Standa cordhc for full classif		
m.	DCN	Standard endorsement code	Stand This d efforts		
n.	DCO	Standard restriction code	Stand This effort		
o.	DCP	Jurisdiction-specific vehicle classification description	Text code auth		
p.	DCQ	Jurisdiction-specific endorsement code description	Tex cod prio veh		
q.	DCR	Jurisdiction-specific restriction code description	Tex res		

Race

AI	Alaskan or American Indian (Having Origins in Any of The Original Peoples of North America, and Maintaining Cultural Identification Through Tribal Affiliation of Community Recognition)
AP	Asian or Pacific Islander (Having Origins in Any of the Original Peoples of the Far East, Southeast Asia, or Pacific Islands. This Includes China, India, Japan, Korea, the Philippines Islands, and Samoa)
BK	Black (Having Origins in Any of the Black Racial Groups of Africa)
W	White (Having Origins in Any of The Original Peoples of Europe, North Africa, or the Middle East)

Ethnicity

H	Hispanic Origin (A Person of Mexican, Puerto Rican, Cuban, Central or South American or Other Spanish Culture or Origin, Regardless of Race)
O	Not of Hispanic Origin (Any Person Other Than Hispanic)
U	Unknown

The category which most closely reflects the individual's recognition in his community should be used to report persons of mixed racial and or ethnic origins. *Example:* a Black person of Hispanic origin would be coded BKH; an Asian person not of Hispanic origin would be coded APO.

Source:

Race and Ethnic Standards For Federal Statistics and Administrative Reporting, Directive No. 15, Bureau of the Census. (Issued before 8/29/1979)

D.12.3.3 Additional data elements

Jurisdictions wishing to encode data elemen
lists of mandatory and optional data elemen
to use for that data. This will prevent the int

UNDERSTANDING THE REALITIES OF REAL ID: A REVIEW OF EFFORTS

March 26, 2007

BACKGROUND

Prior to the passage of the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA), standards with respect to drivers' licenses and personal identification cards were determined on a state-by-state basis with no national standards in place. However, the 9-11 Commission found that all but one of the 9-11 hijackers acquired a form of U.S. identification document, some by fraud, which would have assisted them in boarding commercial flights, renting cars, and other activities. As such, the Commission recommended the federal government set standards for the issuance of birth certificates and sources of identification, such as drivers' licenses.

The IRTPA required the Secretary of Transportation, in consultation with the Secretary of Homeland Security, to issue regulations with respect to minimum standards for federal acceptance of drivers' licenses and personal identification cards.

The IRTPA required the use of negotiated rulemaking to bring together agency representatives and concerned interest groups to negotiate the text of a proposed rule. The proposed rule would include minimum standards for the documentation required by the applicant, the procedures utilized for verifying the documents used, requirements for what was to be included on the card, and the standards for processing the applications. In addition, if a state granted a certain category of individuals (i.e., aliens, legal or illegal) permission to obtain a license, nothing in the implementing regulations were to infringe on that state's decision or its ability to enforce that decision. In addition, the regulations were also not to require a single uniform design and were required to include procedures designed to protect the privacy rights of individual applicants. The parties to the negotiated rulemaking process met once before the *REAL ID Act* became law.

REAL ID Act

The REAL ID Act, introduced by Representative James Sensenbrenner on January 26, 2005, passed Congress as part of H.R.1268, *the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief of 2005*, and replaced the provisions in the IRTPA to secure drivers' licenses.

The REAL ID Act requires DHS to issue regulations to establish minimum issuance standards for federal recognition requiring that before a state can issue a driver's license or photo identification card, a state will have to verify with the issuing agency, the issuance, validity, and completeness of: (1) a photo identification document or a non-photo document containing both the individual's full legal name and date of birth; (2) date of birth; (3) proof of a social security number (SSN) or verification of the individual's ineligibility for a SSN; and (4) name and address of the individual's principal residence.

The Act also requires states to verify an applicant's legal status in the United States before issuing a driver's license or personal identification card and adopt procedures and

practices to: (1) employ technology to capture digital images of identity source documents; (2) retain paper copies of source documents for a minimum of seven years or images of source documents presented for a minimum of ten years; (3) subject each applicant to a mandatory facial image capture; (4) establish an effective procedure to confirm or verify a renewing applicant's information; (5) confirm with the Social Security Administration a SSN presented by a person using the full Social Security account number; (6) refuse issuance of a driver's license or identification card to a person holding a driver's license issued by another state without confirmation that the person is terminating or has terminated the driver's license; (7) ensure the physical security of locations where cards are produced and the security of document materials and papers from which drivers' licenses and identification cards are produced; (8) subject all persons authorized to manufacture or produce drivers' licenses and identification cards to appropriate security clearance requirements; (9) establish fraudulent document recognition training programs for appropriate employees engaged in the issuance of drivers' licenses and identification cards; (10) would limit the length of time a drivers' license or personal identification card is valid to eight years.

Lastly, the Act requires states to provide electronic access to their databases to all other states. States must adopt federal standards and modify any conflicting state laws or regulations in order for such documents to be used to enter federal buildings, to board aircraft, or for other federal purposes. A federal agency may not accept a driver's license or personal identification card after May 11, 2008, unless the state has been certified by DHS to meet the requirements of the law. The DHS Secretary may grant a state an extension to meet the certification requirement if the state provides adequate justification for noncompliance

Since enactment of REAL ID, several organizations have come forward with concerns about the law, including the National Governors Association (NGA), the National Conference of State Legislatures (NCSL), and the American Civil Liberties Union (ACLU). In general terms, the concerns focus on several key themes: REAL ID could create an unfunded mandate for the states, REAL ID could be a national ID card, REAL ID could make it easier to steal personal information, and REAL ID could violate civil liberties. A paper issued by NGA, NCSL, and the American Association of Motor Vehicle Administrators (AAMVA) is included in this notebook which lays out their concerns. A report issued by the ACLU on its concerns with privacy and civil liberties is also included.

REAL ID Act Regulations

On March 1, 2007, DHS released a notice of proposed rulemaking, which were published in the Federal Register on March 9, 2007. The comment period runs for 60 days from the date of publication. A brief summary of the regulations follows.

Deadlines, Reenrollment, and Funding

States must begin issuing REAL ID-compliant driver's licenses (DLs) and identification cards (IDs) by May 11, 2008 in order for them to be recognized for federal purposes. The Secretary has the authority to grant an extension up to December 31, 2009. Extension requests must be made by October 2007. States receiving an extension must submit, no later than 6

months from the date on which the extension was received, a plan detailing milestones, schedules and budgets allowing the state to meet the requirements of the final regulation. All states, including those granted extensions will have until May 11, 2013, to reenroll all existing DL/ID holders. While NGA, NCSL, and AAMVA welcomed the deadline extension, there are still concerns about the reenrollment period.

DHS estimated the cost of implementation at $23.1 billion over 10 years, of which $10 billion to $14 billion are costs to states. DHS will enable states to use up to 20 percent of their State Homeland Security Grant Program (SHSGP) funds for implementation of the REAL ID. (Under current law states are required to pass 80 percent of these funds to local governments, leaving 20 percent for states). This program received $525 million in federal funds in FY 2007. The President's budget request reduces funds for this program to $187 million for FY 2008. Most states already have dedicated SHSGP funds for other homeland security projects.

States will have to submit, by February 10, 2008, the following documents for an initial certification and will have to re-certify prior to January 1 each year:

- A detailed narrative of the state's program for issuing REAL ID compliant cards, including a description of the state's exception process and the state's waiver process;
- A comprehensive security plan for all DMV offices and storage and production facilities, databases and facilities. This includes demonstrating best practices to protect privacy;
- A letter from the state Attorney General confirming the state has the legal authority to impose requirements necessary to meet the standards established;
- A copy of all statutes, regulations, administrative procedures and practices and other documents that demonstrate the state's implementation program; and
- A certification by the Governor that the state is in compliance with REAL ID

Under the draft regulations, states may use the exception process for:

- Difficulties arising from attempts to verify the birth information for individuals born before 1935, who, due to various considerations, may not have been issued a birth certificate;
- Individuals who have difficulties producing some of the required identification documents, such as address of principal residence; and
- Individuals who have lost their information because of natural disasters such as Hurricanes Katrina and Rita.

The regulations also establish requirements for the exception process. This includes, at a minimum, that:

- The driver record maintained by the DMV must indicate when an alternate document is accepted;
- Any driver's license or identification card issued using exception processing requires a complete record of the transaction, including a full explanation of the reason for the exception, alternative documents accepted and how applicable information from the document was verified; and
- The jurisdiction retains the alternate documents accepted or copies thereof in the same manner as for other source documents as described in the regulations and provides these upon request to DHS for audit review.

Identification Documents and Verification Systems

Under the REAL ID Act, states and territories are required to verify, with the issuing agency, the validity of the identification documents an applicant presents to establish identity; date of birth; proof of social security number or that the person is not eligible for a social security number; the person's name and address of principal residence; and the person's lawful status in the United States. An applicant would have to present at least one of the acceptable documents proposed by DHS:

- a valid unexpired U.S. Passport (approximately 25 percent of Americans hold passports);
- a certified copy of a birth certificate;
- a consular report of birth abroad;
- an unexpired permanent resident card (Form I-551);
- an unexpired employment authorization document (EAD) (Form I-766);
- an unexpired foreign passport with valid U.S. visa affixed;
- a U.S. certificate of citizenship;
- a U.S. certificate of naturalization; or
- a REAL ID DL or ID issued subsequent to the standards established by the regulations.

If an individual's name has changed through adoption, marriage, divorce or other court order, the individual must present an original or certified copy of the document showing a legal name change. The documents must come from a Federal or State Court or government agency. States can have an exception process for individuals who, for reasons beyond their control, are unable to present all necessary documents and must rely on alternate documents to establish identity. An exception process cannot be used to demonstrate lawful status.

The REAL ID Act contemplates that states will need to have access to six national databases in order to verify the validity of the required identification documents. This includes access to:

- Social Security On-Line Verification (SSOLV) -- Almost all states currently use this.
- Department of State -- DHS is working with the Department of State.
- Electronic Verification and Vital Events (EVVE) -- Currently in a pilot phase.
- Systematic Alien Verification for Entitlements (SAVE) -- All 50 states have Memorandums of Understanding (MOUs) for access to SAVE; however, only 20 are currently using it to verify lawful status.
- Student and Exchange Visitor Information System (SEVIS) -- DHS expects a SEVIS-SAVE connection to be in place by May 2008.
- All-State DL/ID Records System -- To be determined.

DHS states in the draft regulations that it is supporting the development of, but will not operate, a federated querying system, where a state could conduct all queries through one portal. State participation will be voluntary. DHS is proposing to leave the operation of this data query, including the development of the business rules, to the states.

DHS proposes to define principal address as, "The place at which a person has been physically present and that the person regards as home; a person's true, fixed, principal and

permanent home, to which the person intends to return and remain even though currently residing elsewhere." DHS recognizes that there is no national database to verify principal address and recommends that each applicant present at least two documents that include his or her name and current principal address. The states will retain the flexibility to determine for themselves which documents or combination of documents an applicant must present and how a state will validate or verify the information. States are required to establish a written policy on this issue, which would be part of a state's initial certification package. Whatever documents states determine to be acceptable, they must contain a street address. Post office boxes and rural route numbers are not acceptable. One exception might be American Samoa as this territory does not use the same type of addresses commonly used in the 50 States. Documents issued monthly cannot be more than three months old at the time of application. Documents issued annually (e.g. property tax records) would need to be for the most current year. Applicants would also be required to sign a declaration affirming that the information they present is true and correct. For minors and other dependents, parents and legal guardians would need to present photo identification (that the DMV would need to verify), and would be required to submit two or more address documents, and sign the affirmation.

DHS anticipates states will be able to verify electronically the issuance of birth certificates though EVVE, which has not been tested nationwide. If such system is not available nationally by May 11, 2008, or a state is seeking to verify the validity of a birth certificate from a state that is not participating in the EVVE system, a state may establish and document its written procedures for how it will attempt to verify the records. At a minimum the applicant's record should contain a notation that the birth certificate was not electronically verified and that verification will be necessary at the next renewal or reissuance, if the information is at that time available for electronic verification.

It is anticipated that a state will be able to verify U.S. passports or consular reports of birth abroad with the U.S. Department of State. Individuals presenting U.S. visas affixed in an unexpired foreign passport would require only a SAVE and SSOLV check.

DHS proposes allowing an applicant to establish their social security number by presenting a social security card, a W-2 form, a SSA 1099, a non-SSA 1099, or a pay stub with the applicant's name and SSN on it. An alien in the United States without authorization to work is generally not eligible for a SSN. In order to prove ineligibility for a SSN, an alien must present evidence that he or she is currently in a non-work authorized non-immigrant status. States will be required to check the validity of the number using SSOLV.

The regulations require a state to maintain a motor vehicle database that contains at a minimum all data fields printed on the driver's license and identification cards, individual serial numbers of the card, and social security numbers; and motor vehicle driver histories, including motor vehicle violations, suspensions and points. States must provide to all other states electronic access to the information contained in the database in a manner approved by DHS pursuant to the regulation. Prior to issuing a REAL ID compliant license, states must check with all other states to determine if any state has already issued a REAL ID driver's license or card to the applicant. The regulations have requirements regarding what steps a state must take if the query confirms that the individuals does hold a REAL ID compliant license in another state. It

has not been determined whether the Commercial Driver's License Information System (CDLIS) or some other service will be the platform for the state-to-state exchange. The draft regulations state that it will be necessary for the states, working with DHS and the Department of Transportation, to define the privacy protections.

Facility Security and Employee Background Checks

Under the REAL ID Act, a state must ensure "the physical security of locations where DLs and IDs are produced and the security of document materials and papers from which DLs and IDs are produced." The proposed regulations would require that a state's comprehensive security plan address:

- the measures taken to ensure the physical security of facilities used in the manufacture and issuance of REAL ID-compliant DLs and IDs;
- the policies and procedures for securing storage areas for materials used to manufacture DLs and IDs; and
- the policies and procedures for securing the databases used to store and access an individual's personal information for the issuance of DLs and IDs;
- the policies and procedures in place to identify and minimize fraud; and
- an emergency/incident response plan if security procedures are violated.

DHS seeks to encourage states to develop collectively best practices for the security of and access to DMV databases. State compliance will be evaluated based upon performance-based standards approved by DHS.

Under the REAL ID Act, a state must ensure that "all persons authorized to manufacture or produce drivers' licenses and identification cards [are subject] to appropriate security clearance requirements." The draft regulations require states, as part of their comprehensive security plans, to conduct background checks for all applicants, employees, and contractors who have the ability to:

- affect the recording of information that must be verified for a REAL ID compliant DL and ID;
- have the ability to affect identity information that is included on a REAL ID compliant DL and ID; or
- are otherwise involved in the manufacture or production of a REAL ID compliant DL and ID.

Each state will determine which applicants, employees or contractors will be subject to the background check. States will also be required to provide notice to the applicant, employee and contractor that a background check will be conducted.

The background check must include:

- a validation of references from prior employment;
- a name-based and fingerprint-based criminal history records check through the state and two FBI's databases—National Crime Information Center (NCIC) and Integrated Automated Fingerprint Identification System (IAFIS) (at the cost of the state);
- a financial history check; and

- a lawful status check (as verified through the Systematic Alien Verification for Entitlements system (SAVE)).

Any "covered" applicant, existing employee or contractor is disqualified from employment if the employee or applicant is convicted of certain felonies. A "covered" applicant, employee or contractor may be disqualified if the person is:

- convicted of a disqualifying offense within 7 years of the application;
- released from incarceration within 5 years of the application; and
- under a felony warrant.

The state may waive the "interim disqualifying criminal offense" through a state documented waiver process. In addition, each "covered" applicant, employee or contractor is subject to a financial history check. However, each state will have the discretion on how to use the financial history check and the financial history check does not disqualify a "covered" applicant or employee from employment.

REAL ID Card Requirements

The REAL ID Act prescribes that a certain set of information and features appear on state-issued DLs and IDs. The law stipulates the following nine as minimums:

- the person's full legal name;
- the person's date of birth;
- the person's gender;
- the person's DL or ID number;
- a digital photograph of the person;
- the person's address of principal residence;
- the person's signature;
- physical security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purposes; and
- a common machine-readable technology, with defined minimum data elements.

DHS proposes to adopt the International Civil Aviation Organization (ICAO) 9303 Standard for the name as it will appear on the face of the DL/ID. This standard requires Roman alphabet characters, allows a total of 39 characters on the face of the card, and provides standards for truncation of longer names. Up to 125 characters of the name must be captured in the machine-readable portion of the card using the proposed PDF-417-2D bar code. Each DL/ID must display a unique card number. As federal law prohibits the display of a person's SSN on a DL, states must generate a different and unique document number. States must capture a full facial color digital image of everyone applying for a DL/ID. If a DL/ID is issued, the image must appear on the face of the card. If a DL/ID is not issued, DHS suggests that states retain the image for one year. Digital photographs should comply with ICAO standards, including diffused lighting over the full face eliminating shadows or "hotspots," a full face image from the crown to the base of the chin and from ear-to-ear, and prohibition of veils, headdresses or eyewear that obscure facial features or the eyes. DHS contends that the law makes no allowances for facial photographs based on religious or other beliefs, but states could use profiles for a DL/ID issued to those under 21 years of age. An applicant's photo should be updated upon reapplication and any prior photos should be discarded in favor of the image associated with the issued DL/ID. If

a state does not issue a DL/ID on suspicion of fraud, DHS requires that the record be maintained for 10 years and note the reason for non-issuance.

The person's address of principal residence must appear on the face of the card. DHS also proposes that state exemption processes for confidential addresses (of judges, victims of domestic violence, protected witnesses, etc.) and applicants with no fixed address be continued. DHS proposes that the person's signature meet the size, scaling, cropping, color, borders, and resolution requirements stated in existing AAMVA standards. DHS is proposing to use the existing AAMVA standard 2D bar code for the machine-readable technology on the card. DHS suggests that the PDF-417 2D bar code approved by AAMVA store the minimum data elements – expiration date, bearer's name, issue date, date of birth, gender, address, unique number, DL/ID format revision date, and inventory control number – necessary to fulfill the purpose of the Act. DHS is encouraging but not requiring encryption of this machine-readable information.

The REAL ID Act requires states to utilize multiple layers of physical security features on a DL and ID that are not reproducible using commonly used or available technologies in order to deter forgery and counterfeiting and to promote an adequate level of confidence in the authenticity of the document. The draft regulations mandate certain security features — such as intricate, fine-line, multicolored background design produced by offset lithography in place of dye sublimation printing; microline printing; an intentional error/field check; an optically variable feature; an ultraviolet (UV) responsive feature; tamper-proof printed information; and covert taggants and/or markers — with a performance standard based on impartial adversarial testing of the card and security features. The card stock must comply with the following performance standards: durability up to an eight-year life span, a controlled UV response, a counterfeit resistant background pattern that avoids enumerated primary colors and typical digital printing technologies, serial numbers with inventory control measures such that missing cards can be recorded and reported to law enforcement, and a format revision date. States must provide DHS with samples of REAL ID compliant DLs and IDs. States must also annually review, via a recognized independent laboratory experienced with adversarial analysis, and report to DHS on the integrity and security of the card.

Non-Compliant and Temporary Cards

Under the REAL ID Act, a state that issues non-compliant REAL ID DLs and IDs must clearly state on the face of the DL/ID that it may not be accepted by any federal agency for federal identification or any other official purpose; and use a unique design or color indicator to alert federal agency and other law enforcement personnel that the DL/ID may not be accepted for any such purpose.

DHS is requiring that the card clearly state on its face, in bold lettering, and in the machine readable zone that it may not be accepted by any federal agency for federal identification or any other official purpose. DHS is also requiring states to incorporate a unique design or color indicator to alert federal agencies and other law enforcement personnel that it may not be accepted for federal purposes. DHS is seeking comment on whether a uniform design/color should be implemented nationwide.

Under the REAL ID Act, a state must issue an individual a temporary DL or ID if that individual provides evidence of lawful status (as verified by SAVE) by presenting one of the following:

- a valid, unexpired nonimmigrant visa or nonimmigrant visa status for entry into the United States;
- a pending application for asylum in the United States;
- a pending or approved application for temporary protected status in the United States;
- approved deferred action status; or
- a pending application for adjustment of status to that of an alien lawfully admitted for permanent residence in the United States or conditional permanent resident status in the United States.

Temporary DLs and IDs must clearly indicate that they are temporary and must state the date on which DL/ID expires. The temporary DLs and IDs may only be valid for the time period of the applicant's authorized stay in the United States. If there is no definite end period for the authorized stay, then the DL/ID shall be good for a period of one year. Under the draft regulations issued by DHS, a temporary DL/ID may be issued to an individual who has temporary lawful status in the United States. The regulations require that a temporary DL/ID is valid:

- for the period of time in which the individual is authorized to stay in the United States (limited to 8 years); or
- for one year (if there is no definite period of time the individual is authorized to stay or is otherwise limited by DHS — asylum applicant, TPS applicant, and adjustment applicant).

In addition, any temporary DL/ID must clearly state on its face in bold and in the machine readable zone of the card that it is a temporary. A state may not reissue a temporary DL/ID unless the document of lawful presence has been extended by DHS or the person has qualified for another lawful status. A renewal of a temporary DL/ID must be in person.

Record Retention

Under the REAL ID Act, states are required to retain copies of source documents for at least seven years and images of source documents must be retained for at least 10 years. Under the regulations, DHS is requiring states to retain either paper or electronic copies of the following source documents:

- signed declaration affirming that the information presented by the applicant is true and accurate;
- an original or certified copy of identity documents or source documents, such as a birth certificate or passport; and
- if applicable, the alternate documents accepted or copies thereof used under a state's exceptions process.

The draft regulations require that states retain paper copies or microfiche copies of source documents for a minimum of 7 years. States that choose to retain a digital image of a source document must retain the image for at least 10 years. In addition, DHS is requiring states using digital image capture to:

- use color imagers on or after December 31, 2011;

- store digital images in a transferable format (the digital storage system must be interoperable with the AAMVA Digital Image Exchange Program);
- store photo images in Joint Photographic Experts Group (JPEG) 2000 format, or standard that is interoperable with this format;
- store document and signature images in a compressed Tagged Image Format (TIF), or a standard that is interoperable with the TIF standard; and
- link all images to the applicant through the applicant's unique identifier assigned by the DMV.

Renewal and Re-issuance Process

The REAL ID Act limits the period of validity of all DL/ID cards that are not temporary to a period that does not exceed eight years. Under the draft regulations, remote renewals will be allowed for REAL ID compliant DL/ID cards if the state has retained images or paper copies of the source documents used to issue the original REAL ID DL/ID card and if no information has changed since the issuance of the REAL ID compliant DL/ID card. Prior to issuing a renewal, states are required to re-verify the identity documents used to issue the original REAL ID compliant DL/ID. DHS is considering how best to authenticate the identity of an individual requesting a remote renewal and is proposing that the state may choose to use personal identifiers such as PIN numbers or questions whose answers only the proper holder would know, or through the use of biometric information. DHS is requesting comments on how best to authenticate remote renewals. A holder of a REAL ID DL/ID card must renew the card in person at least once every sixteen years. The state will be required to re-verify original source documents.

Renewal of temporary licenses issued to certain categories of legal immigrants must be made in person. The person must present valid documentary evidence that the status by which the applicant qualified for the temporary DL/ID has been extended or that the individual has qualified for another lawful status category listed in the act. The renewal process of non-REAL ID compliant DL/ID cards is not subject to the regulation.

Privacy and Civil Liberties

On March 21, 2007, the DHS Data Privacy and Integrity Advisory Committee held a public meeting to discuss the REAL ID regulations. Several groups expressed concern that REAL ID infringes on Americans privacy rights and civil liberties. With regards to privacy, concerns have been raised over the actual data on the card, the ability of third parties to capture and share the data on the card, and the possibility of identity theft based on the sharing of personal information by electronic means and the electronic storage of personal information by the DMV and on the card. Concerns have also been raised that the REAL ID Act violates the Constitution by placing burdens on the right of individuals to travel, assemble, petition the government, and practice their religion.

On March 1, 2007, DHS issued a Privacy Impact Assessment (PIA) on the REAL ID proposed regulations. The PIA noted that the following privacy protections should be further clarified in the final rule: (1) providing for state control and operation of the state query of

federal reference databases and the state-to-state data exchange; (2) requiring states to submit a Comprehensive Security Plan, including a privacy policy and plan to protect the personal information associated with implementation of the Act; and (3) employing encryption to protect the personal information stored on REAL ID driver's licenses and identification cards, while ensuring appropriate law enforcement access. The PIA also noted that these protections are a floor and do not prevent the states from using their own statutory or executive authority to provide additional privacy protections for the personal information stored on the REAL ID credentials and in the state databases.

As of today, 28 states have measures introduced or passed in the state legislature calling for the repeal of REAL ID or to opt out of participating in REAL ID. Maine and Idaho are the only states who have already passed measures to opt out of REAL ID.

LEGISLATION

S. 563, *A bill to extend the deadline by which State identification documents shall comply with certain minimum standards*, introduced by Senators Susan Collins (R-ME), Olympia Snowe (R-ME), Lamar Alexander (R-TN), Thomas Carper (D-DE), and Chuck Hagel (R-NE), and referred to the Committee on Homeland Security and Governmental Affairs.

S. 717, *The Identification Security Enhancement Act of 2007*, introduced by Senators Daniel Akaka (D-HI), John Sununu (R-NH), Patrick Leahy (D-VT), and Jon Tester (D-MT) on February 28, 2007, and referred to the Committee on the Judiciary.

H.R. 1117, *The REAL ID Repeal and Identification Security Enhancement Act of 2007*, introduced by Representative Tom Allen (D-ME) and 16 cosponsors on February 16, 2007, and referred to the House Committee on Oversight and Government Reform and the Committee on the Judiciary.

ADDITIONAL INFORMATION

Final Report of the National Commission on Terrorist Attacks Upon the United States, July 22, 2004, http://www.9-11commission.gov/report/911Report.pdf.

The REAL ID Act: National Impact Analysis, the National Governors Association, the National Conference of State Legislatures, and the American Association of Motor Vehicle Administrators, September 2006, http://www.nga.org/Files/pdf/0609REALID.PDF

REAL ID Scorecard, American Civil Liberties Union, March 2007, http://www.realnightmare.org/images/File/Real%20ID%20Scorecard%20-%20Fed%20Reg%20page%20numbers.pdf.

Privacy Impact Assessment for the REAL ID Act, Department of Homeland Security, March 1, 2007, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_realid.pdf

Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 72 Fed. Reg. 46, (to be codified at 6 C.F.R. pt. 37), March 9, 2007), http://a257.g.akamaitech.net/7/257/2422/01jan20071800/edocket.access.gpo.gov/2007/07-1009.htm

The Real ID Act: National Impact Analysis

Presented by:
National Governors Association
National Conference of State Legislatures
American Association of Motor Vehicle Administrators

September 2006

Executive Summary

On May 11, 2005, Congress passed the Real ID Act (Real ID) as part of the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief Act (P.L. 109-13), creating national standards for the issuance of state driver's licenses (DLs) and identification cards (IDs). The act establishes certain standards, procedures and requirements that must be met by May 11, 2008 if state-issued DL/IDs are to be accepted as valid identification by the federal government. These standards are likely to alter long-standing state laws, regulations and practices governing the qualifications for and the production and issuance of DL/IDs in every state. They also will require substantial investments by states and the federal government to meet the objectives of the act.

To ensure Congress and the federal government understand the fiscal and operational impact of altering these complex and vital state systems, the American Association of Motor Vehicle Administrators (AAMVA) in conjunction with the National Governors Association (NGA) and the National Conference of State Legislatures (NCSL) conducted a nationwide survey of state motor vehicle agencies (DMVs). Based on the results of that survey, NGA, NCSL and AAMVA conclude that Real ID will cost more than $11 billion over five years, have a major impact on services to the public and impose unrealistic burdens on states to comply with the act by the May 2008 deadline. The organizations also provide practical and cost effective solutions for Congress and the Department of Homeland Security (DHS) to address these shortcomings and meet the objectives of the act.

PROCESS

In February 2006, NGA, NCSL and AAMVA provided a section-by-section analysis of Real ID to DHS that identified several critical issues for states and made recommendations on the most feasible means to implement the law.

The organizations followed that report with detailed surveys of DMV officials to estimate the potential costs of the legislation. The surveys included approximately 114 multi-part questions and required 6-8 weeks to complete. Since DHS has yet to publish regulations to guide state estimates, the surveys relied on the earlier state recommendations and information from ongoing discussions with the federal government to establish baseline assumptions. Responses were completed by 47 of 51 polled jurisdictions representing 89.6% of all state issued DL/ID cards.

The findings contained in this report have likely underestimated the full impact of Real ID. Costs could escalate significantly if federal regulations differ substantially from the recommendations states used to form baseline assumptions. Lacking regulatory guidance, states were unable to estimate several elements of the act that will almost certainly contribute additional cost and administrative burdens to the compliance process including:

- facility security requirements;
- development of federal verification systems and transaction costs;
- expansion of the AAMVAnet system to support additional verification connectivity requirements;
- law enforcement training and technology deployment;
- expanded public education/data privacy protection; and
- increased customer demand/care/advocacy.

KEY FINDINGS

Real ID will cost more than $11 billion to implement. One time upfront costs approach $1 billion, while ongoing costs total more than $10.1 billion over the first five year period.

- **Re-enrollment** **$8.48 billion**
  States based their analysis on the assumption that to implement Real ID, all 245 million U.S. DL/ID holders must be re-credentialed within five years of the May 2008 compliance deadline. This standard will require an in-person visit by every current DL/ID holder as well as new applicants to review and verify all required identification documents and re-document information for the new license including place of principal residence, new photographs and new signatures. Efficiencies from alternative renewal processes such as Internet and mail will be lost during the re-enrollment period, and states will face increased costs from the need to hire more employees and expand business hours to meet the five year re-enrollment deadline.

- **New Verification Processes** **$1.42 billion**
  Real ID supplants traditional DMV vetting processes by requiring states to independently verify each identification document with its issuing agency. While the act contemplates the use of five national electronic systems to facilitate verification, currently only one of these systems is available on a nationwide basis. System development, programming, testing and training will take considerable time and investment that far exceed the deadlines or funds provided by the act or Congress.

- **DL/ID Design Requirements** **$1.11 billion**
  The act calls for states to incorporate security features into DL/ID cards to prevent tampering and counterfeiting. Although most states have incorporated security features into their card designs, the contemplated regulations are likely to mandate the use of a single security configuration that will maximize cost by minimizing state flexibility in card design and production. Depending on the technology chosen, such a requirement could dictate DMV business practices by effectively requiring DMVs to move away from over-the-counter issuance systems and toward central issuance systems.

- **Support Costs** **$0.04 billion**
  Real ID contains several other requirements that will affect state business practices and budgets including requirements to conduct security clearances on all employees involved in the production and issuance process and mandatory fraudulent document recognition training.

Real ID will reduce efficiencies and increase wait times for citizens. To comply with the requirement that all DL/ID card holders re-verify their identity with the state, individuals must gather and present all their identification documents, which may more than double the length of time they spend at their DMVs. Real ID will also effectively reverse state practices designed to ease an applicant's interaction with motor vehicle agencies (e.g., Internet, mail in renewal, over-the-counter issuance).

MAJOR RECOMMENDATIONS

Governors, state legislators and motor vehicle administrators are committed to improving the security and integrity of state DL/ID systems, but the timelines and requirements mandated by REAL ID are unrealistic. In order to meet the objectives of the act, Congress and DHS should at a minimum incorporate the following recommendations into the law and any final regulations[1]:

- **General**
  - **Extend the compliance deadline.**
    It will be impossible for states to comply with Real ID by the May 2008 deadline. DHS has yet to issue regulations and most of the major systems necessary to comply do not exist.

  - **Provide funds necessary for states to comply with Real ID.**
    As this report indicates, the projected cost of complying with the act far exceeds the Congressional Budget Office estimate and will require a more significant investment by Congress.

  - **Grant the Secretary of Homeland Security the flexibility to recognize innovation at the state level.**
    Several states have updated their systems to meet objectives similar to those of Real ID. The Secretary of Homeland Security should have the discretion to recognize state practices and innovations that accomplish the goals of the act.

- **Re-enrollment**
  - **Implement a 10-year, progressive re-enrollment schedule.**
    It is impracticable for states to renew all 245 million DL/IDs in five years. States should be given the flexibility to delay re-verifying certain populations in order to maximize resources and avoid severe disruptions to customer service.

  - **Allow reciprocity for persons already vetted by the federal government.**
    States could realize significant savings and reduced transaction time if individuals whose identity has already been verified for certain federal identification cards are considered pre-qualified for a Real ID compliant DL/ID.

- **Verification**
  - **Provide the federal electronic verification systems necessary to comply with the law.**
    Only one of the five national electronic systems required to verify identification documents is fully operational. It will take considerable time and testing for the federal government to update its systems to meet the information requirements of the act.

[1] Additional recommendations are included in the Impact Analysis section of this report and the February 2006 NGA, NCSL, AAMVA section-by-section report.

- **Require states to employ electronic verification systems only as they become available.**
  Until electronic systems are fully operational, states must be allowed to use existing verification processes to comply with the act.

- **Adopt uniform naming conventions to facilitate electronic verification between files.**
  An individual's name is a person's most common identifier. For electronic systems to work seamlessly, the federal government must adopt and universally apply common naming conventions to its systems.

- **DL/ID Design Requirements**
  - **Establish card security criteria based on performance—not technology.**
    Limiting states to a single technology configuration increases risks and reduces innovation.

CONCLUSION

Governors, state legislators, motor vehicle administrators and federal officials share the goal of improving the security of state-issued DL/ID cards and the integrity of the issuance process.

As evidenced by this analysis, the Real ID Act presents significant operational and fiscal challenges to states and the federal government. Officials at all levels of government must also recognize the personal impact Real ID will have on individual citizens. The four major categories described in this report represent the most critical challenges facing states and consumers as the act's implementation deadline approaches. Even with full funding and aggressive state implementation plans, however, the difficulties of complying with yet unpublished regulations by the statutory deadline of May 2008 are insurmountable.

Our organizations strongly believe the recommendations presented here offer reasonable and workable alternatives to help states meet the objectives of Real ID. It is our intention to work towards implementation of the act in a cost-effective and reasonable manner. Governors, state legislators and motor vehicle administrators encourage DHS to adopt regulations and Congress to pass legislation that incorporates the recommendations of this report. We also urge Congress to appropriate sufficient funds to allow states to implement the act. The objectives of Real ID are laudable, but only by working together will state and federal governments succeed in meeting the challenges presented by Real ID.

Impact Analysis

The following analysis details the effects of the Real ID Act (Real ID) on states, state licensing systems and individual driver's license and identification card (DL/ID) holders. The analysis is organized by the four major requirements that will have the greatest affect on states: re-enrollment, verification, DL/ID design and support requirements. The findings in each section are based on responses by state motor vehicle administrators to a survey sponsored by the American Association of Motor Vehicle Administrators (AAMVA) along with the National Governors Association (NGA) and National Conference of State Legislatures (NCSL).

1. Re-Enrollment

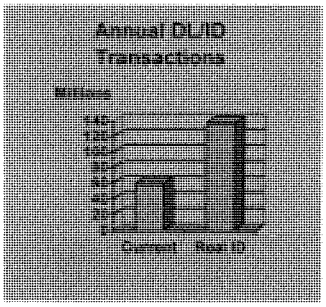
$8.48 billion
Over 5 years

The Real ID Act will require all applicants to present their original identification credentials in person in order to be issued a Real ID compliant driver's license or identification card. More than 245 million existing cardholders and all new applicants must obtain and provide original identification documents to their state licensing agency for electronic verification and the scanning and storing of images before a Real ID compliant DL or ID card may be issued.

Findings

Federal officials have indicated they likely will require states to re-enroll all DL/ID card holders over a five-year period. This requirement will place an onerous fiscal and operational burden on states. States estimate the five-year re-enrollment cost at more than $8.48 billion, which represents 71% of the total estimated known cost for implementing Real ID.

The primary cost drivers behind re-enrollment are the amount of additional time and resources required to re-enroll all DL/ID card holders over a five year period. Prior to Real ID, states anticipated handling more than 295 million DL/ID issuance transactions over the next five years.[2] Of those, nearly 38 million (13%) would have been original issuance transactions, which typically require an individual to appear in person and produce three to four identification documents. The remaining 257 million transactions (87%) would have been renewals—32 million of which would have taken place through alternative channels such as mail, Internet, and kiosk services. The typical in-person renewal takes one-half the time of an original issuance, while alternate renewals take one-fourth the time.



New Real ID requirements will more than double the workload of state motor vehicle departments (DMV) by increasing the number of individuals who must appear to renew their licenses and the time it takes

[2] States' re-enrollment analysis is limited to original and renewal transactions only and does not include approximately 21 million annual DL/ID transactions such as requests for duplicates, replacements or reinstatements.

to complete each transaction. Twenty-four states with existing renewal periods greater than five years will need to accelerate their renewal process to meet the new deadline. Because of this change DMVs will need to service nearly 30 million additional individuals during the next five years. Per-person transaction times will increase because every renewal will be processed as an original issuance, requiring an in-person visit and the production and verification of identification documents. The net effect of these changes will be to increase DMV workloads by 132.4% and more than double transaction times for renewals of existing DL/IDs.

The increased workload attributed to re-enrollment will also exceed the existing capacity of most state licensing agencies. A majority of states indicate they are operating at full capacity to meet existing demand. If states are to maintain their present levels of service while incorporating the added transaction volumes mandated by Real ID, states will need to:

- hire additional employees and increase service hours;
- expand or increase the number of facilities to accommodate additional customer volume;
- purchase additional equipment to support personnel;
- create and implement public education campaigns to inform customers; and
- anticipate and handle increases in calls, complaints, and return visits due to confusion and adjustments resulting from the new requirements.

Re-enrollment alone will require significant investments in DMV systems, personnel and facilities. However, even if full funding were provided, meeting the five-year re-enrollment deadline would result in severe customer service disruptions due to the increase in annual transactions. Providing states with flexibility to manage enrollment over a greater length of time would still meet the objectives of the act while reducing the fiscal effect on states and minimizing service disruptions for customers.

Recommendations

- Adopt a progressive re-enrollment period of at least 10 years. Currently, 24 states have a renewal period longer than five years. Extending the re-enrollment period beyond the proposed five-year period would negate some costs relating to expanding capacity and allow the remaining cost to be spread over a longer period of time.
- Allow for alternative renewal processes to continue during the re-enrollment period, provided existing customer data can be validated before issuance. This approach could include comparison of each existing Social Security number to the DMV's complete data file and Social Security Administration file, as well as comparison of each photograph against the complete photo file for that state.
- Allow for a waiver of verification requirements to facilitate applicants who have already been through an identity vetting process by the federal government (e.g., military ID, federal employee credential, transportation worker identification credential, U.S. passport.)
- Allow applicants with valid and compliant Real ID document(s) to transfer state-to-state without further documentation other than proof of residence, provided critical information has not changed. The previous state of record must transfer the applicant's record and image files to allow this provision to be acceptable.

- Exempt segments of applicants based on certain requirements related to applicable risk such as year of birth or duration of continuous relationship with the state of licensure.

2.New Verification Processes

$1.42 billion
Over 5 years

Verification processes comprise the second largest category influencing Real ID implementation costs, accounting for approximately 12.8% of the $11 billion known costs—or a total of $1.42 billion over 5 years. The largest contributing factor is the more than 2.1 million computer programming hours states will need to adapt their systems for new requirements involving eligibility verification, business process re-engineering, photo capture and database design.

2.1 Verification of Eligibility: $408 million

The Real ID Act requires DMVs to independently verify the validity of an applicant's identification documents with the appropriate issuing agency. This requires states to be able to contact all issuers of birth certificates and other name records, the U.S. Citizenship and Immigration Services, the U.S. State Department, the Social Security Administration and every other state motor vehicle administration prior to issuing a Real ID.

Findings
Confirming the validity of an identification document with the issuing agency will be one of the most expensive requirements of Real ID. Because DMVs will need to verify at least three identification documents for each applicant, states can anticipate processing more than 1 billion verification transactions over the next 5 years. In addition, the Real ID verification process also requires new conventions for capturing full legal name, processing photos and signatures, determining lawful presence and retaining images of identification documents.

Verification costs are expected to exceed $408 million over five years. Of this amount, $129 million is for one-time costs primarily related to states establishing connections with verification systems once they are made available. The remaining $278 million is for ongoing operational costs during the five-year enrollment period. These estimates do not include transaction fees that may be required for states to access these systems or the cost of developing and maintaining required information systems.

Compliance with the eligibility verification requirement is contingent on the completion and implementation of at least five national identity verification systems and the necessary time for states to complete the required systems integration. States anticipate spending more than $400 million, primarily in programming hours, to design, connect and test their issuance systems once the verification systems are available to states. Complicating these efforts will be the need to comply with state and federal procurement requirements, system security measures and data privacy laws.

The five verification systems are:

1. **All-State DL/ID Records System**—A system is necessary to ensure an applicant is not already licensed in another state or fraudulently holding multiple DL/ID cards. Such a system could be modeled after the existing Commercial Driver's License Information System (CDLIS), which supports verification requirements for all

commercial drivers. It also is necessary to verify the validity of an existing Real ID DL/ID card should that be submitted as proof of identify in another state.

2. **Department of State**—While the Department of State U.S. Passport database already includes birth records of U.S. citizens born overseas, there is no way for states to access this information. Implementation of the Real ID Act would require the Department of State to define the requirements for such a system, construct the system and test and work with the states to make it available for deployment prior to the May 2008 deadline.

3. **EVVER** (Electronic Verification of Vital Events Records)—States have worked with AAMVA to pilot the EVVER system to verify birth information. The pilot does not involve all states and does not include information concerning marriage, divorce and death records. In addition, the system is still in its early development stage.

4. **SSOLV** (Social Security On-Line Verification)—Currently 46 states have the ability to verify applicants' Social Security numbers with the Social Security Administration.

5. **SAVE** (Systematic Alien Verification for Entitlements)—Initially this system was created to verify eligibility for federal benefits. The system will have to be retrofitted to fulfill its expanded role under Real ID. At least 21 states currently are using SAVE or are in the process of gaining access to the system.[3] Once the system is constructed, all jurisdictions would need time to test and certify the system before the May 2008 deadline.

Recommendations

- To utilize all funding possibilities more efficiently, the U.S. Department of Transportation's Federal Motor Carrier Safety Administration (FMCSA) and DHS should coordinate and re-assess their approach to funding implementation of Real ID requirements.

- Prohibit federal agencies from charging transaction fees to the states for the required electronic verification of federal information.

- Establish a cooperative effort between the DMVs, the National Association for Public Health Statistics and Information Systems (NAPHSIS), and state vital records agencies to provide reliable data and acceptable fees related to the verification of birth, marriage, divorce and death information.

- To ensure the successful implementation of verification systems supporting Real ID, it is imperative for states to be required to employ electronic verification systems only as they become available.

- Consolidate and synchronize system development schedules in a cooperative effort to maximize resources, ensure system efficiency and minimize the impact on state and federal systems.

---

[3] States have indicated a preference to utilize the AAMVAnet environment to accomplish this verification. AAMVAnet is a secure network connecting 51 motor vehicle agencies (and their various legacy systems). It currently supports CDLIS and other highway safety systems. The motor vehicle agencies already access SSOLV through AAMVAnet.

2.2 Record system: $48 million

Electronic verification processes will require states to record verification results and make that information part of the driver history record.

Findings
Record system changes will cost approximately $48 million over five years. Many states will need time to seek legislative changes, solicit and award contracts and make system upgrades. Of the $48 million, $30.9 million is for one-time implementation costs and $17.3 million is for total ongoing costs over the five years.

Currently, states are not required to capture or store verification information. System changes will be required for states to be able to capture, store and share information, photos and signatures with other states. States must also be able to share applicants' identity information with other relevant state and federal systems for law enforcement purposes. One of the most significant impacts to record systems is increasing the number of characters to accommodate a full legal name. Currently, there is a considerable variance in name formats and character allowance between states. (For more information on requirements regarding the use of full legal name, see 2.5)

Twenty-one states report investing $289 million over the last five years to modernize their DMV information systems. To become Real ID compliant, many of these investments will be lost and systems will need to be modified to store data required by Real ID.

2.3 Photo Capture: $248 million

Real ID requires a mandatory facial image capture for each person applying for a DL/ID card. This differs from existing practices that capture only images of those who ultimately are issued a DL/ID card.

Findings
Capturing images of all applicants will require states to take photos at the beginning of the licensing process. Only seven states currently capture photos at the beginning of the process. To change state practices requires modifications with a projected cost of $248 million over five years, which includes $72.3 million in one-time costs for items such as equipment and software and $175.9 million in total ongoing costs.

Currently all states capture photos as part of their normal issuance process. Laws in 32 states, however, allow exceptions for individuals such as religious objectors, overseas military personnel and persons who are unable to visit a service center due to physical disabilities.

This projected cost does not include facial imaging recognition software to compare captured images with existing images in any state database. Although photo capture of all applicants is a useful tool, its effectiveness is diminished greatly without a significant investment in facial recognition technology.

Recommendation

- As long as a facial image is captured when a credential is issued and before a credential is denied, states should be provided the flexibility to engineer their system and business processes.

2.4 Lawful Presence: $95 million

Real ID requires non-citizens to present evidence of lawful presence in the United States before states issue a Real ID credential. Therefore, states must verify the validity of the documents presented to prove lawful status in addition to all other required information (i.e., name, date of birth, Social Security number and address.) In addition, the expiration date on the DL/ID card must coincide with the end of the applicant's authorized stay. If the length of stay is indefinite, the DL/ID card must be renewed on an annual basis. Regardless of a state's renewal cycle, the expiration date of the DL/ID card for non-citizens must expire the same day as the end date on the presented immigration document.

Findings

Lawful presence accounts for approximately $95 million of the known implementation costs over the five-year enrollment period. This amount includes $65.5 million in one-time costs and $29.6 million in total ongoing costs.

According to federal statistics from 2005, more than 11 million[4] unauthorized immigrants are in the United States, as well as an estimated 32 million nonimmigrants[5]—those here on a temporary business or visitors visa. Tying the expiration date of DL/ID cards to the end dates on the presented immigration document will increase the total number of required transactions and necessitate new system requirements.

In states that require lawful presence as a condition for obtaining a DL/ID card, state officials must review numerous complex documents to properly determine immigration status. Currently, 21 states have access to, or are in the process of gaining access to, DHS's SAVE system to electronically verify lawful presence. However, insufficient information is available for states to reliably identify and validate an individual's "pending" immigration status. States also report real-time verification is not attainable approximately one-quarter of the time, which necessitates a time-consuming process to meet this requirement. Improved SAVE functionality is necessary to effectively implement this requirement.

Recommendations

- Limit the acceptance of the foreign documents to official passports accompanied by appropriate and clearly defined U.S. immigration documents.
- Limit document verification to what can be accomplished through an enhanced SAVE program that is fully developed, operational in real-time and accessible to all jurisdictions at no cost to states.
- DHS should establish a state working group to ensure the appropriate use of the SAVE system for purposes of this act.

---

[4] Office of Immigration Statistics, Department of Homeland Security, *Estimates of the Unauthorized Immigrant Population Residing in the United States: January 2005, (Washington, D.C.: DHS, 2005).*

[5] Office of Immigration Statistics, Department of Homeland Security, *Temporary Admissions of Nonimmigrants to the United States: 2005, (Washington, D.C.: DHS, 2005).*

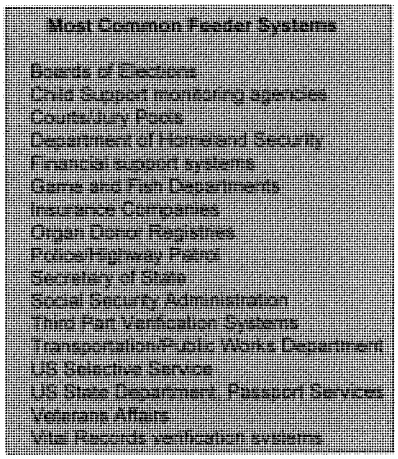
- Expand the SAVE database to include Certificates of Naturalization.
- SAVE operability must allow for reliable real-time response in a high-volume hub-based query environment, which can be integrated into DMV transaction processes similar to SSOLV.
- Provide states time to pass legislation to require lawful presence for the issuance of a Real ID-compliant DL/ID, synchronize the DL/ID card expiration date with the authorized end-of-stay date and train employees to verify lawful presence through the SAVE system.

2.5 Full Legal Name: $242 million

Real ID requires each state to include a person's "full legal name" on a Real ID-compliant credential. DHS is considering requiring a name field that would capture between 125 and 175 characters.

Findings

The name is a critical data element used by states to collect, record, store, display and match identification data. Collecting and linking all name variations (e.g. William, Will, Bill) is necessary to prevent the issuance of multiple licenses and identification cards as various events may affect the base name record (e.g., adoption, marriage, divorce, court orders).



Currently, state databases capture anywhere from 27 to 125 characters for the name field. Only six states reported meeting the 125 character requirement.

The full legal name requirement would cost $242 million over five years, which includes $186 million in one-time system costs and $56 million in ongoing costs. Over 1.1 million required programming hours are the primary driver of these costs, along with interface changes and testing. Additional unmeasured costs could be significant since state databases interface with numerous other systems, known as feeder systems, which may also need to be changed.

Costs also may be incurred from the need to change documents, forms and related fields to accommodate full legal name requirements. Reconciling truncation practices when states have to reduce a full legal name of up to 125 characters in its database down to the 39 characters available on the front of the DL/ID is also a major concern to states.

Recommendations

- Common conventions for the full legal name must be defined and universally applied to all federal document issuers for this requirement to be effective.

- Truncation guidelines should be developed with input from states and applied to all systems accessed for Real ID.

2.6 Address of Principal Residence: $200 million

The Real ID Act requires states to verify and include an address of principal residence on the DL/ID card.

Findings

This requirement presents states with a significant challenge as there is no defined standard for principal address that can be used on the DL/ID card. A consequence of America's mobile society is frequent relocations and ownership of multiple properties and mobile homes, which may not include a permanent address.

Address changes are a normal, frequent occurrence and constitute the largest number of driver record change transactions. Many states accommodate this volume through address changes in their record systems without requiring the issuance of a replacement DL/ID card until the next scheduled renewal. Since this is one of the most common changes made to an individual's DL/ID between renewal cycles, a requirement to re-verify address change documents will significantly increase in-person visits.

The $200 million to implement the principal address requirement over five years includes $53.7 million in one-time costs and $146.8 million in ongoing costs. Primary cost factors include the redesign of forms and changes to business process to verify addresses and enter them into the database.

All states retain at least one address in each motor vehicle record, but there is a wide variety of protocols used. Six states do not utilize a standard protocol, and 25 states allow masking—the option of not printing the address of principal residence on the card—for persons in protected classes (e.g., law enforcement purposes, judges, victims of domestic violence).

Recommendations

- Address of principal residence should be determined by having the applicant provide an affidavit and corroborating documentation.
- "Masking" of an address should be permitted on the credential for persons in certain protected classes while securely retaining the information in the database.
- States should be allowed to propose interim methods of tracking address changes between renewal cycles without the requirement for the full issuance of a replacement credential.

2.7 Records Retention: $175 million

The Real ID Act requires states to retain copies of identification documents for a minimum of seven years or images of source documents for a minimum of 10 years.

Findings

Record retention accounts for approximately $175 million over the five-year enrollment, with $64.5 million coming from one-time costs and $110.2 million attributable to ongoing costs. This does not include additional costs states would face if required to capture and

store documents presented to verify address of principal address or the cost of record storage over the life of a valid Real ID-compliant DL/ID.

On average, states utilize three or four identification documents to process name, date of birth, Social Security number and lawful presence status. States will be required to capture images of more than 1 billion identification source documents over the five-year enrollment period. Twenty-two states plan to save digital images separately, rather than integrating them with their motor vehicle record systems.

States also expressed concern regarding the application of the Drivers Privacy Protection Act (DPPA) to the records retention and information sharing requirements of Real ID. The DPPA is a federal law that regulates how a DMV releases and shares the information in DMV records. DPPA forbids states from distributing personal information to direct marketers, but allows sharing of personal information with law enforcement officials, courts, government agencies, private investigators, insurance underwriters and similar businesses.

Recommendations

- The federal government must reconcile the new requirements of Real ID with the existing Driver Privacy Protection Act (DPPA) (18 U.S.C. Sec. 2721, et. sec.) to reflect the new responsibilities of DMVs and advances in technology since the DPPA was passed.
- States should not be required to capture documents presented by an applicant to verify address of principal residence.

3.DL/ID Design Requirements

$1.1 billion
Over 5 years

The Real ID Act requires states to incorporate security features into the DL/ID card to prevent tampering, counterfeiting or duplication for fraudulent purposes.

3.1 Security Configuration: $1 billion

The regulations likely will specify a uniform security configuration that prescribes a single substrate or cardstock and set of security features for use on all DL/ID cards issued by U.S. jurisdictions.

Findings
Protecting the DL/ID card from tampering, counterfeiting or fraudulent duplication is essential to improving the overall security of DL/ID cards nationwide. However, requiring one single acceptable configuration will limit jurisdictions' ability to adapt to changing threats in their particular environment and may drive up costs unnecessarily. Although it is not realistic to expect significant improvements to be made while keeping the cost per card at or near current levels, improving the level of security for the DL/ID card can be achieved at significantly less cost than a single stringent configuration.

While the anticipated regulations will likely provide a good security configuration based on currently available technology, restricting all state-issued DL/ID cards to a single security configuration could introduce new security vulnerabilities rather than protect the DL/ID card against fraud. States recognize the risk of relying on a single technology and now include provisions in their card security contracts that call for periodic re-evaluations of their document security configuration and allow for changes in design when needed. Such re-evaluations provide opportunities to alter configurations that have been copied or simulated and adopt new technologies that provide superior or more cost effective performance. If all DL/ID cards have the same basic configuration, counterfeiters will only need to overcome one configuration to be able to counterfeit any jurisdiction's card. DL/ID cards would be more secure if states are given the flexibility to use multiple security technologies, thereby forcing counterfeiters to overcome multiple and different technologies in each jurisdiction.

A single card configuration is also likely to maximize cost by mandating a certain technology and forcing all states to alter existing systems. No state currently employs the security configuration contemplated by DHS. Mandating a new technology will require significant investments in new production systems and training that will force states to move to central issuance systems to reduce start-up costs and eliminate over-the-counter issuances. A single technology will also reduce the ability of states to choose between competing security technologies and make cost effective purchases.

States' estimate the five-year cost to implement the proposed security requirement at $1 billion. These costs include $237 million in one-time costs and $767 million in total ongoing costs.

Recommendations

- Promulgate regulations that establish performance requirements for DL/ID cards rather than mandating use of a specific set of security features.
- Initiate an advisory group composed of document security experts from federal and state agencies to establish national performance criteria.
- Create a testing program in cooperation with states to determine the resistance of DL/ID cards to tampering, counterfeiting or duplication for fraudulent purposes.

3.2 Non-Conforming DL/ID Card: $68 million

Real ID requires DL/ID cards that do not satisfy federal requirements to state clearly on the face of the card that it may not be accepted by any federal agency for identification or any other official federal purpose. The DL/ID card must use a unique design or color indicator to alert a federal agency or official that it may not be accepted for any such purpose.

Findings

Eleven states indicated they may offer non-conforming DL/ID cards as permitted by the act. Design of non-conforming cards will cost those 11 states an estimated $68 million to incorporate language and color requirements. These costs include $14 million in one-time costs and $54 million in total on-going costs over five-years. A majority of this cost stems from programming hours associated with system design and testing. In addition, some states will incur increases in fees to outside vendors and costs for on-going equipment replacements.

Recommendation

- Allow states to meet the requirement at reduced cost by placing a restriction code on the front of license, with clarifying language on back.

4. Support Costs

$44 million
Over 5 years

4.1 Fraudulent Document Recognition Training: $33 million

The Real ID Act requires states to establish fraudulent document recognition training programs for designated employees engaged in the issuance of DL/ID cards.

Findings
Fraudulent document recognition training is a critical component of securing the DL/ID issuance process. Forty-one states currently conduct fraudulent document recognition training programs. Of these, 34 states use AAMVA's Fraudulent Document Training program. Many states are concerned that training cost could increase significantly if DHS does not recognize these existing state training programs.

Meeting the requirements of the act could require more than 35,000 existing employees, and all new hires, to receive 12 hours of level one fraudulent document training. Of these, 10,000 employees who serve in supervisory roles will require level two advanced fraudulent document recognition training. In addition, all certified employees must attend an annual four-hour re-certification class.

Fraudulent document recognition training will cost states $12.6 million in the first year of Real ID compliance and $20.4 million in total on-going costs over the five-year enrollment period. The primary costs for the training program are class fees, facility costs, instructor salaries, materials and providing coverage for front-line employees while they attend training.

Recommendation
- The regulations should allow the current AAMVA fraudulent document recognition training program to be used to meet the act's requirements.

4.2 Employee Background Check: $8 million

The Real ID Act requires states to conduct appropriate security clearance background investigations on all people authorized to manufacture or produce driver's licenses and identification cards.

Findings
To meet this requirement, states will incur costs of approximately $4.32 million in the first year of Real ID compliance and $3.55 million in total on-going costs over five years. This does not include security clearances required for employees of vendors and suppliers, which likely will be passed on to states through increased contract costs.

Most states that undertake background checks only perform them at the time of hiring. Of the 29 states that currently carry out some level of employee background checks, only two conduct credit checks.

In addition, this requirement will have a significant effect on many states' labor contracts. Numerous employees were hired under terms and conditions not requiring a security clearance. Should these employees be disqualified under the new regulations, states may be obligated to provide them with alternative employment or severance. States could also face additional costs associated with recruiting, hiring and training replacement employees.

Recommendation

- Provide states maximum flexibility to implement the regulations in a manner that is specific to the needs of their jurisdiction and avoids unnecessary confusion and disruption in services.

4.3 Certification: $3 million

Real ID requires the secretary of the DHS to determine every three years whether a state is meeting the requirements of the act.

Findings

Certification will cost $3 million over the initial five-year implementation period. For the purpose of this survey, DMVs used the costs and time associated with the Commercial Driver's License (CDL) certification process to extrapolate estimated costs for the Real ID certification process.

Successful implementation of Real ID will depend on the flexibility afforded states through the secretary's use of authority to extend deadlines for non-compliance. Additional authority may be needed to allow the secretary to recognize state innovations and practices that meet the objectives of Real ID, but differ from mandated requirements.

Recommendations

- The secretary must employ reasonable use of the extension authority to allow successful implementation of the act and recognize state flexibility.
- Extensions must be granted consistently; when a legitimate reason for extension exists for one state, it should apply equally to all states.
- Provide the secretary with the authority to recognize state innovations and practices that meet the objectives of Real ID.
- Provide states ample opportunity for review and appeal of decisions regarding their self-certification.

Conclusion

Governors, state legislators, motor vehicle administrators and federal officials share the goal of improving the security of state-issued DL/ID cards and the integrity of the issuance process.

As evidenced by this analysis, the Real ID Act presents significant operational and fiscal challenges to states and the federal government. Officials at all levels of government must also recognize the personal impact Real ID will have on individual citizens. The four major categories described in this report represent the most critical challenges facing states and consumers as the act's implementation deadline approaches. Even with full funding and aggressive state implementation plans, however, the difficulties of complying with yet unpublished regulations by the statutory deadline of May 2008 are insurmountable.

Our organizations strongly believe the recommendations presented here offer reasonable and workable alternatives to help states meet the objectives of Real ID. It is our intention to work towards implementation of the act in a cost-effective and reasonable manner. Governors, state legislators and motor vehicle administrators encourage DHS to adopt regulations and Congress to pass legislation that incorporates the recommendations of this report. We also urge Congress to appropriate sufficient funds to allow states to implement the act. The objectives of Real ID are laudable, but only by working together will state and federal governments succeed in meeting the challenges presented by Real ID.

TABLE 1: REAL ID IMPLEMENTATION COSTS

	One Time Costs	On-going Costs for 5 year period	Total Five-Year Cost
1. Re-Enrollment			
Re-Enrollment	N/A	$8,481,299,660	$8,481,299,660
Subtotal	**N/A**	**$8,481,299,660**	**$8,481,299,660**
2. New Verification Processes			
2.1 Verification of Eligibility	$129,188,744	$278,316,015	$407,504,759
2.2 Record Systems	$30,961,607	$17,283,505	$48,245,112
2.3 Photo Capture	$72,350,410	$175,851,005	$248,201,415
2.4 Lawful Presence	$65,456,640	$29,549,065	$95,005,705
2.5 Full Legal Name	$185,700,476	$56,041,958	$241,742,434
2.6 Address of Principal Residence	$53,743,884	$146,783,173	$200,527,057
2.7 Records Retention	$64,545,738	$110,214,475	$174,760,213
Subtotal	**$601,947,499**	**$814,039,196**	**$1,415,986,695**
3. DL/ID Design Requirements			
3.1 Security Configuration	$270,186,383	$767,454,973	$1,037,641,356
3.2 Non-Conforming DL/ID Card	$14,227,981	$53,973,695	$68,201,676
Subtotal	**$284,414,364**	**$821,428,668**	**$1,105,843,032**
4. Support Costs			
4.1 Fraudulent Document Training	$12,634,712	$20,627,105	$33,261,817
4.2 Employee Background Checks	$4,320,983	$3,546,178	$7,867,161
4.3 Certification	$1,106,384	$1,475,177	$2,581,561
Subtotal	**$18,062,079**	**$25,648,460**	**$43,710,540**
Grand Total	**$904,423,942**	**$10,142,415,984**	**$11,046,839,927**

Table 2: Re-enrollment

Real ID Enrollment	BEFORE: 5-year Transactions without Real ID	Real ID Impact: Increased transactions due to accelerating renewals for states with expirations periods longer than five years	Real ID Impact: 100% increase in equivalent in-person renewal transactions due to full vetting taking twice as long as renewals	Real ID Impact: 300% increase in equivalent alternative channel transactions due to full vetting taking four times as long	AFTER: 5-year Equivalent Transactions With Real ID
Original Issuance Transactions	37,871,139				37,871,139
In Person Renewal Transactions	225,733,093		225,733,093		451,466,186
Alternative Channel Renewal Transactions	31,665,468			94,996,403	126,661,871
Real ID Impact: Increased in-person renewals due to accelerating longer expirations into five years		24,630,241	24,630,241		49,260,482
Real ID Impact: Increased alternative channel renewals due to accelerating longer expirations into five years		5,202,024		15,606,071	20,808,095
Total Transactions	295,269,700				686,067,773
Percent Growth					132.4%
5-year budget for License/ID transactions	$6,408,094,050				$14,889,393,720
Increased budget impact for REAL ID re-enrollment (base budget x percent increased "equivalent" transactions)					$8,481,299,670

REAL ID ENROLLMENT TRANSACTION IMPACTS			
Real ID Acceleration	29,832,265	7.63%	$647,435,069
Real ID Full Process in lieu of renewal	250,363,334	64.06%	$5,433,513,133
Real ID Loss of Alternative Channels	110,602,474	28.30%	$2,400,351,469
TOTAL	390,798,073	100.00%	$8,481,299,670

Table 3: Data on State Issuance of DL/IDs (Spring 2006)

Data Topic	TOTAL	States With Less Than 2 Million DL/IDs	States With Between 2 and 5 Million DL/IDs	States With More Than 5 Million DL/IDs
# of states	51 States	17 States	17 States	17 States
# of Valid DL/ID Records				
DL	207,950,328	12,259,106	51,670,390	144,020,832
ID	37,266,029	1,925,578	7,636,709	27,703,742
Total	245,216,357	14,184,684	59,307,099	171,724,574
Annual Volume Totals				
Annual total of DL original and renewal transactions	59,053,940	4,558,299	15,836,602	38,659,039
States Issuance Processes				
# of states that have central issuance	16	6	3	7
# of states that have over the counter issuance	31	10	13	8
Alternative Issuance Methods				
Combined issuance total	9,360,408	107,158	866,141	8,387,109
% of states that provide alternative issuance	85%	88%	82%	88%
% of total DL/ID issuances	12%	2%	4%	15%
Maximum Valid Issuance Term				
DL issuance > 8 years for at least some populations	3	0	2	1
ID issuance > 8 years for at least some populations	10	2	4	4
DL issuance > 5 years for at least some populations	21	4	10	7
ID issuance > 5 years for at least some populations	23	5	10	8
Issuing Sites and Service Centers (including 3rd parties)				
Total # of issuance, production, and storage facilities	7,091	969	2,130	3,992

Data Topic	TOTAL	States With Less Than 2 Million DL/IDs	States With Between 2 and 5 Million DL/IDs	States With More Than 5 Million DL/IDs
# of Characters for Full Legal Name in Database				
# of states with length ≤35	14	4	5	5
# of states with length between 40 and 124	18	7	7	4
# of states with length ≥125	7	3	2	2
Programming Hours for Verification Systems				
# of programming hours	2,003,794	331,652	599,874	1,072,268
Funds spent by States in Record Systems in the last 5 Years				
# of states	21	8	5	8
Total amount of funds	$289,026,586	$34,952,000	$77,400,000	$176,674,586
Barcode/Magnetic Stripe on DL/ID Card				
% using Barcode	47	13	17	17
Storage of Digital Images				
# of states who plan to save images on a separate system	19	8	2	9
# of states that plan to integrate saved images with their motor vehicle records system	9	5	2	2
Synchronization of DL Expiration Date with VISA Length of Stay				
Of those states that issue a temporary immigrant DL, # with DL renewal period equal to length of stay on immigration documents	26	7	9	10
SSN Verification via SSOLV				
# of states that use SSOLV	46	17	14	15
Legal Presence Verification via SAVE				
# of states that use SAVE	19	4	5	10

Data Topic	TOTAL	States With Less Than 2 Million DL/IDs	States With Between 2 and 5 Million DL/IDs	States With More Than 5 Million DL/IDs
Upfront Photo Capture				
# of states that currently capture photos at the beginning of the DL/ID Issuance process	8	1	3	4
Issue DL/ID without Photographs				
# of states with DL/ID photograph exceptions	32	11	11	10
Annual issuance of Non-Photo DL/IDs				
Total	1,083,832	21,843	90,650	971,339
DL without photograph	264,103	2,725	74,440	186,938
ID without photograph	1,389	28	110	1,251
Learner's permit without photograph	818,340	19,090	16,100	783,150
Masking Addresses				
# of states that allow masking of addresses	25	8	8	9
Employee Background Check				
# of states that provide some level of background check	34	11	11	12
# of employees requiring a background check	35,521	4,221	11,791	19,509
Average turnover rate for employees who will need a background check	13.32%	8.95%	16.32%	14.93%
Fraudulent Document Training Program				
# of states with fraudulent document training programs	42	11	16	15
# of states that use AAMVA's training program	35	10	14	11
# of states that use in-house training programs	10	2	3	5
# of employees requiring entry level training	25,754	2,587	8,535	14,632
# of employees requiring supervisory level training	5,126	762	2,369	1,995
Average annual turnover rate for employees who will receive training	13.41%	9.47%	17.02%	14.70%

APPENDIX

REAL ID ACT IMPACT ANALYSIS
SURVEY TWO

Purpose:
Quantify the impact of REAL ID implementation on the States, utilizing "best case" State recommendations as assumptions in the absence of draft regulations. Additionally analyze the impact of possible options known to be under consideration by DHS.

Organization:
The survey is organized around implementation issues, and split into two parts, one each for system impacts and business process impacts. The analysis separates one-time implementation costs from on-going operational costs.

Methodology:
States will analyze and develop answers internally and/or with the help of experts and vendors as they choose. Contact info is provided for questions and clarification. Conference calls will be scheduled as necessary to discuss and/or amplify issues. Results will be tabulated via phone surveys.

There will be related efforts to quantify/estimate costs that individual State's cannot (e.g. upgrade of federal systems, AAMVAnet enhancements, etc.). When possible, AAMVA will suggest default numbers (e.g. cost per background check, cost of training) if no local number is known. Please bring these opportunities to our attention early.

Guidelines:
- Use the 90/10 rule - It will be impossible to quantify perfectly
- Try to get to get to 90% confidence
- Focus on "big ticket" items
- When in doubt, round up. There are many off-setting costs we're not measuring at all (e.g. public education, complaint handling, web-site updates, etc.)
- When estimating implementation times, assume necessary funding is in hand (we ask elsewhere how long it would take to get budgets/legislation approved).
- When in doubt, use the assumption that's most likely, or easiest on your ability to develop and answer.
- ***Always*** identify when/how a new assumption is used or an existing one is changed.

Deadline:
States should be prepared for survey interviews no later than May 17, with strong encouragement for earlier completion where possible (there will be a prize!). Details about interview scheduling will follow later in the month. Those who anticipate being ready early should notify Anne Witt.

Contacts for Questions/Clarification:
Harold Kocken, AAMVA Senior Director, Driver Licensing
hkocken@aamva.org 703-908-5774
Anne Witt, AAMVA REAL ID Task Force Chair
anne.witt@dc.gov 202-727-4704

REAL ID ACT IMPACT ANALYSIS
SURVEY TWO

Part One
System Impacts

Full Legal Name

The Act requires each state to include a persons "full legal name" on a REAL ID credential.

Assuming states are required to maintain a name data field of 125 characters which would appear in the database, and

Assuming a minimum of 39 characters must print on the DL/ID card (according to standard truncation rules) and

Assuming it will be necessary to maintain additional database fields to capture the truncated name as well as AKA name fields to track other/prior names used:

1. If you have a contract supporting your license issuance process, on what date does it expire?

2. Describe how your current system handles these items:

   - Number characters for name field:_____
   - Truncation protocol utilized (e.g. CDLIS, ICAO, etc.)_____
   - Separate field capturing truncated name? ☐ Yes ☐ No
   - Separate field for AKA name tracking? ☐ Yes ☐ No

3. Describe the changes your issuance system would require to conform:

4. Based on the above, what are the estimated time and costs to implement the required system changes?

Initial One-Time Costs	Number Hours/ Units	Average Unit Cost	Estimated Total Cost	Elapsed Project Time (in weeks)	Comments
Business Process Engineering					
System Programming					
System Testing					
Hardware Purchase					
Other (Specify)					
On-Going Annual					

Costs					
License/Warranty Fees					
System Maintenance					
Supplies/Materials					
Other (Specify)					

5. Identify if/how these costs would change from the above, if at all, for the implementation of a 175 character name field, as DHS may propose?

6. Are there other systems with which you interface that rely on a name field match that would be affected by the above change?
   - If so, which system(s) (e.g. Board of Elections per HAVA, Courts, etc.)?
   - If so, what additional changes would you need to undertake to resolve this?

7. Are there other systems which utilize your data which might be affected by the above change?
   - If so, which system(s) (e.g. NADA, etc.)?
   - If so, what additional changes would you need to undertake to resolve this?

8. Estimate any costs of changes above and beyond those in the matrix above to allow interfaces with other systems.

Card Design Specifications

The Act requires States to incorporate "physical security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purposes."

Assuming REAL ID required compliance with the AAMVA Card Design Specifications (found at - www.aamva.org/Documents/std2005DL-IDCardSpecV2FINAL.pdf, and attached,) as follows:

- *DL/ID Card Design, Part 4- Human Readable Data Elements (pgs 19-24), specifically items a, b, c, g, h, i, j, and n; and the information related to them in Annex A – Card Design (pgs 26-28),*
- *Annex B - Physical Security (pgs 39-44) including the AAMVA OVD as the single mandatory/common security feature*
- *Annex D - Mandatory PDF417 Barcode (pgs 55-67), specifically items e, f, h, i, l, m, n, o, and p:*

9. Per the assumptions, what changes/additions would your jurisdiction need to make to the DL/ID card design related to: (describe substance of change needed):

   - Human Readable Elements in Card Design (Annex A)
   - Physical Security Features (Annex B)

10. What are the estimated system costs and time required to design procure and implement the revised card to meet the AAMVA specifications for human readable elements and physical security features.

Initial One-Time Costs	Number Hours/ Units	Average Unit Cost	Estimated Total Cost	Elapsed Project Time (in weeks)	Comments
Business Process Engineering					
System Programming					
System Testing					
Hardware Purchase					
Other (Specify)					
On-Going Annual Costs					
License/Warranty Fees					
System Maintenance					
Supplies/Materials					
Other (Specify)					

Assuming the PDF barcode would have to contain at least the 125 character full legal name, date of birth, gender, DL/ID number, and potentially the digital photograph and/or digital signature:

11. Describe how your current system handles these items:
    a.. Use a PDF417 2D barcode? ☐ Yes ☐ No
    b. If yes, items encoded in barcode:
    - Name with ____ characters? ☐ Yes ☐ No
    - Date of Birth? ☐ Yes ☐ No
    - Gender? ☐ Yes ☐ No
    - DL/ID number? ☐ Yes ☐ No
    - Digital Photo? ☐ Yes ☐ No
    - Digital Signature? ☐ Yes ☐ No
    - Other_____

12. What are the estimated costs and time required for changes/additions would your jurisdiction need to make to the above DL/ID card design related to the PDF 2D Barcode, in the following scenarios:

Data Encoded on the PDF 2D Barcode	Scenario I Full legal name @ 125 characters, gender, date of birth, DL/ID number	Scenario 2 Full legal name, @ 125 characters, gender, date of birth, DL/ID number and digital photo	Scenario 3 Full legal name @ 125 characters, gender, date of birth, DL/ID number and digital signature	Scenario 4 Full legal name@ 125 characters, gender, date of birth, DL/ID number, digital photo and digital signature
Cost: IT Programming				
Cost: License Redesign				
Cost: Equipment				
Cost: Materials (annually)				
Cost: Other (specify)				
Elapsed Time Required (in weeks)				

The Department of Homeland Security has indicated it's considering certain mandatory license security features in lieu of the AAMVA standards:

13. Indicate which of the following license features your jurisdiction currently uses:

- card stock. Yes ☐ No ☐ Planned ☐
- intricate, fine-line, multicolor background design produced via offset lithography to include micro-line printing and an intentional error field check (NOT dye sublimation) Yes ☐ No ☐ Planned ☐
- serial/inventory number on the card stock Yes ☐ No ☐ Planned ☐
- optically variable feature – ink and/or diffraction grating (e.g. statement that valid for official use) Yes ☐ No ☐ Planned ☐
- UV (long wave) responsive feature Yes ☐ No ☐ Planned ☐
- personalization of some information via laser engraving to include tactile features and micro-line printing specific to the bearer Yes ☐ No ☐ Planned ☐
- check digit numbers or letters Yes ☐ No ☐ Planned ☐
- revision date printed or engraved on the card surface to be updated any time the card design changes Yes ☐ No ☐ Planned ☐

14. What is your/your vendor's estimate of the cost and time to issue DL/ID's with all eight requirements above?

Cost: IT Programming	
Cost: License Redesign	
Cost: Equipment	
Cost: Materials (Annually)	
Cost: Other (specify)	
Elapsed Time Required (in weeks)	

Non-Conforming License:

The REAL ID Act requires DL/ID's that don't satisfy the federal requirements must clearly state on its face that it may not be accepted by any Federal agency for federal identification or any other official purpose; and must use a unique design or color indicator to alert Federal agency and other law enforcement personnel that it may not be accepted for any such purpose.

15. Does your jurisdiction plan to issue REAL ID conforming DL/ID's?

16. Does your jurisdiction plan to issue a separate license/ID that does not meet the federal requirements?

17. If yes to both above, what are the estimated incremental system costs and time for the non-conforming license design and procurement above and beyond the REAL ID costs elsewhere in this survey:

Initial One-Time Costs	Number Hours/ Units	Average Unit Cost	Estimated Total Cost	Elapsed Project Time (in weeks)	Comments
Business Process Engineering					
System Programming					
System Testing					
Hardware Purchase					
Other (Specify)					
On-Going Annual Costs					
License/Warranty Fees					
System Maintenance					
Supplies/Materials					
Other (Specify)					

Lawful Presence Requirements

The Act requires States to require evidence of lawful presence in the United States before issuing a REAL ID credential, and to limit the validity of the license/ID to the length of authorized stay.

Assuming DL/ID's may only be issued to those providing proper evidence of lawful presence, and DL/ID duration limited to the authorized length of stay (or one year if unknown), and accompanied by adding a new restriction code on the front with clarifying language "License Duration Limited For Non-Permanent US Residency" on the back.

18. Is there a measurable cost to your jurisdiction for adding an additional restriction/endorsement code on the front with explanation on the reverse of the DL/ID (like the current "eyeglasses required" type code)? If so, please indicate.

Initial One-Time Costs	Number Hours/ Units	Average Unit Cost	Estimated Total Cost	Elapsed Project Time (in weeks)	Comments
Business Process Engineering					
System Programming					
System Testing					
Hardware Purchase					
Other (Specify)					
On-Going Annual Costs					
License/Warranty Fees					
System Maintenance					
Supplies/Materials					
Other (Specify)					

19. If, instead of a restriction code, a separate DL/ID with separate markings on its face was required, what are the estimated system time and cost requirements for this separate license type.

Initial One-Time Costs	Number Hours/ Units	Average Unit Cost	Estimated Total Cost	Elapsed Project Time (in weeks)	Comments
Business Process Engineering					
System Programming					

System Testing					
Hardware Purchase					
Other (Specify)					
On-Going Annual Costs					
License/Warranty Fees					
System Maintenance					
Supplies/Materials					
Other (Specify)					

20. Do you currently limit the license/ID duration to approved length of stay?

21. What are the estimated time and cost for your jurisdiction to implement a non-standard expiration date to coincide with the authorized length of stay?

Initial One-Time Costs	Number Hours/ Units	Average Unit Cost	Estimated Total Cost	Elapsed Project Time (in weeks)	Comments
Business Process Engineering					
System Programming					
System Testing					
Hardware Purchase					
Other (Specify)					
On-Going Annual Costs					
License/Warranty Fees					
System Maintenance					
Supplies/Materials					
Other (Specify)					

Verification of Eligibility

The Act requires States to verify, with the issuing agency, the issuance, validity and completeness of documents required to be presented.

Assuming the federal government, in consultation with the States, designed, created, developed and provided the following systems with reliable real-time access:

- *SSOLV (Social Security On-Line Verification) incorporating death records and enhanced for Saturday operations*
- *SAVE (Systematic Alien Verification for Entitlements) including lawful presence status and authorized end-of-stay date*
- *EVVER (Electronic Verification of Vital Events Records) with all jurisdiction birth, marriage, divorce and death records*
- *A Department of State US Passport database including birth records of US citizens born overseas*
- *An All-Driver Database (such as DRIVeRs) with US-issued license and ID records*

And, assuming the AAMVAnet hub was available as an option for access to these systems such as currently available for CDLIS, SSOLV, etc.:

22. Do you current use SSOLV?

23. If yes, is your access via batch or on-line processing?

24. What would be the estimated time and cost for your jurisdiction to integrate on-line SSOLV verification, assuming SSOLV is fully developed, funded and accessible to the States (check and answer for whichever of the following scenarios is applicable):

    ☐ Connect to the application via AAMVAnet

    ☐ Develop your own connection to the application

Initial One-Time Costs	Number Hours/ Units	Average Unit Cost	Estimated Total Cost	Elapsed Project Time (in weeks)	Comments
Business Process Engineering					
System Programming					
System Testing					
Hardware Purchase					
Other (Specify)					
On-Going Annual Costs					

License/Warranty Fees					
System Maintenance					
Supplies/Materials					
Other (Specify)					

25. Do you currently use SAVE?

26. If yes, is your access via batch or on-line processing?

27. If yes, what percent of your transaction require additional processing beyond the first inquiry?

28. What would be the estimated time and cost for your jurisdiction to integrate on-line SAVE verification, assuming SAVE is fully developed, funded and accessible to the States (check and answer for whichever of the following scenarios is applicable):

☐ Connect to the application via AAMVAnet

☐ Develop your own connection to the application

Initial One-Time Costs	Number Hours/ Units	Average Unit Cost	Estimated Total Cost	Elapsed Project Time (in weeks)	Comments
Business Process Engineering					
System Programming					
System Testing					
Hardware Purchase					
Other (Specify)					
On-Going Annual Costs					
License/Warranty Fees					
System Maintenance					
Supplies/Materials					
Other (Specify)					

29. Are any of your State's birth records automated?

30. If yes, what percent of the records or what is the earliest year that is currently automated?

31. How far back (to what year) does your vital records agency intend to automate?

32. What is the vital records agency's estimate (year) when automation is complete?

33. Is your vital records agency funded to accomplish this automation?

34. What would be the estimated time and cost for your jurisdiction to integrate on-line EVVER verification, assuming EVVER is fully developed, funded and accessible to the States (check and answer for whichever of the following scenarios is applicable):

☐ Connect to the application via AAMVAnet

☐ Develop your own connection to the application

Initial One-Time Costs	Number Hours/ Units	Average Unit Cost	Estimated Total Cost	Elapsed Project Time (in weeks)	Comments
Business Process Engineering					
System Programming					
System Testing					
Hardware Purchase					
Other (Specify)					
On-Going Annual Costs					
License/Warranty Fees					
System Maintenance					
Supplies/Materials					
Other (Specify)					

35. Does your state currently have any ability to do automated passport verifications with the Department of State?

36. If yes, is this verification via batch or on-line processing?

37. What would be the estimated time and cost for your jurisdiction to integrate on-line Department of State passport verification, assuming a passport verification system is fully developed, funded and accessible to the States (check and answer for whichever of the following scenarios is applicable):

☐ Connect to the application via AAMVAnet

☐ Develop your own connection to the application

Initial One-Time Costs	Number Hours/ Units	Average Unit Cost	Estimated Total Cost	Elapsed Project Time (in weeks)	Comments
Business Process Engineering					
System Programming					
System Testing					
Hardware Purchase					
Other (Specify)					
On-Going Annual Costs					
License/Warranty Fees					
System Maintenance					
Supplies/Materials					
Other (Specify)					

38. What would be the estimated time and cost for your jurisdiction to integrate on-line all-driver verification, assuming an all-driver verification system is fully developed, funded and accessible to the States (check and answer for whichever of the following scenarios is applicable):

☐ Connect to the application via AAMVAnet

☐ Develop your own connection to the application

Initial One-Time Costs	Number Hours/ Units	Average Unit Cost	Estimated Total Cost	Elapsed Project Time (in weeks)	Comments
Business Process Engineering					
System Programming					
System Testing					
Hardware Purchase					
Other (Specify)					
On-Going Annual Costs					
License/Warranty					

Fees					
System Maintenance					
Supplies/Materials					
Other (Specify)					

Address of Principle Residence

The Act requires States to document the applicant's address of principle residence.

Assuming States are NOT required to verify an address through any electronic system, but that instead the address will be determined via the citizen's production of an affidavit and accompanying proofs, but

Assuming the provided address must be captured and maintained in the database, and

Assuming States are required to allow the "masking" of an address on the credential for persons in certain protected classes (e.g. victims of domestic violence) while retaining the information in the database:

39. Does your jurisdiction currently retain an address in the database?

40. Does your jurisdiction currently allow the use of an alternative mailing address?

41. Does your jurisdiction use a standard address protocol (e.g. USPS Postal Addressing Standards)? If so, which?

42. Does your jurisdiction currently allow the "masking" of an address for persons in certain protected classes (e.g. victims of domestic violence, law enforcement or court personnel, etc.)?

43. Describe the changes required to your system to comply with the capture and maintenance of the address of principle residence, while allowing the masking of addresses which appear on the license for certain protected classes

44. What would be the estimated time and cost for your jurisdiction to implement the required changes:

Initial One-Time Costs	Number Hours/ Units	Average Unit Cost	Estimated Total Cost	Elapsed Project Time (in weeks)	Comments
Business Process Engineering					
System Programming					
System Testing					
Hardware Purchase					
Other (Specify)					
On-Going Annual					

Costs					
License/Warranty Fees					
System Maintenance					
Supplies/Materials					
Other (Specify)					

Records Retention

The Act requires States to employ technology to capture digital images of identity source documents so that the images can be retained in electronic storage in a transferable format.

Assuming you must capture digital images of documents accepted for proof of full legal name, date of birth, social security number, and lawful presence, and

Assuming they must be retained in a transferable electronic storage format, and retained for a minimum of ten years or the duration of a renewed REAL ID, whichever is longer;

45. How many documents per average transaction would you expect to process:
    - Full legal name
    - Date of birth
    - Social security number
    - Lawful presence

46. Would your jurisdiction plan to save the digital images in a system separate from or integrated with your DL/ID database?

47. What are the estimated added costs and time to capture and save the digital images?

Initial One-Time Costs	Number Hours/ Units	Average Unit Cost	Estimated Total Cost	Elapsed Project Time (in weeks)	Comments
Business Process Engineering					
System Programming					
System Testing					
Hardware Purchase					
Other (Specify)					
On-Going Annual Costs					
License/Warranty Fees					
System Maintenance					
Supplies/Materials					
Other (Specify)					

Photo Capture

The Act requires States to subject each person applying for a driver's license or identification card to mandatory facial image capture.

Assuming jurisdictions must capture and retain the digital photograph and basic identifying information of ALL applicants at the beginning of the process, not just of those who complete the vetting process and ultimately receive the DL/ID, and

Assuming the business process changes identified in Part Two, Page 22.

48. What are the estimated time and cost for the system changes for your jurisdiction to implement the required changes?

Initial One-Time Costs	Number Hours/ Units	Average Unit Cost	Estimated Total Cost	Elapsed Project Time (in weeks)	Comments
Business Process Engineering					
System Programming					
System Testing					
Hardware Purchase					
Other (Specify)					
On-Going Annual Costs					
License/Warranty Fees					
System Maintenance					
Supplies/Materials					
Other (Specify)					

Database

The Act requires States to provide electronic access to all other States to information contained in the States motor vehicle database (at a minimum: all data fields printed on drivers' licenses and identification cards issued by the State; and motor vehicle drivers' histories, including motor vehicle violations, suspensions, and points on licenses).

Assuming these data elements also include the digital photo and signature, and

Assuming these data elements must be able to be shared with all other jurisdictions via a query / response method via AAMVAnet (e.g. Digital Image Exchange Project) or individually developed connections:

49. What are the estimated time and cost for the system changes for your jurisdiction to implement the required changes?

50. Does your jurisdiction currently have any limitations on the sharing of DL/ID data, driver record and/or photographs with other state licensing agencies?

51. If so, what legislative changes will be required in order to comply?

52. What system changes and/or upgrades would be required to comply?

53. What are the estimated time and costs for implementation?

☐ Connect to the application via AAMVAnet

☐ Develop your own connection to the application

Initial One-Time Costs	Number Hours/ Units	Average Unit Cost	Estimated Total Cost	Elapsed Project Time (in weeks)	Comments
Business Process Engineering					
System Programming					
System Testing					
Hardware Purchase					
Other (Specify)					
On-Going Annual Costs					
License/Warranty Fees					
System					

Maintenance					
Supplies/Materials					
Other (Specify)					

54. What are the estimated time and costs for implementation?

55. When was your driver license information system developed or when did it have its last major redesign?

56. What was the cost of that re-design?

57. Did your jurisdiction have major driver license system re-designs/upgrades planned independent of REAL ID Act Requirements?

    a. If so, for when?

    b. If so, how much was budgeted for this?

Part Two
Business Process Impacts

Certification

The Act requires the Secretary of Homeland Security to determine whether a State is meeting the requirements of this section based on certifications made by the State to the Secretary

Assuming the REAL ID Act compliance certification process was similar to that currently in place for the Department of Transportation Federal Motor Carrier Safety Administrations CDL audit process, where the Governor certifies annually to the State's compliance and DHS performs an audit, at least every three years:

58. What is the estimated number of staff hours currently devoted by your jurisdiction to a federal CDL audit?

59. What is a ball-park average hourly salary rate of the persons most involved in the federal CDL audit process?

60. Based on the above, what is your estimate of the cost of a CDL audit?

61. Based on common subject matter, what percent of the time involved in the CDL audit would you estimate might be duplicated in a REAL ID compliance audit?

To understand the relative scale of your CDL population compared to all driver's and ID holders:

62. What is the number of Active CDL's in your jurisdiction?

63. What is the number of Active Non-CDL's in your jurisdiction?

64. What is the number of non-driver ID holders' in your jurisdiction?

Lawful Presence Requirements

The Act requires States to require evidence of lawful presence in the United States before issuing a REAL ID credential, and to limit the validity of the license/ID to the length of authorized stay, through verification of US Immigration documents through the Department of Homeland Security's SAVE system.

Assuming SAVE is available to electronically verify all permitted classes of lawfully present citizens, but,

Assuming it's still necessary for a subset of these (e.g. 15%) to be subject to more time-consuming second and/or third tier research by SAVE which would not allow instant verification:

65. What is the estimated number/percent of non-permanent US residents processed by your jurisdiction?

66. Do you anticipate this processing will be possible at all service locations, or limited to a subset of locations?

67. If the number of locations will be limited, indicate the number of service locations which will and won't have this capability.

68. Are there any additional investments your jurisdiction would find necessary to implement these provisions (e.g. bi-lingual staff, forms and materials translation, etc.) as result of REAL ID requirements.

.

Address of Principle Residence

The Act requires States to document the applicant's address of principle residence.

Assuming States do NOT have to verify the address of principle residence via an electronic system, but

Assuming the DL/ID application process required an affidavit declaring address of principle residence, accompanied by at least two proof documents matching the address (e.g., lease/mortgage, recent utility/tax bill, etc.) which do NOT need to be imaged or retained.

69. Describe the operational changes would your jurisdiction require.

70. What do you estimate the added per transaction processing time would be in minutes and percent?

71. What are the estimated costs and time for implementing the changes?

Initial One-Time Costs	Number Units	Average Unit Cost	Estimated Total Cost	Elapsed Project Time (in weeks)	Comments
Business Process Engineering					
Facility Redesign					
Forms Redesign					
Hardware Purchase					
Policy/Regulation Change Adoption					
Employee Training					
Other (Specify)					
On-Going Annual Costs					
Supplies/Materials					
Annual FTE equivalents for added transaction time					
Equipment maintenance etc.					
Other (Specify)					

Photo Capture

The Act requires States to subject each person applying for a driver's license or identification card to mandatory facial image capture.

Assuming jurisdictions must capture the digital photograph of the applicant (as opposed to the DL/ID recipient) at the beginning of the process, along with the basic applicant information, but prior to full vetting and license issuance:

72. What type of DL/ID's do you currently issue without a photo?

73. What are the estimated numbers of each type above?

74. Do you currently capture the photograph at the beginning of the in-take process (e.g., photo is on file even if license/ID not ultimately issued?)

75. Describe how your current business practices would have to be revised to meet the mandatory photo capture for each applicant.

76. What are the estimated time and cost of the required business process changes (note: related system cost changes are already covered in Part One of the survey)

Initial One-Time Costs	Number Units	Average Unit Cost	Estimated Total Cost	Elapsed Project Time (in weeks)	Comments
Business Process Engineering					
Facility Redesign					
Forms Redesign					
Hardware Purchase					
Policy/Regulation Change Adoption					
Employee Training					
Other (Specify)					
On-Going Annual Costs					
Supplies/Materials					
FTE equivalents for added transaction time					
Equipment-related					
Other (Specify)					

License Validity

The Act requires States to limit the period of validity of DL/ID's that are not temporary to a period that does not exceed 8 years.

Assuming the period of validity for all DL/ID's may not exceed eight years, for those jurisdictions currently having validity periods in excess of 8 years:

77. What types of credentials currently have validity periods in excess of 8 years?

78. What is the estimated number of each type above?

79. Describe how your current business practices would have to be revised.

80. What are the estimate time and costs for your jurisdiction to implement the required changes (not including the one-time re-enrollment covered in a following question)?

Initial One-Time Costs	Number Units	Average Unit Cost	Estimated Total Cost	Elapsed Project Time (in weeks)	Comments
Business Process Engineering					
Facility Redesign					
Forms Redesign					
Hardware Purchase					
Policy/Regulation Change Adoption					
Employee Training					
Other (Specify)					
On-Going Annual Costs					
Supplies/Materials					
FTE equivalents for added transaction time					
Equipment-related					
Other (Specify)					

81. Does your jurisdiction currently allow a person to hold both a DL and ID concurrently? If so, how many persons currently hold both credentials?

82. If yes, what is the estimated impact and cost if this practice were prohibited?

Card Design Specifications

The Department of Homeland Security has indicated it's considering certain mandatory license security features in lieu of the AAMVA standards:

- card stock
- intricate, fine-line, multicolor background design produced via offset lithography to include micro-line printing and an internal error field check (NOT dye sublimation)
- serial/inventory number on the card stock
- optically variable feature – ink an/or diffraction grating (e.g. statement that valid for official use)
- UV (long wave) responsive feature
- Personalization of some information via laser engraving to include tactile features and micro-line printing specific to the bearer
- Check digit numbers or letters
- Revision date printed or engraved on the card surface to be updated any time the card design changes

83. What issuance method does your jurisdiction currently use?

    - Centralized
    - Over-the-Count
    - Hybrid

84. If all eight features above were required, would your jurisdiction need to change the above issuance method? If so, describe.

85. If yes, what is the estimate and time and costs to convert to the new issuance method:

Initial One-Time Costs	Number Units	Average Unit Cost	Estimated Total Cost	Elapsed Project Time (in weeks)	Comments
Business Process Engineering					
Facility Redesign					
Forms Redesign					
Hardware Purchase					
Policy/Regulation Change Adoption					
Employee Training					
Other (Specify)					
On-Going Annual Costs					

Supplies/Materials					
FTE equivalents for added transaction time					
Equipment-related					
Other (Specify)					

Employee Background Checks

The Act requires States to subject all persons authorized to manufacture or produce drivers' licenses and identification cards to appropriate security clearance requirements.

Assuming every employee and involved in the applicant vetting/issuance process, cashiering and payment processing, procurement, inventory control, facility maintenance and support, information systems, as well as all supervisors and managers were required to undergo a state and federal criminal background check and credit check, and

Assuming the employees of every vendor involved in the above functions were to be contractually required to undergo the same criminal background and credit checks:

86. How many of your jurisdiction's employees would be subject to the background check requirements?

87. What is your average annual employee turnover rate?

88. Do you currently conduct background checks?
    - If so, describe type and scope and frequency
    - if so, describe number and type of covered employees
    - if so, describe disqualifying offenses

89. Describe what legal, labor contract, hiring process, etc. changes this would require in your jurisdiction and their impacts (e.g. finding alternative jobs for pre-existing employees who can't pass).

90. What is the estimated cost of a federal and state criminal background check in your jurisdiction?

91. What is the estimated cost of a federal and state criminal background and credit history check in your jurisdiction?

92. How many contracts would need to be modified to include the required background checks?

93. By applying the costs above to the estimated number of affected contractual employees, or by utilizing a vendor-provided number, what is the estimated cost impact of any new background check provisions for your vendors due to REAL ID?

Physical Security

The Act requires States to ensure the physical security of locations where drivers' licenses and identification cards are produced and the security of document materials and papers from which drivers' licenses and identification cards are produced.

Assuming every facility where DL/ID's are produced and/or where document materials and papers from which DL/ID's are handled or stored was required to be physically secure:

(Note – the State recommendation is for states to submit risk management plans, and the DHS thinking is for high-end secure document standards. More work is necessary to determine costing assumptions, so only baseline measures are requested here).

94. What number of such facilities in your jurisdiction would be affected?

	Issuance Offices	Production Facilities	Storage Facilities
Operated by You			
Operated by Vendor			
Operated by Agents			

95. For each applicable type above, describe the current measures and costs for protecting physical security (e.g. locks, cameras, guards, hours of coverage, etc.)

Fraudulent Document Training

The Act requires States to establish fraudulent document recognition training programs for appropriate employees engaged in the issuance of drivers' licenses and identification cards.

Assuming every employee will be required to successfully complete the equivalent of AAMVA's Level One Fraudulent Document Recognition Training – entailing 12 hours of instruction, and

Assuming at a minimum all supervisors and managers would also require both an additional 12 hours of Level Two training, and

Assuming each employee would need a minimum of 4-hours training each successive year to re-certify:

96. What number of employees will require the training?
    - Level One
    - Level Two
    -

97. What is your average annual employee turnover rate?

98. What change to your current training practices would be required?

99. What percent of your training do you estimate will be provided?
    - In-house
    - Via contract on-site
    - Via contract off-site
    - Via computer-based delivery

    Note: AAAMVA current estimate of Level One on-line training is $100/per student for the computer-based training portion (would likely need to be augmented by on-site hands-on document review skills)

100. What are the estimated additional costs to implement the changes?
    - Training delivery
    - Employee time away from work
    - Facilities
    - Equipment
    - Materials

101. Describe additional facilities/equipment/resources (e.g. training rooms, computers, contractors, etc.) required to comply with new assumptions.

102. How much elapsed time (in months) will you require to be prepared to meet the training requirements?

Re-enrollment

The Act requires States to be compliant with the provisions of the Act by May 11, 2008 in order for DL/ID's issued by the state to be accepted by a federal agency for an official purpose.

Assuming your state was to comply with the Act, and as of May 11, 2008, every new DL/ID produced met the requirements, and all current license holders coming for renewal had to be re-processed in-person under the new requirements, and

Assuming all DL/ID's, including renewals, require in-person visits, and

Assuming due to the new requirements, service times on renewals would now be equivalent to the original issuance service times, and

Assuming all DL/ID holders must be compliant by May 11, 2013 (five years):

103. How many additional in-person visits do you anticipate over the 5-year period due to the lost of alternative channels (mail, internet, kiosks, etc.)

104. How many additional in-person visits do you anticipate over the 5-year period due to the need to "accelerate" due to your previous renewal cycle being longer than 5 years?

105. What is the answer above, If the assumption above was extended to a re-enrollment period of 8-years (until May, 2016)?

106. Estimate the increased DL/ID workload impact on your jurisdiction using the worksheet on the following page.

REAL ID In-Person Workload Increase Estimate Calculation Worksheet:

Assumptions:

- New full REAL ID enrollment transactions take twice as long as current in-person renewal transactions.
- In-person renewal transactions take twice as long as alternative channel (mail, internet) non-in-person renewal transactions.
- All transactions in the first cycle of REAL ID will be in-person, "new" transactions.
- (Note: There's a cumulative impact on alternative channel renewal transactions making them four times as long (first doubling due to appearing in-person and then doubling again due to becoming a "full" transaction).

Current Per Year	REAL ID Per Year
# new (original) transactions = X	# new (original) transactions = X
# in-person renewal transactions = Y	# in-person renewal transactions = 2Y
# non-in-person renewal transactions = Z	# non-in-person renewal transactions = 4Z
Total Current = X + Y + Z	Total REAL ID = X + 2Y + 4Z

Adjust for Renewal Cycle:

If your renewal cycle is longer than 5 years, substitute the following above:

$$Y = \#\text{ in-person renewal transactions} \times \frac{\text{Renewal Period}}{5}$$

$$Z = \#\text{ non-in-person renewal transactions} \times \frac{\text{Renewal Period}}{5}$$

Percent Workload Increase:

$$\frac{\text{Total REAL ID}}{\text{Total Current}} \quad \text{or} \quad \left[\frac{X+2Y+4Z}{X+Y+Z}\right] - 1 = \_\_\_\_\%$$ Transaction Workload Increase Due to REAL ID

Workload Increase Budget Impact:

Your Jurisdiction's Base Annual DL/ID Personnel and Facility Support Budget = $_____
(note: materials and systems impacts are calculated elsewhere)
Estimated cost of increased REAL ID transaction workload = Base Budget X REAL Increase %
= $_____.

The Department of Homeland Security has indicated the potential of "grandfathering (e.g. waiving all new REAL ID requirements to receive a REAL ID) persons who were born before 1935 AND who have a relatively long-term (e.g. 10-years) relationship with the State. The States are interested in expanding that idea to potentially either or both as a means of reducing the re-enrollment pressures on the States. The following questions are to help assess those impacts.

107. What number and percent of your current DL/ID holders were born before 1935 and have held a DL/ID for at least ten years?

108. What number and percent of your current DL/ID holders have held them in your state for longer than 10 years? 16 years?

109. What number and percent of your current license/ID holders were born prior to 1935? 1945?

Legislation:

110. Does your jurisdiction require enabling legislation to implement REAL ID Act requirements? If so, in what areas? What is the earliest this can be accomplished?

111. If funding is not forthcoming from the federal government, in the best case, when would be the earliest you could obtain additional appropriations for the purpose of implementing REAL ID?

Other:

112. Are there other significant impacts (either in terms of service quality or expense) that have not been covered in this survey? If so, please describe the issue (including assumptions) and the impact.

113. For impact comparison purposes, what is your annual base operating budget for DL/ID functions in your jurisdiction?

The Act requires States to be compliant with REAL ID provisions by May 11, 2008.

Assuming DHS issues its regulations on January 1, 2007 and,

Assuming the regulations match the State recommendations contained in the assumptions of this survey, and

Assuming the federal verification systems were all in place , and

Assuming you had the funding you require:

114. What is the earliest date your state could be compliant?
(Allow the critical time path for the estimates in this survey for necessary law/regulations change, business process reengineering, contract changes, employee background checks, new hires, training, procurements, systems redesign, programming and deployment, equipment delivery and installation, etc. etc.)

New Federal Regulations Get an 'F' in Addressing Issues with the Real ID Act

DHS Rules Score Only 9 Percent On ACLU Scorecard

On March 1st, the Department of Homeland Security issued proposed Federal regulations for implementing the Real ID Act, the law that would federalize state driver's licenses and the motor vehicles departments that issue them and create the nation's first-ever de facto national identity card system.

In preparation for the issuance of the regulations, the ACLU prepared this Real ID Scorecard to assist in the systematic analysis of this complex legislation. It attempts to list all the issues that have been identified as concerns with Real ID by a variety of parties, including privacy activists, domestic violence victims, anti-government conservatives, religious leaders, and DMV administrators.

The Scorecard shows that the regulations utterly fail to remedy the problems with Real ID. Of the 56 issues listed, the regulations passed 5 (9 percent), scored an incomplete on 9 (16 percent), and failed the rest.

Indeed, the government was often strikingly forthright in admitting that the regulations do not solve deep problems with this statute. The regulations acknowledge that wait times at the DMV will increase substantially; that many applicants will not have source documents they need to obtain a Real ID card; that "there is no single way for States to comply" with Real ID's verification requirements by the statute's deadline "or in the reasonably foreseeable future"; and that the regulations will be extremely costly. (The most authoritative prior estimate of Real ID's costs was $11 billion. The regulations, however, concede that the price tag for Real ID will come to a whopping $23 billion.)

DHS cannot be blamed for such problems when they arise out of what is, at its core, simply an ill-conceived and impossible law. In other cases, however, the government fails to set forth rules that could have solved or ameliorated problems with the act. On Real ID's onerous verification requirements, for example, DHS did not ease burdens on states and individuals, but in fact increased them (by requiring verification of all identity documents not just to obtain a Real ID, but even to renew one; requiring not one, but two documents showing proof of address). Similarly, the agency acknowledges the danger of license data being scanned by third parties, but fails to take action to stop the problem, and merely encourages the states to come up with a solution. DHS says it "leans toward" requiring that data to be encrypted but opts not to due to "practical concerns."

Aside from failing to solve the problems with Real ID, the regulations add up to a striking federal takeover of state DMV offices. The regulations put the federal government in the position of dictating the minutiae of DMV operations, from the colors that can be used on a license to the computer format in which image files (.JPG) and scanned documents (.TIF) are stored, to the details of how a DMV office secures its plant, to many other details.

Initial media coverage of the new regulations focused on the additional time that states were being given to comply with Real ID. But what this scorecard makes clear is that Real ID is a fundamentally misguided policy that will waste large amounts of money and other limited resources, and impose significant inconveniences, without improving our safety. We don't need to delay Real ID, we need to throw it away and start fresh.

The grades

The following grades indicate whether the federal regulations succeed in fixing each problem. In cases where DHS addressed the problem but could not or did not fix it, we list a grade of "incomplete."

Problems with the act have been grouped into four categories: 1) impact on individuals, 2) impact on privacy, 3) impact on states and 4) impact on Constitutional rights.

Impact on Individuals	
PASS ☐ FAIL ☒ INC ☐	**Increased wait time at the Department of Motor Vehicles ("DMV").** Many state DMVs predict extensive increases in customer wait times resulting from the many new requirements imposed by Real ID. In a survey by the American Association of Motor Vehicle Administrators (AAMVA), states predict that Real ID will bring increased "customer traffic flow and customer wait/visit time in all field offices" and will have a "significant influence on customer service." (*"The Motor Vehicle Administrators Survey on Real ID: An ACLU White Paper"*) **The regulations impose significant new burdens on individuals that, as DHS acknowledges (p. 98), will increase wait times and service times at DMVs, as well as the time necessary to obtain new source documents. Partly this would be caused by the fact that initial applications for all Real IDs (as well as many renewals) must be done in person (p. 146), and many applicants will not have source documents when they need them (p. 107). DHS estimates opportunity costs to individuals from waiting at the DMV at $1.7 billion (p. 106).**
PASS ☐ FAIL ☒ INC ☐	**"Full Legal Name" requirement.** Wide inconsistency often exists between names even on federal documents, such as a social security card and a passport belonging to the same individual. All these records must be verified and harmonized under REAL ID prior to the issuance of a license. Recently in Alabama tens of thousands of older drivers had difficulty renewing licenses because the names in their DMV records were not consistent with other records such as the Social Security database. Many Americans have records that reflect not only their "legal name", but also the everyday names they use. James Joseph Johnson Jr. may have documents in the name of Jim Johnson, JJ Johnson, Jim Johnson Jr., Joe Johnson, etc. (*ACLU analysis, "The Alabama Mess: One State Tries to Begin Tackling Real ID"*). **The regulations do not address or solve the problem of individuals who are recorded under different names on different documents or in different databases. The regulations simply state that all license holders must use their legal name in applications and that the identity documents they submit must contain that name (p. 142).**

PASS	FAIL	INC	
☐	☒	☐	**Individuals with changed names.** Individuals whose name on one source document does not match the name on another will find themselves in a bureaucratic bind under Real ID. This is a substantial portion of the population including women who have taken their spouses' last names and a large percentage of the Asian-American community (whose first and last name may be switched on their source documents). (*National Governors Association ("NGA"), National Conference of State Legislators ("NCSL'), & AAMVA, "The Real ID Act: National Impact Analysis"*) **According to the regulations, in order to prove a name change an applicant must present a certified copy of a record from "US or state-level Court or government agency" (pp. 65 & 133). This does not address the issue of individuals whose name is recorded differently in different databases or records. It also requires individuals to take the formal step of changing their name; currently in many states it is lawful to simply use a different name as long as an individual has no fraudulent intent. Finally, many marriage certificates are issued by county (not state) officials, making it unclear how individuals could comply.**
PASS	FAIL	INC	
☐	☐	☒	**Principal address requirement.** The act requires, without exception, that compliant IDs contain one's "principal address." It is unclear how people without such an address or who live in different places – such as students, those who live in RVs and other mobile homes, and the homeless – will solve this issue. (*See ACLU, "Real Costs: Assessing the Financial Impact of the Real ID Act on the States"*) **The regulations attempt to address this issue by defining principal address as the place where an individual has his "true, fixed and principal home" (p. 129), and stating that DMVs can make exemptions for the homeless (pp. 44 & 70). There is still some concern regarding whether all states will be able and willing to create workable methods for utilizing these exemptions.**

PASS ☐ FAIL ☒ INC ☐	**Threat to safety from principal address requirement.** A number of states have laws that allow judges, police officers, domestic violence victims, or others at risk of retaliatory criminal violence to use agency addresses or P.O. boxes in lieu of their actual residence address. Yet states cannot keep those laws on the books if they are to comply with Real ID. (*"Motor Vehicle Administrators Survey"*) **Under the regulations, the vulnerability of domestic violent victims and others will be increased. The regulations do create a partial exemption to the principal address requirement, but it is inadequate. It covers "individuals who are entitled to enroll in State address confidentiality programs, whose addresses are entitled to be suppressed under State or Federal law or by a court order" and some individuals protected by immigration law (p. 69). However, only 24 states currently have such confidentiality programs, according to the National Network to End Domestic Violence. In the other jurisdictions, victims are now protected instead by the fact that they are not required to put their principal address on their license – as are federal judges, who are not shielded by state laws at all (DHS solicits comments on how to fix the problem with regard to the judges). The regulations seem to maintain the same status that police officers, state and local judges, and protected witnesses currently enjoy under state law. However, by removing the option of not listing an address and relying solely on state laws that don't cover many vulnerable individuals, the regulations fail badly.**
PASS ☐ FAIL ☒ INC ☐	**Disproportionate burden on low-income individuals.** It is feared poorer people will find it harder not only to absorb higher license-issuance or renewal fees, but also to skip what will sometimes be multiple days of work in order to stand in long queues to prove their identities in order to obtain a Real ID. (*ACLU, "Real Answers: FAQ on Real ID"*) **Real ID is expected to cost $23.1 billion nationally (p. 106), including $7.8 billion in costs to individuals, and will require increased time waiting at the DMV and seeking source documents. The regulations estimate that visits to the DMV alone will cost Americans $1.7 billion.**
PASS ☒ FAIL ☐ INC ☐	**Individuals who lack birth certificates.** Over time, many records are lost through natural disasters, such as flood or fire, and by human error. And the births of many, especially older citizens from rural areas, simply were not recorded. Because the birth certificate is likely to be one of the core documents that must be verified (especially to prove citizenship) it is not clear how these problems will be addressed. (*"FAQ"*) **The regulations seem to address this issue by allowing states to create an exemption process for individuals who do not have a birth certificate (p. 44 and 135). (Ironically, this exemption would seem to undercut the entire security rationale for Real ID: that identity can only be proved by presenting other "breeder documents" like birth certificates).**

PASS ☐ FAIL ☒ INC ☐	**Foreign-born lawful residents who lack passports.** The only foreign document that is acceptable to DMVs under Real ID is an official passport. But that doesn't meet the needs of many legal immigrants, including refugees and dissidents or others who may face hostility or a lack of cooperation from their home governments in obtaining the required documents. (*"FAQ"*) **DHS attempts to address this problem by allowing for the acceptance of some foreign documents other than passports. But there are some categories of immigrants who, while legal, will still not possess any of the documents listed by DHS (for example, asylum seekers).**
PASS ☐ FAIL ☒ INC ☐	**Same-day licenses.** State DMV officials report that Real ID could largely prevent over-the-counter issuance of some or all IDs, resulting in shifts from relatively instant issuance to having to mail documents to applicants, and an overall process that could range from 2 to 6 weeks pending approval of verified documents. (*"Motor Vehicle Administrators Survey"*) **While in theory, if every verification database existed and was fully operational, applicants could have their documents verified instantly and walk away with a Real ID, the regulations make it clear that that simply is not going to happen, at least in the foreseeable future. There are too many burdens in the regulations, too many documents to be verified, and too few existing systems through which to do that, for there to be any realistic chance that same-day licenses will continue to be possible.**
PASS ☐ FAIL ☒ INC ☐	**Fewer offices.** DMV officials in some states also report that the cost increases driven by the act's requirement may force them to close some itinerant field stations and eliminate mobile offices, which can impose considerable burdens on citizens of rural, low-density states. (*"Motor Vehicle Administrators Survey"*) **The regulations fail this test because they create extensive security requirements for DMV offices (p. 150), making it unlikely that many small DMV offices will be able to remain open at a cost the states can afford. This would inconvenience consumers by forcing smaller offices to close their doors and have a disproportionate impact on Americans who live in rural communities.**
PASS ☐ FAIL ☒ INC ☐	**Internet or mail transactions.** Because of the verification requirements, DMV officials report that Real ID could reduce or end mail and Internet address changes and renewals, further straining the resources of DMVs and imposing burdens on drivers and other applicants. (*"Motor Vehicle Administrators Survey"*) **Issuing of licenses through the Internet and mail will not be possible for at least the first 5 years under Real ID because every individual will be required to register in person to get a Real ID. Remote renewals of a Real ID (after initial issuance) will only be possible for every other renewal, and only if none of the licensing information (such as address) has changed (p. 146). Also, it is unclear whether the regulations will allow the mailing of licenses or whether license holders will have to return to the DMV to receive a license.**

PASS ☒ FAIL ☐ INC ☐	**Change of address.** Currently individuals simply notify their DMV when they move. However, the principal address requirement of Real ID (see above) may require people to re-register with the DMV in person every time they change addresses so that their new address can be verified and they can be issued a new ID card. This will not only impose substantial inconveniences on individuals, but also raise costs for DMVs. (*NCSL et al, "Impact Analysis"*) **The regulations seem to address this issue by implying (though not stating directly) that an individual will only have to change their address information when renewing their license (p. 146).**
PASS ☐ FAIL ☒ INC ☐	**Disruption in driving caused by verification procedures.** Will states be able to issue an interim driver's license for individuals whose source documents cannot be immediately verified or will these individuals be prevented from driving? Will such a temporary ID be acceptable for air travel? **The regulations make no provision for this type of temporary license and fail to take into account the fact that delays in verification (due to such inevitabilities as computer problems or verification delays) will make it increasingly difficult to perform same-day licensing.**
Impact on Privacy	
PASS ☐ FAIL ☒ INC ☐	**National ID.** Privacy advocates fear the Real ID and its national database will become a national identity registry. The act states that Real IDs shall be required not only for activities like boarding aircraft, but also for "any other purposes that the Secretary [of Homeland Security] shall determine." This provision allows the Department of Homeland Security to expand unilaterally the scope of identity requirements creating the real possibility of mission creep. Some groups have already suggested that Real ID should become a voter registration card and a border crossing document. (*"FAQ"*) **The regulations do nothing to prevent Real ID from becoming a de facto National ID card. They create a vast infrastructure for such a system, including a common machine readable element (with no protection against private-sector exploitation) and the construction of a national interlinked database. The regulations already require the card in order to fly or enter a federal facility, and explicitly state that Real ID will be considered for a number of other functions including receiving a passport, military common access card, and transportation worker identification card (p. 17).**

PASS FAIL INC ☐ ☒ ☐	**Private-sector piggybacking.** The "common machine-readable technology" on Real IDs would allow for easy, computerized transfer of the data on the cards not only to the government but also to private parties. Already, many bars and clubs collect all their customers' information by swiping driver's licenses handed over to prove legal drinking age. There is concern that even if the states and federal government successfully protect the data, machine readability will result in a parallel, for-profit database on Americans, free from the limited privacy rules in effect for the government. (*"FAQ"*) **The regulations do not protect individuals from private sector piggybacking. They state that protecting machine readable technology from private sector access is outside the scope of DHS responsibility and leave such regulation to individual states (p. 73). They decline to require that data on the card be encrypted, leaving it open to reading by a private-sector entity.**
PASS FAIL INC ☐ ☒ ☐	**A single interlinked database.** Will the national database be secure from identity thieves and criminals? Advocates argue that the government's poor record at information security and at preventing insider fraud and abuse may mean Americans are less secure as a single national database makes their information more vulnerable and available from more sources. (*Center for Democracy and Technology, "Unlicensed Fraud"*) **The regulations fail on this issue because they require creation of a national database of interlinked state systems (p. 149). DHS denies there will be a national database, but having one central database in Washington or 50 state databases in the individual states, all linked together with identical comments and an identical form, are effectively the same thing. Moreover the regulations explicitly provide that the Department is "committed to the expedited development and deployment of a common [federated] querying service" (p. 26).**
PASS FAIL INC ☐ ☒ ☐	**Insider fraud.** Advocates have also argued that linking databases will give more and more parties "legitimate" access to the data and that information that can be accessed by multiple disparate parties is a recipe for fraud. Fraud by DMV officials is a major cause of identity theft. **Insider fraud is one of the core problems with Real ID. It is not solved in the regulations nor is it clear that there is a solution to the problem as the act is written. The regulations attempt to address this issue by requiring criminal background and credit checks for employees (p. 153), but it is unclear whether or how much such checks would reduce fraud by the many insiders who do not have a troubled record. Such fraud is almost certain to continue, especially in light of the fact that the perceived authenticity of a Real ID license is likely to make it even more valuable on the black market and create a new wave of insider fraud. (For more information on identity theft and Real ID please see comments by the Privacy Rights Clearinghouse available here: http://www.privacyrights.org/ar/real_id_act.htm)**

PASS ☐ FAIL ☒ INC ☐	**Accountability vacuum.** Security experts note that a system is only as secure as its weakest point. There is no mechanism to guarantee that every DMV follows adequate procedures and the linked distributed system makes accountability extremely difficult to enforce. Further, a single breach at a single DMV could compromise the entire system and expose the data of every American who drives. **A state that finds its citizens' data threatened or stolen due to the negligent practices of another state will have no remedy or recourse under the regulations. While securing private information is vital, the regulations provide no guidance as to how states should do so, or what a state can do if other states' efforts fall short. (p. 150). The regulations state that information sharing between states will be a state function with only limited oversight from DHS (pp. 25-26).**
PASS ☐ FAIL ☐ INC ☒	**Protecting source documents.** Real ID requires all source documents for licenses to be retained either electronically or in storage at the DMV. Protecting these valuable document troves from security breaches will require the devotion of significant resources to new computer hardware and software, systems redesign, security consulting, and staff expansions. It is expected that identity thieves will quickly recognize that the DMV's records are a central location for obtaining all the documents they need to commit fraud. (*"Real Costs"*) **The regulations state that securing private databases must be part of state physical security measures, but provide no guidance as to how states will secure this information (p. 150).**
PASS ☐ FAIL ☒ INC ☐	**Effect on state privacy laws.** States have varied privacy and safety laws governing everything from what information can be collected for the purpose of driver's licensing, to what information can be contained on the machine-readable component of an ID card. It is expected that Real ID will force state legislatures to alter or repeal many of these laws – potentially creating new privacy and security problems. (*See "The Impact of Real ID on Current State Laws," and accompanying chart prepared by Stanford University Law School*) **The regulations allow states to impose greater privacy protections than required by regulation and allow some flexibility to protect the confidentiality of address information (p. 143). But they are silent on how state laws that are directly in conflict with the Real ID regulations will be affected (p. 120). For example, in order to protect against identity theft, California law allows the DMV to destroy all records that are no longer necessary to issue a license. In New Hampshire, the wholesale sharing of motor vehicle information with other states is prohibited and share sharing shall only be "on a case to case basis." Such state laws would have to be changed in order to secure Real ID compliance (p. 159).**

Impact on the States	
PASS ☐ FAIL ☒ INC ☐	**Unfunded mandate.** Real ID requires sweeping changes to state driver's licenses and the systems by which those licenses are administered. A partial cost estimate issued jointly by AAMVA, NGA, and the NCSL estimated the cost of Real ID on the states at $11 billion. Congress has currently appropriated $40 million to offset Real ID costs. (*NCSL et al, "Impact Analysis"*) **The regulations acknowledge that the AAMVA-NGA-NCSL estimate is inadequate and that the actual cost of Real ID will be $23.1 billion (p. 106).**
PASS ☐ FAIL ☒ INC ☐	**Effect on DMVs of standardizing data elements.** Real ID imposes a requirement for uniform data elements on state IDs. Standardizing these elements will vary in difficulty from state to state, but in many cases will require the reprogramming of multiple interlocking state databases, computer entry screens, communications protocols, and paper forms. (*ACLU analysis, "Real Burdens: the Administrative Problems REAL ID Imposes On The States"*) **The regulations require states to share all their driver's license information. This will force states to make costly changes to their Information Technology (IT) systems. The regulations provide no guidance on how such changes are to be effected, and place the entire burden of constructing a data-sharing system on the states (pp. 27 & 149). The regulations also impose additional onerous IT requirements, such as requiring states to retain the photographs of all applicants (not just license holders) (p. 131) and retaining all name information on applicants even if they subsequently change their name (pp. 66 & 131).**
PASS ☐ FAIL ☐ INC ☒	**Effect on recent improvements to state IT systems.** The NCSL reports that 21 states have invested $289 million over the last five year to modernize their DMV information systems. Real ID may force much of this work to be thrown out. (*NCSL et al, "Impact Analysis"*) **Because the regulations do not provide guidance regarding how data sharing will be implemented, it is unclear to what degree states will be able to rely on their previous (costly) IT system overhauls (pp. 27 & 149).**
PASS ☒ FAIL ☐ INC ☐	**Cost of processing new applicants.** Real ID's requirement that it be used for a host of federal purposes may force millions of Americans to sign up for driver's licenses or ID cards. This would result in an unplanned wave of new applicants swamping DMVs. **The regulations assume that there are 240 million licensees. This number seems to encompass most of the ID holders in the US.**

PASS FAIL INC ☐ ☒ ☐	**DMVs will have to reprocess existing licensees.** The document verification process will also have to be completed for the entire population of people (approximately 200 million) who already have current licenses and IDs. Motor vehicle administrators have complained that this will significantly strain DMV resources. (*"Real Burdens"*) **Because the regulations state that all license holders will have to reply in person to receive a Real ID-compliant license (p. 146), DMVs will not be able to take advantage of the ease of processing licenses over the Internet or through the mail. This change will substantially increase the number of people coming to DMVs and significant strain existing resources.**
PASS FAIL INC ☐ ☒ ☐	**Diversity in licensing systems.** States have chosen a variety of methods for issuing licenses. In Kentucky, for example, licenses are handled by court clerk offices, in Alabama by probate judges, in Nebraska by county treasurers, and in Oklahoma by third party vendors. It is unclear whether Real ID regulations will continue to allow states to operate under these different licensing models. (*"Motor Vehicle Administrators Survey"*) **The regulations do not address these issues, and taken as a whole the regulations make it clear that many states will have to drastically alter their licensing schemes.**
PASS FAIL INC ☐ ☒ ☐	**Appeal process.** Mistakes in existing DMV and other databases may result in delays or even inability to get a drivers' license. In light of this high penalty some type of appeal process will have to be created to deal with mistakes and document errors. **The regulations contain no appeals process for individuals who are the victims of errors in the information used to verify their identity. Instead, individuals will have to correct errors with the database owners (pp. 56 & 136). (States, however, can appeal determinations made by DHS that their systems are not Real ID compliant [p. 158].)**
PASS FAIL INC ☐ ☒ ☐	**Expertise in immigration law.** The act bars states from issuing compliant IDs to any non-citizen who cannot prove their identity and present verified documentary evidence that they are covered by one of an enumerated number of lawful immigration statuses. But the complexity of our immigration laws make it likely that identifying and processing a variety of different immigration documents will be a difficult task. (*"FAQ"*) **The regulations require intimate familiarity with multiple immigration documents in order to issue a Real ID in two contexts. First, DMV employees have to be trained to recognize a number of types of fraudulent documents for proof of citizenship (visa, permanent resident card, EAD, Certificate of Citizenship, or Certificate of Naturalization). Second, DMV employees will have recognize the very obscure immigration documents that prove that an individual is not eligible for a Social Security number (those that prove an alien "is currently in a non-work authorized non-immigrant status") (pg. 43).**

PASS FAIL INC ☐ ☒ ☐	**Lawful status not described in the Act.** Immigration advocates have complained that there are a number of ways that an immigrant can be in the country lawfully that are not described in the act. It is not clear if these individuals can qualify for a Real ID. **Because the regulations do not expand the description of lawful status for purposes of obtaining a Real ID beyond statutory guidelines, numerous individuals, such as asylum seekers, cannot get any type of Real ID, even though they are in the country lawfully.**
PASS FAIL INC ☐ ☒ ☐	**"Full Legal Name" particularly onerous.** The Act requires that compliant identity papers contain individuals' full legal names. However because a portion of the population possesses extremely long names, the name for licenses is recommended to be at least 100 (some say 126) characters long. For man states this would mean redesign of their entire database structures and program interfaces to standardize how information is entered in each field office and how it is stored centrally. They will also have to revise information and application forms, and train staff to verify legal name. (*"Real Costs"*) **The regulations require states to retain 39 characters of an individual's legal name for the front of a license and 125 characters for the machine readable zone (MRZ) of the license, placing a new burden on the states by requiring them to modify their systems to collect this information in two different ways in order to secure it in their databases and place it in the MRZ (pp. 66, 142 & 144).**
PASS FAIL INC ☐ ☒ ☐	**"Full legal name" requirement reaches beyond DMVs.** Legal name changes in DMV systems will impact other, linked systems such as CDLIS (a commercial license database) and PDPS (a problem driver database) as well as serving as the access point for other systems, including law enforcement, insurance companies, and the election registry. (*"Real Costs"*) **The regulations provide no guidance on how states are to reconstruct their information systems (p. 149).**
PASS FAIL INC ☐ ☒ ☐	**Limited real estate on physical cards.** Many states may have to redesign the face of their ID cards – where space is already limited – to include longer names and new data elements such as principal address. (*"Real Costs"*) **The regulations do not provide any flexibility regarding the information to be placed on the front of the card (p. 142).**
PASS FAIL INC ☒ ☐ ☐	**License holders with multiple addresses.** If mailing address and principal address differ, states will have to retain both – one for printing on the license and one for correspondence. Some individuals – such as students and those who own multiple homes – reside in more than one state. **Regulations address this issue by assuming individuals will choose one principal address, which will be the place where they maintain their "true, fixed and permanent home" (p. 129).**

PASS ☐ FAIL ☒ INC ☐	**Creation of interconnected database.** Real ID requires that each state provide all other states with electronic access to the information contained in its motor vehicle database. Because state DMVs each have their own IT systems with different level of capability and interoperability DMV officials believe this will be an extraordinarily difficult task. (*"Motor Vehicle Administrators Survey"*) **The regulations require a national database of interlinked state systems both for ascertaining whether an individual has a license in another state and for sharing motor vehicle information (p. 149). The regulations provide no guidance on how states are to share information, and place the entire burden constructing a data sharing system on the states (pp. 27 & 149). Nor do they mitigate any of the requirements that states standardize information in their IT systems.**
PASS ☐ FAIL ☒ INC ☐	**Cost of data sharing**. A system similar to that mandated by Real ID, the commercial driver's license pointer system (CDLIS), which covers truck drivers and other commercial drivers, costs roughly $0.08 per month/per record, according to the AAMVA. At the same cost, the price for covering the roughly 200 million current US license holders under Real ID would be $192 million per year. However, since the Real ID database will include significantly more information than CDLIS, this figure would likely be be much higher and it is unclear how this cost burden would be met (and by whom). (*"Real Costs"*) **The regulations indicate that data sharing is likely to be costly. DHS estimates the total for information sharing and IT services to be $1.4 billion. The regulations note that states already use information systems like CDLIS and indicate that it may provide a model for information sharing (p. 27), but provide no guidance for implementing Real ID's much more substantial information-sharing requirements (p. 149).**
PASS ☐ FAIL ☐ INC ☒	**Document verification.** The Real ID Act includes a requirement that states "shall verify, with the issuing agency, the issuance, validity, and completeness of each document required to be presented" to get a Real ID card. No electronic system or systems currently exist which is capable of performing this task. Particular concerns exists regarding birth certificates because they are issued by over 6,000 separate jurisdictions within the United States and there is no central database of certificates (*"Motor Vehicle Administrators Survey"*) **It is impossible to evaluate whether the regulations solve the problem of document verification because most of the verification databases are in their infancy, and because databases will never exist for verifying address (pp. 48-49). The states are required to find their own methods for verifying documents until electronic databases exist (p. 51).**

PASS ☐ FAIL ☒ INC ☐	**Inadequacies in existing verification systems.** An additional verification problem is that DMVs report that existing database such as SAVE (for verifying immigration status) would be inadequate for Real ID purposes either because they are expensive, inaccurate, or do not provide a timely response. (*"Motor Vehicle Administrators Survey"*) **The regulations fail to address this issue except in a cursory fashion. The fact is that many verification databases that do exist (such as SAVE and SSOLV) are incomplete, inaccurate and so far unable to perform the functions required by Real ID (pg 55).**
PASS ☐ FAIL ☐ INC ☒	**Verification cannot be compelled.** The act requires DMVs to authenticate source documents with issuing entities (such as address checks from public utility companies). Because that process will impose substantial burdens on verifying entities it may be met with resistance. However state DMVS have no power to compel or reward compliance. **The regulations circumvent this problem by stating that, in direct contradiction to the statute, DMVs won't have to verify addresses with the issuing agency. ("The proposed regulation would require States to establish a written policy identifying acceptable documents and how, or if, they will be independently validated or verified." [p. 50]). However, they still require documents like birth certificates to be verified even though there is no existing database of birth certificates from all 50 states.**
PASS ☐ FAIL ☒ INC ☐	**Investigations into Social Security Numbers.** States are required to verify that an individual has a valid social security number – and requires that "[i]n the event that a social security account number is already registered to or associated with another person . . . the State shall resolve the discrepancy and take appropriate action." However it is not clear what "appropriate action" entails nor do state officials have the authority to change the Social Security database. (*"Real Burdens," "Motor Vehicle Administrators Survey"*) **The regulations do not provide any guidance for states on this issue, simply stating, "In the event of a non-match with SSA, a DMV must not issue a driver's license or identification card to an applicant until the information verifies with SSA's database." (p. 137)**
PASS ☐ FAIL ☒ INC ☐	**Document storage.** The act requires storage of electronic copies of source documents for 10 years or paper copies for seven years. DMVs lack the equipment and storage space for document retention. DMVs report that this will have a major impact on their operations – requiring additional staff, new equipment, policy changes, training, the remodeling or redesign of offices, and computer software, development, and storage costs. (*"Real Costs," "Motor Vehicle Administrators Survey"*) **The regulations affirm this requirement and estimate the cost of data systems and information technology at $1.4 billion.**

PASS ☐ FAIL ☐ INC ☒	**Standardizing the machine-readable element.** Many states have already deployed a variety of machine-readable technologies – such as bar codes and magnetic stripes – on the licenses they issue. Real ID's standardization mandates will impose substantial costs on the large number of states that will have to replace their existing machine-readable components. (*"Real Costs"*) **The regulations require states to use a 2-D barcode compliant with PDF417 standard (p. 144). The regulations state that 45 states have 2-D barcodes, plus the District of Columbia (p. 75). It appears that all or most of those barcodes comply with the PDF417 standard. However, if a significant number of DMVs report that they will need to make expensive changes to the format of their bar codes, this may change to a "fail."**
PASS ☐ FAIL ☒ INC ☐	**Additional costs for standardization.** Police departments will have to be equipped with new readers, at significant cost to taxpayers. During the five-year changeover to full 50-state Real ID compliance, numerous data storage systems and sets of readers will have to be maintained simultaneously. (*"Real Costs"*) **The regulations provide no additional funding to offset this concern. They state that the AAMVA-approved barcode can be read by a standard 2-D barcode reader (p. 76), but do not address costs for states that must convert to new machine readable standards.**
PASS ☐ FAIL ☒ INC ☐	**Facial image capture.** The act appears to mandate that image capture must apply not to all license recipients, but to all *applicants*. This will require a new database for pending and failed applications, alterations to the licensing process to change the stage at which an image is captured, and increased personnel and equipment for additional image capture. (*"Real Costs"*) **The regulations confirm that DMVs will face an increased IT burden because they have to save photo images for at least one year for all applicants (not just those that receive licenses), and for ten years for those denied licenses because they are suspected of fraud (pp. 67 & 131).**
PASS ☐ FAIL ☐ INC ☒	**Facial recognition technology.** The act's requirements for "facial image capture" may require states to purchase facial recognition technology and begin strictly regulating how photos are taken to correct for variations in lighting, expression, camera type, background, and the exposure of facial characteristics, such as facial hair, glasses, headscarves, etc. Facial recognition technology is often costly, inaccurate and difficult to implement. (*"Real Costs"*) **The regulations do not fully address the issue of face recognition. While they take some steps consistent with the technology, such as prescribing the physical appearance of individuals in photos (p. 142), they are silent on whether photos will be used as part of a facial recognition system.**

PASS ☒ FAIL ☐ INC ☐	**Security clearance.** Real ID requires that state employees who are authorized to manufacture ID cards must be subject to "appropriate security clearance requirements." It is not clear what standards states should set in disqualifying employees or hiring new employees. The fact that some states contract with private entities for ID production further complicates this issue. (*"Real Burdens"*) **The regulations do set down clear standards for state employees who should be checked: those who "have the ability to affect the recording of any information required to be verified, or who are involved in the manufacture or production of REAL ID driver's licenses and identification cards, or who have the ability to affect the identity information that appears on the driver's license or identification card" (p. 153). They also make clear what the standards of those checks should be: those set forth in TSA's Hazardous Materials Endorsement program (HAZMAT program) and Transportation Workers Identification Credential (TWIC) program (p. 85).**
PASS ☐ FAIL ☐ INC ☒	**Security clearance and labor contracts**. Security clearance requirements may run afoul of contract stipulations and union rules. States may need to provide employees disqualified under new regulations with alternative employment or severance. (*NCSL et al, "Impact Analysis"*) **The regulations are incomplete because they do not address how workers' collective bargaining agreements will affect whether they can be asked to undergo background checks.**
PASS ☐ FAIL ☐ INC ☒	**New training requirements.** Under Real ID state employees must undergo "fraudulent document recognition training programs." It is not clear what these programs entail or the impact on the cost of issuing licenses. (*"Real Burdens"*) **The regulations do saddle DMVs with the increased cost and burden of training employees in fraudulent document recognition without providing any funding. They do not elaborate on this training requirement except to affirm that it must be part of every DMV security program (p. 151). It is expected to take approximately 2 hours and cost $44 per person in lost man hours (p. 112).**
Constitutional Impact	
A. Burdens on constitutional rights of the states.	

PASS	FAIL	INC	
☐	☒	☐	**Federalism and the Tenth Amendment**. States have always been the exclusive regulator of driver licensing. Each state has developed an extensive statutory and regulatory framework in this area, and each state employs workers to carry out that statutory and regulatory scheme. The Tenth Amendment provides that "[t]he powers not delegated to the United States by the Constitution, nor prohibited by it to the states, are reserved to the states respectively . . . ." The REAL ID Act seizes the power reserved for the states by federalizing drivers licensing. Real ID was vigorously opposed by the organizations representing the states and seems to violate the Tenth Amendment. (*See ACLU analysis, "Constitutional Problems with the REAL ID Act of 2005"*) **The regulations violate the Tenth Amendment by seizing state authority over licensing and by forcing states to engaged in regulation on behalf of the federal government. The regulations argue that Real ID does not violate the Tenth Amendment because the burden will fall on citizens rather than on "the State as a sovereign." This is an incorrect reading of the law. The test under existing law is whether a state (as sovereign) has been compelled to adopt a federal program, not whether the program acts directly on the state. The regulations do not address the states' traditional authority in the field of drivers licensing.**
PASS	FAIL	INC	
☐	☒	☐	**The Anti-Commandeering Doctrine and the Tenth Amendment.** The REAL ID Act requires states driver's licensing officials to perform two exclusively Federal functions: enforcing immigration laws and creating a federal ID card. Constitutional and statutory schemes governing immigration law make clear that immigration enforcement is entirely a Federal function. Additionally the Real ID Act turns state drivers' licenses into Federal identity documents, necessary for official purposes like entering a Federal facility. According to the Supreme Court's anti-commandeering doctrine, if the Federal government wants to conduct interior immigration enforcement or create Federal identity cards it must hire and pay Federal government employees to do so, rather than forcing states' licensing employees to carry out this activity. (*"Constitutional Problems with the REAL ID Act"*) **The regulations do not address the main constitutional issue: whether imposing penalties on citizens when states don't act amounts to a violation of the Anti-Commandeering doctrine. The regulations claim that "the proposed rule would not formally compel any State to issue driver's licenses or identification cards that will be acceptable for federal purposes" and instead that it is pressure on individual citizens that will force compliance with Real ID (p. 120). But this doesn't answer the main question: if a state can only reject federal law at the expense of denying its citizens access to basic aspects of American life like entering a federal facility or traveling on a plane, does this rise to the level of coercion necessary to trigger constitutional scrutiny?**

B. Burdens on constitutional rights of individuals.	
PASS ☐ FAIL ☒ INC ☐	**Free exercise of religion and the photo requirement.** Real ID requires, without exemption, that a digital photograph appear on each ID. This requirement violates the religious beliefs of Amish Christians, Muslim women and others and impacts the free exercise of their religion. (*"Constitutional Problems with the REAL ID Act"*) **The regulations affirm that in order to receive a Real ID, every applicant must have a photo taken. It acknowledges individual religious objections but states that security requirements override those objections (pp. 67-68).**
PASS ☐ FAIL ☒ INC ☐	**Free exercise of religion and Social Security numbers.** Some Christian sects believe that "the enumeration" of individuals is tantamount to stamping them with the Mark of the Beast referred to in the Biblical Book of Revelations. Therefore due to these religious beliefs, certain citizens may not have the Social Security Number or Social Security Card necessary to gain a Real ID. (*"Constitutional Problems with the REAL ID Act"*) **The regulations do not provide for a religious exemption in this context. They require that every applicant for a license have a Social Security number. The only way under to establish ineligibility for an SSN is for an alien to "present evidence that he or she is currently in a non-work authorized nonimmigrant status" (p. 134).**
PASS ☐ FAIL ☒ INC ☐	**Gender designation requirement.** Real ID requires inclusion of each person's gender on his or her license. Many states and municipalities recognize the unique difficulties faced by issuing identity licenses to transgender people, and, accordingly, provide for exceptions to gender-listing requirements. The act would preempt those exceptions and may violate of the Constitution's Equal Protection Clause for transgender individuals. The gender classification will also lead to data inconsistencies within the databases that will "red flag" transgender people when their licenses are scanned by government officials. (*"Constitutional Problems with the REAL ID Act"*) **The regulations do not address this issue.**
PASS ☐ FAIL ☒ INC ☐	**Burdens on right to travel.** The U.S. Supreme Court has repeatedly recognized a constitutionally protected right to travel. By ruling a state out of compliance the federal government may keep a state's residents from boarding a plane and possibly other modes of transportation, which would likely burden their First Amendment-protected right to travel. The situation is particularly acute for residents of Hawaii or Alaska who often have no choice but to fly or travel via federally regulated modes of travel such as plane or ship. (*"Constitutional Problems with the REAL ID Act"*) **The regulations affirm that after the effective date of the act, a Real ID will be required to board a plane (p. 129). They do not address the constitutional issue.**

PASS FAIL INC ☐ ☒ ☐	**Burdens on right of assembly**. The First Amendment protects "the right of the people to peaceably assemble." Blocking individuals from non-compliant states from using their licenses to enter federal buildings seems to burden that right. (*"Constitutional Problems with the REAL ID Act"*) **The regulations affirm that after the effective date of the act, a Real ID will be required to enter a federal facility (p. 129). They do not address the constitutional issue.**
PASS FAIL INC ☐ ☒ ☐	**Burdens on right of petition**. The First Amendment also guarantees the right to "petition the government for a redress of their grievances." Lack of a Real ID compliant license would bar a citizen from a face-to-face meeting with his or her elected or appointed government representatives. In fact, many statutory and regulatory schemes *require* individuals to at times present themselves before elected or appointed officials to raise their grievances. Blocking individuals from entering their representatives' offices, Federal agencies or courthouses would be burden on the right to petition the government for redress. (*"Constitutional Problems with the REAL ID Act"*) **The regulations affirm that after the effective date of the act, a Real ID will be required to enter a federal facility (p. 129). They do not address this constitutional issue or the related question of whether barring access to a courthouse, the ability to bring or defend a lawsuit or witness a court proceeding would also be prohibited under the Constitution.**
PASS FAIL INC ☐ ☒ ☐	**Lack of procedural or substantive due process.** The Real ID Act fails to provide for a system for individuals to access government records about them, challenge inconsistencies and correct data errors concerning their files. The Real ID Act's failure to include a procedure whereby individuals can quickly, efficiently and permanently reverse data errors is likely to impact a number of substantive rights – such as receiving government benefits or boarding a plane – and violates the Constitution's guarantees of both procedural and substantive Due Process found in the Fifth and Fourteenth Amendments. (*"Constitutional Problems with the REAL ID Act"*) **The regulations contain no appeal process for individuals who are confronted with errors in the information used to verify their identity. Instead individuals will have to correct errors with the database owners (pp. 56 & 136). The regulations do not address the constitutional issue.**

Statement of Jay Maxwell
to
U.S. Senate Committee on Homeland Security and Governmental Affairs

Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia

Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers' Licenses and Identification Cards

March 26, 2007

CLERUS SOLUTIONS LLC

Mr. Chairman and Members of the Subcommittee, my name is Jay Maxwell and I am the President & CEO of Clerus Solutions, an organization dedicated to assisting the states and the Federal government with implementing secure identification as called for in the 9/11 Commission Report. I have over 25 years experience working with state and federal agencies, specializing in the implementation of nationwide, large-scale information systems that involve the driver license program area. I designed and implemented the National Driver Register's Problem Driver Pointer System (PDPS) while at the National Highway Traffic Safety Administration (NHTSA) in the 1980's. I then leveraged that work in the development and implementation of the Commercial Driver License Information System (CDLIS), which I managed while at AAMVAnet, Inc., a subsidiary of the American Association of Motor Vehicle Administrators (AAMVA).

I greatly appreciate this opportunity to submit testimony for your consideration as you review efforts to secure drivers' licenses and identification cards. My testimony will be focused on my direct experiences working with state and federal agencies that have been trying to solve the driver license identity issue over the past 25 years.

Terrorists, criminals and problem drivers want to have multiple driver's licenses. We know, based on the conclusions and recommendations of the 9/11 Commission and the results of analyses in states such as North Carolina and Illinois, that these individuals indeed do hold multiple licenses, some under the same name, some under completely different identities. To say the least, these elements of society have proven themselves to be detrimental to the safety, security and welfare of the citizens of this country.

These bad actors have taken advantage of existing technical and procedural intra-state and inter-state vulnerabilities that have existed for years. These vulnerabilities create a medium through which it is relatively easy to steal another person's identity or create a fake one for nefarious purposes. State driver licensing agencies and the Federal government have known about this problem for decades and have been working responsibly as a team to reform the current system.

Federal legislation passed by Congress in 2004 (the Intelligence Reform Bill) and 2005 (the Real ID Act ("RIDA")) have catalyzed this necessary reform and have received much publicity. While they are important steps to enable reform, these laws do not promote revolutionary ideas. Rather, they support what have been the next logical steps in a progression of improvements occurring in the United States over many years. Benefits of this reform will be significant, and will include:

- improved homeland security;
- improved highway safety;
- reduction of identity theft and fraud;
- reduction of benefits fraud; and
- reduction of voter fraud.

In order to put the current activities into context, it is important to understand events that happened in the past, why we have developed systems to respond to these events, and

how the current environment makes Real ID more important than ever. A description of those past events is included as Attachment A to this testimony.

Driver's license reform is sure to be a complex endeavor, requiring the integration of many disparate systems and interstate and interagency cooperation. Attachment A indicates that a roadmap toward delivering effective and responsible reform already exists. However, there are several impediments that are unnecessarily delaying progress. These include:

- Misunderstanding of the effectiveness of current information systems upon which Real ID must rely;
- Cost estimates provided to date, based on incomplete guidance from DHS, have been used by some as an excuse to delay necessary reform;
- Delay of pilot programs; and
- Inappropriate instillation of privacy fears to delay responsible driver license and ID card reform.

Misunderstanding of the effectiveness of current information systems upon which Real ID must rely.

There are two major information system requirements to Real ID:

- A system to provide source document verification; and
- A system to detect and prevent the issuance of duplicate licenses and ID cards.

Both of these systems are needed to implement the recommendation of the 9/11 Commission to improve identification security.

Source Document Verification

RIDA does not state that source document verification must be electronic, but in practical terms, there is no other way for states to fulfill the requirement. For example, there is no reasonably scalable or cost-effective method through which Idaho's driver license agency can manually verify a Georgia birth certificate. Information systems must be put in place to allow Idaho to electronically verify, in seconds, that the Georgia birth certificate data appears to be legitimate.

A few years ago, the National Association of Public Health Statistics and Information Systems (NAPHSIS) developed the Electronic Verification of Vital Events (EVVE) system to make birth and death information available to SSA. State driver licensing agencies have now started to obtain access to EVVE. However, there are some realities that must be considered before anyone can say that EVVE is an effective means to verify birth certificates:

- NAPHSIS and its members have identified a timeline for connecting all state vital records agencies to EVVE. However, once that connection is made, the quantity and quality of the data maintained by the state vital records agencies will govern the effectiveness of EVVE for Real ID purposes. A preliminary nationwide review of state vital records indicates that not all states have accurate, complete

and automated data of the type needed by Real ID. The next question to be answered, then, is what will it take, from a cost and time standpoint, to automate the needed data? That is unknown at this time.

- ❖ Driver license agency use of EVVE has been very limited to date. Currently, there are only a handful of driver licensing agencies that access EVVE, and they do not rely on it to make licensing decisions, because too little of the data is available.

Although we may be able to connect all state vital records agencies to EVVE within two to three years, we do not know when the vital records data will be complete and accurate. We must also work to connect state driver license agencies to EVVE, as the vast majority of states are not connected to it today.

Some driver license agencies now have access to the Systematic Alien Verification for Entitlements ("SAVE"), to verify immigration documents. Again, applying practicality to that statement, the states are using SAVE in an exception environment and do not have SAVE integrated into their driver license issuance information systems. This lack of integration is an important issue. By handling SAVE in a stand-alone manner, driver license clerks have the option to override "red light" conditions returned by SAVE. This opens the door for fraud. We must design access to all of the source documentation verification systems in such a way that driver license clerks cannot override the results.

The most effective verification tool that states have available to them today is the on-line check with the Social Security Administration (SSA). The system used by most states is called the Social Security On-line Verification System (SSOLV). SSA has the most complete, accurate set of data that can be used for verification that the name, birth date and Social Security Number (SSN) are a matched set (i.e. the SSA's files indicate that the name, birth date and SSN sent by the driver licensing agency matches the name, birth date and SSN of a singular record on the SSA file). SSOLV will also return information that indicates that the person is deceased, if that is known to SSA.

The shortfall of SSOLV is that the system cannot verify that the person applying for the license in the state "owns" the identity data on the SSA file. If I obtained the name, birth date and SSN of anyone other than myself, I could pose as that person and, if the state checked the data with SSA, SSOLV would return a "green light", indicating that the data matched with their file. This leaves open the door for fraud, as is highlighted in sections 3 & 4 of Attachment A to this testimony.

The conclusion for source document verification, then, is that we should start work now to create an effective infrastructure for it, but we need to be realistic in the near term with regard to its effectiveness. With that in mind, there is an option that can enable near-term effective identity verification. I will discuss this option later in this testimony.

Detecting and Preventing the Issuance of Duplicate Licenses and ID Cards

Let me start by saying that the Real ID Notice to Proposed Rulemaking ("NPRM") undermines the intent of the 9/11 Commission when it states that driver license agencies only need to exchange information on possession of Real ID licenses. By leveraging existing data currently maintained by state driver licensing agencies, we can readily identify existing fraudulent duplicate licenses and ID cards and build an immediate

foundation for a trusted driver's license. Exchanging data on a date-forward basis, as proposed by the NPRM, needlessly allows existing fraud and identity theft to continue for years to come. Attachment B shows a graphic representation of a comparison between the approach proposed in the NPRM and an approach proposed by the states of North Carolina and Kentucky. The NPRM approach would not significantly diminish existing fraud and ID theft for several years. The approach favored by North Carolina and Kentucky would start significantly decreasing fraud and identity theft within six months of the start date for the effort. In addition, the approach proposed in the NPRM would cost $8.5 billion, as estimated by the NGA, NCSL, and AAMVA report. The approach favored by North Carolina and Kentucky would cost less than $1 billion.

Attachment C provides some detail regarding the North Carolina/Kentucky approach. More information can be obtained directly from the North Carolina Division of Motor Vehicles.

The conclusion on this topic is that the method proposed by North Carolina and Kentucky would detect and eliminate the existing driver license and ID card fraud within two years, at a reasonable cost.

If DHS pursues the approach favored by North Carolina and Kentucky, within two years, all state driver license databases will be cleansed such that the occurrence of driver license and ID card fraud will be negligible. That being the case, the existing driver licenses, already issued, will be the best "source document" that can be used to link a person to an identity (because the driver licenses and ID Cards contain a photo of the person). Used in combination with checks of other databases, such as the SSOLV described above, the cleansed driver's licensing system forms the basis for a highly dependable document verification program. This is the option that I referred to in the above discussion of source document verification.

Cost estimates provided to date, based on incomplete guidance from DHS, have been used by some as an excuse to delay necessary driver license and ID card reform.

States will need significant funding to implement Real ID. However, cost estimates they have provided were based on incomplete guidance from DHS and therefore may be substantially misleading. Unfortunately, some may use these estimates as an excuse to delay necessary driver license and ID card reform.

Real ID could very well cost $12 to $15 billion if we choose the wrong way forward. However, I believe that there are ways to implement the Real ID program that cost significantly less. One suggested method is provided as Attachment C to this testimony. It is very likely that others have cost-effective ideas that will move the Real ID program forward. We need to test these ideas.

I urge Congress not to be swayed by those that want to use the existing estimates as an excuse to delay necessary reform.

Delay of Pilot Programs

When comparing the progress made to date with Real ID implementation in contrast to the progress made with the Federal Commercial Driver License (CDL) program over the same time frame, there is a marked difference.

Nineteen months after the Commercial Motor Vehicle Safety Act of 1986 was passed, USDOT had selected two lead states for the program, Nebraska and New York, and those states had contracts in place with integrators to develop the infrastructure for the information system required by the Act, the Commercial Driver License Information System (CDLIS). CDLIS was designed, developed, tested and implemented within 27 months after passage of the Act.

Real ID, on the other hand, is not likely to have progressed beyond an initial pilot during the same time frame, despite the huge body of work done by the states to identify the problems and a plan of action prior to passage of RIDA, as described in Attachment A.

Thankfully, DHS recently established a program office for Real ID. The newly appointed head of that program office, Darrell Williams, appears to be providing the leadership that is needed to move the program forward. . However, I do not believe he has adequate program funding and staffing to implement Real ID nationwide.

I ask Congress to significantly increase the budget for the Real ID program office for FY2008.

The only way we will be able to accurately estimate the cost of implementing and operating Real ID is to start implementing pilot programs that test technologies and best practices specifically related to the program. Congress appropriated $40 million in FY2006 for Real ID. To date only $3 million has been obligated and very little of that has been spent.

I urge Congress to direct DHS to release the FY2006 appropriations for pilot efforts aimed at identifying technologies, best practices and accurate costs for Real ID.

Inappropriate instillation of privacy fears to delay responsible driver license and ID card reform

Privacy issues are of great concern to all. We must ensure that any information systems, processes, and procedures that are developed for Real ID protect the privacy rights of individuals. Both privacy and security are suffering now, under the current driver license issuance process. I believe that both will benefit greatly from Real ID.

I submit to you that the current state of driver licensing provides very little in the way of privacy protection. In fact, the current situation fosters an environment of identity theft.

Recent studies by states such as North Carolina and Illinois, applying facial recognition technology to their intra-state driver photo databases, have uncovered the scale of the fraudulent license problem. In North Carolina, one analysis discovered an individual that had obtained 45 North Carolina driver licenses under 45 different identities. Of particular note, all 45 identities were verified against SSA's Social Security database – indicating this individual had stolen the identities of U.S. citizens from other states. To accomplish

this, he simply appropriated the name, birth date and Social Security number of other people. Illinois has had similar cases.

Based on the work performed in North Carolina, we estimate the 0.3% of the population hold fraudulent driver licenses. Based on a total driver population nationwide of 250 million drivers, there are likely 750,000 people holding fraudulent licenses nationwide.

States need to exchange information on all drivers and ID card holders to detect and prevent this identity theft. Real ID provides a mechanism for that exchange. I encourage Congress to provide DHS and the states the resources that they need to implement this much needed program.

Additional Thoughts and Concerns

Encryption of the Machine Readable Data on a Driver's License

There is debate regarding encrypting the data stored electronically on driver's license and ID cards. I hold to a position that the data stored on the machine readable technology (i.e. the bar codes and magnetic strips), should not be encrypted, as long as that data is restricted to the data shown on the face of the license. Any data stored electronically on the license that is in addition to that which can be found on the face of the license may need encryption, depending on the nature of the data.

My position is founded on the following:

- Data found on a bar code or magnetic strip cannot be read without the owner first handing the document to another individual. Therefore, the owner of the document is aware that they handed the license to someone for a purpose.

  If the document is lost and someone with nefarious intent finds it, they would have plenty of time to manually capture the data from the front of the license. Consequently, the argument that the machine readable technology assists them is very weak.

- Many entities probably should be allowed to read the data. Therefore, if the data were to be encrypted, the decryption key would need to be readily available to many people, including vendors supplying product to support law enforcement, the courts and others that would have access to the data. It would be difficult to keep the decryption key confidential.

There are other issues such as costs to maintain such an infrastructure, the problems caused when an authorized user would be denied access to the data because of computer or clerical problems, etc.

In light of the above, I don't believe that instituting an encryption scheme will provide the wanted benefits, which in my mind relate to privacy issues, but it will cause other problems and increase the cost of the program.

In lieu of encrypting the data, I propose that federal law must dictate that anyone that reads the data must post a notice to the owner of the card regarding the uses to which the data will be applied. The owner of the card would then have the option to decline to present the card to the entity that wishes to read the machine readable data.

In conjunction with this notice, there should be penalties to those that read the card if they indeed use the data for purposes unrelated to those stated to the owner of the card. Those penalties should be serious and significant.

Undocumented Aliens

State driver licensing agencies should not regulate immigration activities. Immigration is a federal responsibility. Some have argued that RIDA puts state driver licensing agencies in a position of regulating immigration. I disagree with that statement. Implementation of RIDA does not put the driver license agency in a position of regulating immigration.

Existing driver licenses currently owned by undocumented aliens will surface as the country implements Real ID. RIDA provides a mechanism that states can use to continue to license this segment of the driving population while still improving identification security. States should work collectively with DHS to define the implementation details of the RIDA feature that allows states to issue driver licenses to anyone that does not have verifiable identification documentation.

Thank you again for this opportunity to contribute to this discussion.

BRENNAN
CENTER
FOR JUSTICE

Committee on Homeland Security & Government Affairs

Subcommittee on Oversight of Government Management, the Federal Workforce and the District of Columbia

United States Senate

Statement Concerning the REAL ID Act of 2005

By Wendy R. Weiser and Myrna Pérez
Brennan Center for Justice at NYU School of Law[1]

March 26, 2007

The Brennan Center for Justice appreciates the opportunity made possible by the Subcommittee to provide testimony with respect to the REAL ID Act of 2005. This hearing is entitled, "Understanding the Realities of Real ID"; the reality that we would like Subcommittee members to understand is that millions of Americans do not, and will not, have access to the documents required to obtain a REAL ID. Consequently, important rights and privileges of millions of Americans will be affected, like access to essential federal services and federal buildings, and, for residents of many states, the ability to drive a car or travel by airplane. And that is just the beginning. The pernicious effects of REAL ID will be even greater if its use is expanded and its possession is required to vote or to receive state and local government or non-government services and benefits.

The Brennan Center for Justice is a nonpartisan think tank, public interest law firm, and advocacy organization that focuses on democracy and justice. We have researched extensively the subject of identification and proof of citizenship requirements, especially in the voting context.

There is widespread objection to the REAL ID Act from a broad range of sources. State governments are concerned that the REAL ID Act will be costly and cumbersome to implement. The National Governors Association, National Conference of State Legislatures, and American Association of Motor Vehicle Administrators have estimated that it will cost more than $11 billion dollars to execute the REAL ID Act over the first five years.[2] Civil libertarians are concerned that the REAL ID Act will be discriminatorily applied because it empowers and requires DMV workers to make sensitive and difficult decisions with high-stakes consequences for individuals. Privacy advocates are concerned that the REAL ID Act exposes individuals to greater risks of identity theft. Advocates of

[1] Wendy R. Weiser is a Deputy Director of the Democracy Program and Myrna Pérez is Counsel at the Brennan Center for Justice at NYU School of Law.

[2] Nat'l Governors Ass'n, Nat'l Conference of State Legislatures & Am. Ass'n of Motor Vehicle Admin., *The Real ID Act: National Impact Analysis* 3 (2006), *available at* http://www.nga.org/Files/pdf/0609REALID.pdf.

states' rights are concerned that the REAL ID Act strips state governments of the ability to determine the appearances and purposes of their driver's licenses. All of these concerns are valid. To this list, the Brennan Center adds an important objection: a large number of Americans are not currently in possession of the documents required to obtain a REAL ID, and many are not likely to obtain those underlying documents because they are difficult and costly to obtain.

Under the REAL ID Act, to obtain a state-issued driver's license or non-driver's identification that is acceptable for federal purposes, an individual must present: (1) a photo identity document, or a non-photo identity document that includes both her full legal name and date of birth; (2) documentation showing her date of birth; (3) proof of her Social Security number or that she is not eligible for one; (4) documentation showing her name and the address of her principal residence; and (5) documentation proving her citizenship or her lawful immigration status in the United States.[3] If an individual does not possess or present any *one* of these documents, a state cannot issue her a REAL ID. According to the U.S. Department of State Bureau of Consular Affairs, only about 25% of eligible Americans hold valid passports.[4] As set forth below, a significant number of Americans do not have *any* form of proof of citizenship.

In November 2006, the Brennan Center sponsored a national telephone survey of randomly selected voting-age American citizens conducted by the independent Opinion Research Corporation. The survey found that as many as 7% of United States citizens—which translates into about 13 million individuals—do not have ready access to citizenship documents.[5] These numbers are likely an understatement of the total percentage of Americans who do not have readily available documentation because the survey did not include people under 18 and underrepresented low-income and minority households.[6]

Of those who do have access to citizenship documents, many do not have citizenship documents that reflect their current name.[7] For example, the survey results showed that only 48% of voting-age women with ready access to their U.S. birth certificates have a birth certificate with their current legal name—as opposed to a name they had before marriage, divorce, or other name change—and only 66% have ready access to *any* type of citizenship document with their current legal name.[8] That translates into as many as 32 million voting-age women whose citizenship documents do not show their current legal names.[9]

Citizens with comparatively low incomes are less likely to possess documentation

---

[3] Making Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005, Pub. L. No. 109-13, 119 Stat 231 (codified in relevant part in 49 USCS § 30301 note (2005)).

[4] U.S. State Dep't, Frequently Asked Questions about the New Travel Document Requirements, http://www.travel.state.gov/travel/cbpmc/cbpmc_2225.html#8 (last visited Mar. 26, 2007).

[5] Brennan Ctr. for Justice, *Citizens Without Proof: A Survey of Americans' Possession of Documentary Proof of Citizenship and Photo Identification* 2 (2006), *available at* http://www.brennancenter.org/dynamic/subpages/download_file_39242.pdf.

[6] *See id.* at 1 n.1.

[7] *Id.* at 2.

[8] *Id.*

[9] *Id.*

proving their citizenship. According to the Brennan Center study, at least 12% of voting-age American citizens earning less than $25,000 per year do not have a readily available U.S. passport, naturalization document, or birth certificate.[10] These citizens are more than twice as likely to lack ready documentation of their citizenship as those earning more than $25,000.[11]

The impact that proof of citizenship requirements have on lower income individuals is not surprising considering the costs of citizenship documents. A certified copy of a birth certificate costs from $10.00 to $45.00, depending on the state.[12] A passport costs $97.00.[13] Replacement naturalization papers cost up to $220 and can take up to a year to obtain.[14] If these expenses do not appear onerous, keep in mind that the $1.50 poll tax that the United States Supreme Court found unconstitutional in 1966 has a modern-day value of about $8.79.

Additionally, many elderly persons do not have ready access to documents proving citizenship.[15] According to a survey sponsored by the Center on Budget and Policy Priorities, individuals over the age of 65 are much more likely to lack citizenship documents than those under 65.[16] There are many reasons why a large portion of elderly citizens do not have ready access to proof of citizenship, ranging from documents having been lost because they were not needed in the recent past, to documents having never been issued because a person was born on a reservation or at home, to lost or destroyed documents that cannot be easily replaced because the hospital of birth no longer exists.[17]

The evidence also suggests that people of color will be disproportionately harmed by proof of citizenship requirements.[18] The Center on Budget and Policy Priorities survey found that African Americans were much more likely to lack proof of citizenship

---

[10] *Id.*

[11] *Id.*, *accord*, Robert Greenstein, Leighton Ku, and Stacey Dean, *Survey Indicates House Bill Could Deny Voting to Millions of U.S. Citizens: Low-Income, African American, and Rural Voters at Special Risk* 1 (2006), *available at* http://www.cbpp.org/9-22-06id.htm.

[12] Wendy R Weiser et al., Brennan Ctr. for Justice & Spencer Overton, George Washington Univ. Sch. of Law, *Response to the Report of the 2005 Commission on Federal Election Reform* 4 (2005), *available at* http://www.federalelectionreform.com/pdf/Carter-Baker%20Response.pdf.

[13] U.S. Dep't of State Bureau of Consular Affairs, Passport Fees, http://travel.state.gov/passport/get/fees/fees_837.html (last visited Mar. 26, 2007).

[14] U.S. Citizenship and Immigration Servs., Application for Replacement Naturalization/Citizenship Document, http://www.uscis.gov/n-565 (last visited Mar. 26, 2007); U.S. Immigration Assistance Ctr., Naturalization Frequently Asked Questions, https://www.immigration-bureau.org/c_faq.htm (last visited Mar. 26, 2007).

[15] Families USA, *Citizens Update: Administration Creates Additional Barriers to Medicaid Enrollment* 6 (2006), *available at* http://www.familiesusa.org/assets/pdfs/DRA-Citizenship-Update.pdf.

[16] Greenstein, *supra* note 11 at 3.

[17] *See, e g*, Nat'l Network for Election Reform, *Proof of Citizenship Requirements* 2, *available at* http://www.electiondefensealliance.org/files/PROOF%20OF%20CITIZENSHIP.pdf; Eunice Moscoso, *Medicaid Proof of Citizenship Requirement Could Hurt Poor, Critics Say*, Cox Newspapers, Jan. 21, 2006, *available at* http://www.coxwashington.com/reporters/content/reporters/stories/2006/01/21/BC_MEDICAID_IMMIGRANTS19_COX.html.

[18] While there are other studies finding a disproportionate impact, the Brennan Center survey did not yield statistically significant results for differential rates of possession of citizenship by race, age, or other identified demographic factors.

documents than whites.[19] One explanation for this is that a large number of older African Americans were not issued birth certificates because they were born at home on account of poverty or racial discrimination precluding a hospital birth.[20]

The fact that many Americans do not have documentary proof of citizenship is evident from other contexts in which proof of citizenship requirements have been imposed. For example, Arizona passed a law requiring proof of citizenship in order to register to vote, effective January 1, 2005. In early 2005, election officials in the state's largest county reported that they rejected 75% of applicants for voter registration for lack of proof of citizenship. In the 2006 elections, state officials reported rejecting approximately 21,000 new applications for voter registration.[21]

Similarly, the *New York Times* and the Center on Budget and Policy Priorities reported that U.S. citizens are being adversely affected by new proof of citizenship requirements in the health care context.[22] The Center on Budget and Policy Priorities reported that over a period of seven months, approximately 20,000 Medicaid-eligible individuals were denied Medicaid or lost coverage as a result of proof of citizenship requirements *in the state of Wisconsin alone*.[23] Even when the consequences are as grave as delaying needed surgery or going without needed medication, many individuals do not have and seem to be unable to obtain citizenship documentation.[24]

Any valuation of the benefits of the REAL ID Act must be weighed against its many costs. One of its most significant costs is that it will preclude many eligible individuals from obtaining REAL IDs and hence from enjoying rights, privileges, and benefits dependent on those IDs. The evidence shows that many Americans simply do not have ready access to proof of citizenship documents which are required to obtain REAL IDs.[25] The evidence further shows that the proof of citizenship requirements of the REAL ID Act will disproportionately and adversely affect women, elderly and poor persons, and people of color. Those individuals who cannot obtain REAL IDs will suffer real deprivations; indeed, there are real world examples of American citizens forgoing needed rights and services like registering to vote and receiving medical care because they were unable to provide documentation of citizenship. In contrast to the high costs of the REAL ID Act, the additional security benefits provided by the REAL ID Act will be negligible.

We therefore respectfully urge this Subcommittee to support the repeal of the REAL ID Act.

---

[19] Greenstein, *supra* note 11 at 1, 3 (finding that 8.9% of African Americans lacked a passport or birth certificate, as compared to 5.5% of whites).

[20] *Id.*

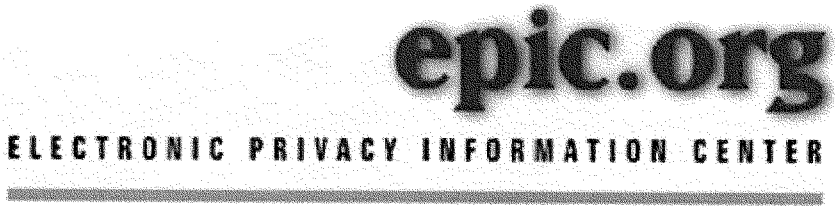
[21] Emergency Motion for Injunction of Plaintiff-Appellant at 10, *Gonzalez v. Arizona*, No. 06-16706, (9th Cir. Sept. 9, 2006). The overall number is likely much larger since a number of counties did not report their figures.

[22] Robert Pear, *Lacking Papers, Citizens Are Cut From Medicaid*, N.Y. Times, Mar. 12, 2007, at A6.

[23] Donna Cohen Ross, *New Medicaid Citizenship Documentation Requirement Is Taking a Toll: States Enrollment Is Down and Administrative Costs Are Up* 4 (2007), *available at* http://www.cbpp.org/2-2-07health.pdf.

[24] Pear, *supra* note 22.

[25] Ross, *supra* note 23, at 1.



Statement Submitted for the Record of

Melissa Ngo
Director of the Identification and Surveillance Project
Electronic Privacy Information Center

Hearing on

"Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers' Licenses and Identification Cards"

Before the

Subcommittee on Oversight of Government Management, the Federal Workforce and the District of Columbia

of the

Committee on Homeland Security and Governmental Affairs
United States Senate

March 26, 2007
Rm. 342 Dirksen Senate Office Building
Washington, D.C.

ELECTRONIC PRIVACY INFORMATION CENTER

Spotlight on Surveillance

March 2007:

Federal REAL ID Proposal Threatens Privacy and Security

EPIC's "Spotlight on Surveillance" project scrutinizes federal government programs that affect individual privacy. For more information, see previous Spotlights on Surveillance. This month, Spotlight scrutinizes the proposed regulations for the national identification scheme created under the REAL ID Act.[1] More than two years after Congress rushed through passage of the REAL ID Act, the Department of Homeland Security ("DHS") announced on March 1 proposed regulations that would turn the state driver's license into a national identity card.[2] The estimated cost of the plan could be as high as $23.1 billion, according to the federal government.[3]

THE DHS REGULATIONS FOR REAL ID

The Department of Homeland Security regulations for Real ID would (1) impose more difficult standards for acceptable identification documents that could limit the ability of individuals to get a state drivers license; (2) compel data verification procedures that the federal government itself is not capable of following; (3) mandate minimum data elements required on the face of and in the machine readable zone of the card; (4) require changes to the design of licenses and identification cards (5) expand schedules and procedures for retention and distribution of identification documents and other personal data; and (6) dictate state collection of personal data and documents without setting adequate security standards for the card, state motor vehicle facilities, or state motor vehicle databases.

Congress is debating legislation to repeal the REAL ID Act in the House and Senate. Maine and Idaho have passed legislation refusing to implement REAL ID. Below is a list of states where anti-REAL ID legislation is pending.

- Arizona
- Arkansas
- Georgia
- Hawaii
- Illinois
- Kentucky
- Maryland
- Massachusetts
- Michigan
- Minnesota
- Missouri
- Montana
- Nebraska
- New Hampshire
- New Mexico
- Oklahoma
- Oregon
- Pennsylvania

The federal agency is imposing more difficult standards for acceptable identification documents. According to the DHS, the only documents that could be accepted by the states to issue these new identity cards would be: valid unexpired U.S. passport or the proposed passport card under the Western Hemisphere Travel Initiative; certified copy of a birth certificate; consular report of birth abroad; unexpired permanent resident card; unexpired employment authorization document; unexpired foreign passport with valid U.S. visa affixed; U.S. certificate of citizenship; U.S. certificate of naturalization; or REAL ID driver's license or identification card.[4]

DHS is also proposing to require the states to change their procedures to verify these identification documents. The states must contact the issuing agency

- Pennsylvania
- Rhode Island
- South Carolina
- Utah
- Vermont
- Washington
- West Virginia
- Wyoming

to verify the "issuance, validity, and completeness of each document required to be presented."[5] The federal agency requires that state DMV workers must physically inspect the identification document and verify the data in the document "with an authoritative or reference database."[6]

The DHS proposal would mandate minimum data elements required on the face of and in the machine readable zone of the card. The following amount of information, at a minimum, must be on the REAL ID card. (1) full legal name; (2) date of birth; (3) gender; (4) driver's license or identification card number; (5) digital photograph of the person; (6) address of principle residence; and (7) signature.[7]

The federal agency would also require changes to the design of licenses and identification cards. The card must include "Physical security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purpose" and "common [machine-readable technology], with defined minimum data elements."[8] DHS is also reviewing card design standardization, "whether uniform design/color should be implemented nationwide for non-REAL ID driver's licenses and identification cards," so that non-REAL ID cards will be easy to spot.[9]

DHS is also expanding schedules and procedures for retention and distribution of identification documents and other personal data. Under the proposed regulations, DHS imposes new requirements on state motor vehicle agencies so that the federal government can link together their databases to distribute license and cardholders' personal data.[10] The states are compelled to begin maintaining paper copies or digital images of important identity documents, such as birth certificates or naturalized citizenship papers, for seven to 10 years.[11] DHS is mandating the increase of both the type of documents that need to be retained and the length of data retention.

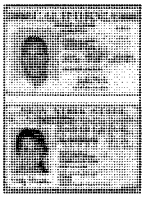
But on security and privacy standards for the card, state motor vehicle facilities, and the personal data and documents collected in state motor vehicle databases, DHS shows little interest and proposes that states prepare a "comprehensive security plan" for REAL ID implementation.[12] The vague plan proposes that states would include 1) an "approach to conducting background checks of certain federal employees"; 2) an approach to ensuring the "physical security of the locations where driver's licenses and identification cards are produced"; 3) an approach to ensuring the "security of document materials and papers from which driver's licenses and identification cards are produced"; 4) a description of the "security features incorporated into the driver's licenses and identification cards"; and 5) if the state decides to use biometrics as a part of its security plan, the state must "describe this use in its security plan and present the technology standard the State intends to use to DHS for approval."[13]

DHS would establish new requirements that states conduct background checks on "certain 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."[14] DHS would mandate that these employees must submit fingerprints and undergo financial and

criminal background checks, and lists the disqualifying offenses.[15] DHS also sets out standards for "security of document materials and papers from which driver's licenses and identification cards are produced," such as the "use of offset lithography in place of dye sublimation printing,"[16] The agency does not list minimum requirements for states to meet in their plans to ensure "physical security of the locations where driver's licenses and identification cards are produced."

The Department of Homeland Security will require states to include information "as to how the State will protect the privacy of the data collected, used, and maintained in connection with REAL ID, including all the source documents."[17] However, DHS does not require states to meet minimum standards to safeguard the privacy of individuals' data.

As for the mandate that "security features incorporated into the driver's licenses and identification cards," the agency is "lean[ing] toward" approving a two-dimensional bar code with encryption as the "common machine readable technology" standard, but it does not require secure encryption.[18] Though Homeland Security lays out the privacy and security problems associated with creating an unencrypted machine readable zone on the license, it does not require encryption because there are concerns about "operational complexity."[19]



Source: California State Government

On security and privacy standards, DHS shows little interest and proposes that states prepare a "comprehensive security plan" for REAL ID implementation.

Homeland Security may also require the use of radio frequency identification (RFID) technology in the cards as part of the "common machine readable technology," which means the sensitive data would be transmitted wirelessly and vulnerable to interception by third parties.[20] The agency is considering "vicinity read" or "long range" RFID tags even though the longer distance increases the risks of security and privacy problems associated with the wireless technology: clandestine tracking, loss of control of data by cardholder, and interception of data by unauthorized individuals.

ASSESSMENT

The mandates that DHS has imposed upon the states are questionable. The federal agency imposes more difficult standards for acceptable identification documents that could limit the ability of individuals to get a state drivers license. However, there are questions as to whether some citizens could produce these documents – such as victims of natural disasters or elderly individuals. The federal agency will require the states to create an exceptions process for such individuals, but does not set standards for eligibility, length of process, cost of process or any other piece of the exceptions process.[21]

DHS compels the states to complete data verification procedures that the federal government itself is not capable of following. The federal agency dictates that the states must verify the "issuance, validity, and completeness of each document required to be presented." [22] States must verify the data in identification requirements "with an authoritative or reference database."[23] However, it is questionable whether certain databases even exist. In the draft regulations, DHS concedes that it still needs to "ensure that the reference databases meet the standards for data quality, reliability, integrity, and completeness required to support REAL ID

data verification."[24] In fact, DHS admits some of these reference databases "are still under development and need investment of resources."[25] Even though DHS mandates state verification of identification documents through these reference databases, the federal government has not yet created reliable systems for the states to use.

The federal agency requires changes to the design of state licenses and identification cards. The card must include "Physical security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purpose" and "common [machine-readable technology], with defined minimum data elements."[26] The federal agency will require the use of a two-dimensional bar code, but will not require the use of encryption. The Department of Homeland Security's own Privacy Office has urged the use of encryption in REAL ID cards. In its Privacy Impact Assessment of the draft regulations, the Privacy Office supported encryption "because 2D bar code readers are extremely common, the data could be captured from the driver's licenses and identification cards and accessed by unauthorized third parties by simply reading the 2D bar code on the credential" if the data is left unencrypted.[27] DHS says that, "while cognizant of this problem, DHS believes that it would be outside its authority to address this issue within this rulemaking."[28] Imposing a requirement for the states to use unencrypted machine readable technology renders the cardholder unable to control who receives her data.

The agency is considering using RFID technology in the REAL ID cards even though it has just abandoned a plan to include long-range RFID chips in border identification documents because the pilot test was a failure. In 2005, the Department of Homeland Security began testing RFID-enabled I-94 forms in its United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program to track the entry and exit of visitors.[29] The RFID-enabled forms stored a unique identification number, which is linked to data files containing foreign visitor's biographic information, including name, date of birth, country of citizenship, passport number and country of issuance, complete U.S. destination address, and digital fingerscans.[30] EPIC warned that this flawed proposal would endanger personal privacy and security, citing the plan's lack of basic privacy and security safeguards. In October 2005 comments to the Department of Homeland Security, EPIC explained use of the wireless technology meant anytime a person carried his I-94 RFID-enabled form, unauthorized individuals could access his unique identification number, and thus the biographic information linked to that number.[31]

In a July 2006 report, the Department of Homeland Security's Inspector General echoed EPIC's warnings. His report found "security vulnerabilities that could be exploited to gain unauthorized or undetected access to sensitive data" associated with people who carried the RFID-enabled I-94 forms.[32] A report released by the Government Accountability Office in late January identified numerous performance and reliability issues in Department of Homeland Security's 15-month test.[33] The many problems with the RFID-enabled identification system led Homeland Security Secretary Michael Chertoff to admit in Congressional testimony on February 9th that the pilot program had failed, stating "yes, we're abandoning it. That's not going to be a solution" for border security.[34]

Homeland Security's failure with the US-VISIT pilot test is just one of several instances where the agency has stumbled with identification systems. The Transportation Security Administration said recently that Secure Flight, a federal passenger screening program, would be delayed until 2010, at least five years behind schedule. Secure Flight was suspended a year

ago after two government reports detailed security and privacy problems.[35] One report found 144 security vulnerabilities.[36] About $140 million has been spent on the program, and the TSA is seeking another $80 million for proposed changes.[37] Homeland Security also has problems with its bloated watch lists. More than 30,000 people who are not terrorists have asked the Transportation Security Administration to remove their names from the lists since September 11, 2001.[38] In January, the head of TSA said that the watch lists were being reviewed, and he expected to cut in half the watch lists (estimated to contain about 325,000 names).[39]

DHS may compel card design standardization, "whether uniform design/color should be implemented nationwide for non-REAL ID driver's licenses and identification cards," so that non-REAL ID cards will be easy to spot.[40] This combined with the mandate to "provide electronic access to all other States to information contained in the motor vehicle database of the State" would create a national database of sensitive personal information that would be a tempting target for identity thieves or other criminals hoping to subvert the national ID system.[41]

The federal agency dictates the expansion of schedules and procedures for retention and distribution of identification documents and other personal data. It creates a massive database with the personal data and copies of identification documents of 245 million state license and identification cardholders nationwide. Yet DHS has chosen not to mandate minimum privacy standards for either the database or the card itself.

DHS sets out standards for background checks on employees and for the type of paper the identification cards will use, yet it does not mandate any minimum standards of security for the national database of sensitive personal information. The creation of this massive database comes at a time when security breaches and identity theft are on the rise. State DMVs already are the victims of inside and outside attackers. For the seventh year in a row, identity theft is the No. 1 concern of U.S. consumers, according to the Federal Trade Commission's annual report.[42] Over 104 million data records of U.S. residents have been exposed due to security breaches since January 2005, according to a report from the Privacy Rights Clearinghouse.[43]

OTHER RISKS

In a recent analysis of the REAL ID Act, EPIC Executive Director Marc Rotenberg explained that "[s]ystems of identification remain central to many forms of security. But designing secure systems that do not introduce new risks is proving more difficult than many policymakers had imagined."[44] The theory that the REAL ID Aet will prevent terrorism is predicated on the belief that, "if we know who you are, and if we have enough information about you, we can somehow predict whether you're likely to be an evildoer," explained Bruce Schneier, security expert and member of the EPIC Board of Directors.[45] This is impossible, because you cannot predict intent based on identification, Schneier said.[46] Upon the release of the draft regulations, Schneier said, "The REAL ID regulations do not solve problems of the national ID card, which will fail when used by someone intent on subverting that system. Evildoers will be able steal the identity -- and profile -- of an honest person, doing an end-run around the REAL ID system."[47]

When it created the

Figure 1: Estimated marginal economic cost of REAL ID proposed rule

Estimated Costs (10 years)	$ million 7% discounted	$ million (2006 dollars) undiscounted	% Total 7% discounted
Costs to States	**$10,770**	**$14,600**	**62.5%**
Customer Services	$5,253	$6,901	30.5%
Card production	$3,979	$5,760	23.1%
Data Systems & IT	$1,127	$1,436	6.5%
Security & Information Awareness	$388	$471	2.3%
Data Verification	$12	$18	0.1%
Certification process	$10	$14	0.1%
Costs to Individuals	**$5,991**	**$7,875**	**34.8%**

Source: Department of Homeland Security

Before the REAL ID Act's passage in 2005, the Congressional Budget Office estimated its cost to be around $100 million. In September, the National Conference of State Legislatures released a report estimating the cost to be $11 billion over the first five years. Now, the Department of Homeland Security has admitted that REAL ID will cost states and individuals from $17.2 billion to $23.1 billion over ten years.

Department of Homeland Security, Congress made clear in the enabling legislation that the agency could not create a national ID system.[48] In September 2004, then-Department of Homeland Security Secretary Tom Ridge reiterated, "[t]he legislation that created the Department of Homeland Security was very specific on the question of a national ID card. They said there will be no national ID card."[49] The REAL ID Act creates a de facto national ID card.

The requirement for non-REAL ID driver's license or ID card to have explicit "invalid for federal purposes" designations turns this "voluntary" card into a mandatory national ID card. Anyone with a different license or ID card would be instantly suspicious. It will be easy for insurance companies, credit card companies, even video stores, to demand a REAL ID driver's license or ID card in order to receive services. Significant delay, complication and possibly harassment or discrimination would fall upon those without a REAL ID card.

Third parties such as insurance companies are not the only ones who will try to broaden the use of the REAL ID card. State licenses and identification cards must meet standards set out in the regulations to be accepted for federal use. Such federal purposes include entering buildings, boarding commercial aircraft, entering nuclear power plants, and "any other purposes that the Secretary shall determine." The Department of Homeland Security, via the draft regulations and Homeland Security Secretary Michael Chertoff, discusses expanding the use of the national identification card. The federal agency seeks comments on "how DHS could expand [the card's official purposes] to other federal activities."[50] In a speech last month, Secretary Chertoff said the REAL ID Act licenses might "do double-duty or triple-duty."[51] These REAL ID cards would "be used for a whole host of other purposes where you now have to carry different identification."[52] Security expert Bruce Schneier, EPIC and others have explained that it decreases security to have one ID card for many purposes, as there will be a substantial amount of harm when the card is compromised.[53] Using a national ID card would be as if you used one key to open your house, your car, your safe deposit box, your office, and more. "The problem is that security doesn't come through identification; security comes through measures -- airport screening, walls and door locks -- that work without relying on identification," therefore a national identification card would not increase national security Schneier said.[54]

A recent case illustrates Schneier's point. According to court documents, earlier this week in Florida, two men entered restricted areas, bypassed security screeners and carried a duffel bag containing 14 guns and drugs onto a commercial plane.[55] They avoided detection, because

they are airline baggage handlers who used their uniforms and legally issued identification cards.[56] Both men had passed federal background checks before they were hired, according to a spokesman for Comair, the airline that employed the men.[57] The men were only investigated and caught after receiving an anonymous tip.[58] If the airport had identification-neutral security systems, such as requiring all fliers go through metal detectors, then the men could not have walked past them. But the identification-based security – allowing some fliers to skip screening because they are presumed to have no evil intent – failed, and the men transported weapons and contraband aboard a commercial flight.

CONCLUSION

The estimated cost of REAL ID implementation has spiraled. Before the Act's passage in 2005, the Congressional Budget Office estimated its cost to be around $100 million.[59] In September, the National Conference of State Legislatures released a report estimating the cost to be $11 billion over the first five years.[60] Now, the Department of Homeland Security has admitted that REAL ID will cost states and individuals from $17.2 billion to $23.1 billion over ten years.[61] Congress has appropriated only $40 million for REAL ID implementation. The Department of Homeland Security now says that a state can use up to 20% of its Homeland Security Grant Program funding for REAL ID implementation, which total about $100 million for 2007.[62] Implementation costs for the state of California alone would be about $500 million.[63] Diverting grant money to REAL ID means that funding originally budgeted by the states for other homeland security projects, including training and equipment for rescue and first responder personnel. Even if the states received $100 million per year for 10 years, that would still amount to only $1.04 billion in federal funds, a fraction of the $17.2 billion to $23.1 billion price tag. The rest of the cost would be borne by states and their residents.

The REAL ID Act was appended to a bill providing tsunami relief and military appropriations, and passed with little debate and no hearings. REAL ID proponents state that the program implements recommendations from the 9/11 Commission. However, REAL ID repealed provisions in a 2004 law that created a negotiated rulemaking process among the states, federal agencies, and concerned parties to implement the Commission's recommendations.[64] The Intelligence Reform and Terrorism Prevention Act of 2004, which contained "carefully crafted language -- bipartisan language -- to establish standards for States issuing driver's licenses," Sen. Richard Durbin said at the time of REAL ID's passage.[65] In response to the draft regulations, Sen. Patrick Leahy said, "It is ironic that we probably would have stronger drivers' licenses today if the original shared rulemaking procedures that Congress agreed to in 2004 had been allowed to move forward."[66] Legislation to repeal REAL ID has been introduced in the House and Senate.[67] Maine and Idaho have passed resolutions rejecting implementation of REAL ID, and 25 other states are debating similar legislation.

DHS is imposing stringent, difficult and, in the case of document verification, impossible requirements upon the states and individual cardholders. The draft regulations are open for comment until May 8, 2007. To take action and talk to Congress about this ill-conceived identification scheme, visit the Electronic Frontier Foundation's Take Action page.

---

[1] Pub. L. No. 109-13, 119 Stat. 231 (2005); *see generally,* EPIC Page on National ID Cards, http://www.epic.org/privacy/id_cards/ and Privacy Int'l Page on National ID Cards, http://www.privacy.org/pi/issues/idcard/index.html (last visited Mar. 7, 2007).

[2] Dep't of Homeland Sec., *Notice of proposed rulemaking: Minimum Standards for Driver's licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes* (Mar. 1, 2007) [hereinafter "REAL ID Draft Regulations"], *available at* http://www.dhs.gov/xlibrary/assets/nprm_realid.pdf (last visited Mar. 7, 2007); http://a257.g.akamaitech.net/7/257/2422/01jan20071800/edocket.access.gpo.gov/2007/07-1009.htm (last visited Mar. 12, 2007); http://www.epic.org/privacy/id_cards/nprm_030107.pdf *and* http://www.epic.org/privacy/id_cards/fr_nprm_071009.pdf.

[3] *Id.* at 106.

[4] *Id.* at 34-35; for a discussion of why the Western Hemisphere Travel Initiative's proposed passport card creates an increased security risk, see EPIC, Spotlight on Surveillance, *Homeland Security PASS Card: Leave Home Without It* (Aug. 2006), http://www.epic.org/privacy/surveillance/spotlight/0806/.

[5] REAL ID Draft Regulations at 25, *supra* note 2.

[6] *Id.* at 47.

[7] *Id.* at 64-65, *supra* note 2.

[8] *Id.* at 65.

[9] *Id.* at 91, *supra* note 2.

[10] REAL ID Draft Regulations at 25, *supra* note 2.

[11] *Id.* at 27.

[12] *Id.*

[13] Id. at 83.

[14] *Id.* at 15.

[15] REAL ID Draft Regulations at 85, *supra* note 2.

[16] *Id.* at 72.

[17] *Id.* at 27.

[18] *Id.* at 31.

[19] *Id.*

[20] *Id.* at 94; for more information on the privacy and security risks associated with the use of radio frequency identification technology, *see* EPIC's page on RFID, http://www.epic.org/privacy/rfid.

[21] REAL ID Draft Regulations at 12, *supra* note 2.

[22] *Id.* at 25.

[23] *Id.* at 47.

[24] *Id.* at 58.

[25] *Id.*

[26] REAL ID Draft Regulations at 65, *supra* note 2.

[27] Dep't of Homeland Sec. Privacy Office, *Privacy Impact Assessment for the REAL ID Act* 16 (Mar. 1, 2007), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_realid.pdf (last visited Mar. 7, 2007). *and* http://www.epic.org/privacy/id_cards/pia_030107.pdf.

[28] REAL ID Draft Regulations at 73, *supra* note 2.

[29] Dep't of Homeland Sec., *Notice With Request For Comments: United States Visitor and Immigrant Status Indicator Technology Notice on Automatic Identification of Certain Nonimmigrants Exiting the United States at Select Land Border Ports-of-Entry*, 70 Fed. Reg. 44934 (Aug. 5, 2005), *available at* http://frwebgate1.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=021420363270+2+0+0&WAISaction=retrieve (last visited Mar. 7, 2007).

[30] Dep't of Homeland Sec., *Notice of Availability of Privacy Impact Assessment*, 70 Fed. Reg 39300, 39305 (July 7, 2005), *available at* http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/05-13371.htm (last visited Mar. 7, 2007).

[31] EPIC, *Comments on Docket No. DHS-2005-0011: Notice With Request For Comments: United States Visitor and Immigrant Status Indicator Technology Notice on Automatic Identification of Certain Nonimmigrants Exiting the United States at Select Land Border Ports-of-Entry* (Dec. 8, 2005), *available at* http://www.epic.org/privacy/us-visit/100305_rfid.pdf.

[32] Dep't of Homeland Sec. Inspector Gen., *Additional Guidance and Security Controls Are Needed Over Systems Using RFID at DHS (Redacted)* 7 (July 2006), *available at* http://www.dhs.gov/xoig/assets/mgmtrpts/OIGr_06-53_Jul06.pdf (last visited Mar. 7, 2007).

[33] Richard M. Stana, Dir., Homeland Sec. & Justice Issues, Gov't Accountability Office, *Testimony Before the Subcom. on Terrorism, Tech., & Homeland Sec., S. Comm. on the Judiciary*, 110th Cong. (Jan. 31, 2007), *available at* http://www.gao.gov/new.items/d07378t.pdf (last visited Mar. 7, 2007).

[34] Michael Chertoff, Sec'y, Dep't of Homeland Sec., *Testimony at a Hearing on the Fiscal*

Year 2008 Dep't of Homeland Sec. Budget Before the H. Comm. on Homeland Sec., 110th Cong. (Feb. 9, 2007), *available at* http://www.epic.org/privacy/us-visit/chertoff_020907.pdf.

[35] Edmund S. "Kip" Hawley, Nominee for Assistant Sec'y of Homeland Sec., Transp. Sec. Admin., Dep't of Homeland Sec., *Testimony at Hearing on TSA's Secure Flight and Registered Travelers Programs Before the S. Comm. on Commerce, Science & Transp.*, 109th Cong. (Feb. 9, 2006); for more information, *see* EPIC's page on Secure Flight, http://www.epic.org/privacy/airtravel/secureflight.html.

[36] Cathleen Berrick, Dir., Homeland Sec. & Justice, Gov't Accountability Office, *Statement at a Hearing on TSA's Secure Flight and Registered Travelers Programs Before the S. Comm. on Commerce, Science & Transp.*, 109th Cong. (Feb. 9, 2006), *available at* http://www.gao.gov/new.items/d06374t.pdf (last visited Mar. 7, 2007).

[37] Press Release, Dep't of Homeland Sec., *Fact Sheet: U.S. Department of Homeland Security Announces Eight Percent Increase in Fiscal Year 2008 Budget Request* (Feb. 5, 2007), *available at* http://www.dhs.gov/xnews/releases/pr_1170702193412.shtm (last visited Mar. 7, 2007).

[38] Anne Broache, *Tens of thousands mistakenly matched to terrorist watch lists*, CNet News.com, Dec. 6, 2005.

[39] Edmund S. "Kip" Hawley, Assistant Sec'y, Transp. Sec. Admin., Dep't of Homeland Sec., *Testimony at Hearing on Aviation Security: Reviewing the Recommendations of the 9/11 Commission Before the S. Comm. on Commerce, Science & Transp.*, 110th Cong. (Jan. 17, 2007), *available at* http://commerce.senate.gov/public/_files/TestimonyofMrHawley.pdf (last visited Mar. 7, 2007); Walter Pincus & Dan Eggen, *325,000 Names on Terrorism List*, Wash. Post. Feb. 15, 2006..

[40] REAL ID Draft Regulations at 91, *supra* note 2.

[41] *Id.* at 27.

[42] Fed. Trade Comm'n, *Consumer Fraud and Identity Theft Compliant Data: January – December 2006* (Feb. 7, 2007), *available at* http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf (last visited Mar. 7, 2007).

[43] Privacy Rights Clearinghouse, Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Mar. 7, 2007).

[44] Marc Rotenberg, EPIC Exec. Dir., *Real ID, Real Trouble?*, Communications of the ACM, Mar. 2006, *available at* http://www.epic.org/privacy/id_cards/mr_cacm0306.pdf.

[45] Bruce Schneier, *Real-ID: Costs and Benefits,* Bulletin of Atomic Scientists, Mar./Apr. 2007, *available at* http://www.schneier.com/blog/archives/2007/01/realid_costs_an.html (last visited Mar. 7, 2007).

[46] *Id.*

[47] Press Release, EPIC, After Long Delay, Homeland Security Department Issues Regulations For Flawed National ID Plan (Mar. 2, 2007) [hereinafter "EPIC Press Release on Regulations"], *available at* http://www.epic.org/press/030207.html.

[48] Pub. L. No. 107-296, 116 Stat. 2135 (2002).

[49] Tom Ridge, Sec'y, Dep't of Homeland Sec., *Address at the Center for Transatlantic Relations at Johns Hopkins University: "Transatlantic Homeland Security Conference"* (Sept. 13, 2004), *available at* http://www.dhs.gov/xnews/speeches/speech_0206.shtm (last visited Mar. 7, 2007).

[50] REAL ID Draft Regulations at 17, *supra* note 2.

[51] Michael Chertoff, Sec'y, Dep't of Homeland Sec., *Remarks by Secretary Michael Chertoff at the National Emergency Management Association Mid-Year Conference* (Feb. 12, 2007), *available at* http://www.dhs.gov/xnews/speeches/sp_1171376113152.shtm (last visited Mar. 7, 2007).

[52] *Id.*

[53] Melissa Ngo, Dir., EPIC Identification & Surveillance Project, *Prepared Testimony and Statement for the Record at a Hearing on "Maryland Senate Joint Resolution 5" Before the Judicial Proceedings Comm. of the Maryland Senate* (Feb. 15, 2007), *available at* http://www.epic.org/privacy/id_cards/ngo_test_021507.pdf.

[54] EPIC Press Release on Regulations, *supra* note 59.

[55] Jim Ellis, *Feds: Bag Of Guns Smuggled Onto Plane*, Associated Press, Mar. 9, 2007.

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] Cong. Budget Office, *Cost Estimate: H.R. 418: REAL ID Act of 2005* (Feb. 9, 2005), *available at* http://www.cbo.gov/showdoc.cfm?index=6072&sequence=0&from=6 (last visited Mar. 7, 2007).

[60] Nat'l Conference of State Legislatures, *The REAL ID Act: National Impact Analysis* (Sept. 19, 2006), *available at* http://www.ncsl.org/print/statefed/Real_ID_Impact_Report_FINAL_Sept19.pdf (last visited Mar. 7, 2007).

[61] REAL ID Draft Regulations at 106, *supra* note 2.

[62] Press Release, Dep't of Homeland Sec., DHS Issues Proposal for States to Enhance Driver's Licenses (Mar. 1, 2007), *available at* http://www.dhs.gov/xnews/releases/pr_1172765989904.shtm (last visited Mar. 7, 2007).

[63] Cal. Dep't of Motor Vehicles, *Report to the Legislature on the Status of the REAL ID Act* 3 (Dec. 15, 2006), *available at* http://www.dmv.ca.gov/about/real_id/real_id.pdf (last visited Mar. 7, 2007).

[64] Pub. L. No. 108-458, 118 Stat. 3638 (2004).

[65] Sen. Richard Durbin, *Speech on Floor During Senate Debate about Emergency Supplemental Appropriations Act of 2005* (April 20, 2005), *available at* http://www.epic.org/privacy/id-cards/durbin_senate_4_20_05.html.

[66] Press Release, Office of Sen. Patrick J. Leahy, Comment of Sen. Patrick Leahy On Release of the Draft REAL ID Regulations By the U.S. Department of Homeland Security (Mar. 1, 2007), *available at* http://leahy.senate.gov/press/200703/030107b.html (last visited Mar. 7, 2007).

[67] For information on legislation concerning REAL ID, *see* EPIC Page on National ID Cards, *supra* note 1.

EPIC Spotlight on Surveillance Page | EPIC Privacy Page | EPIC Home Page

CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Working for Civil Liberties on the Internet

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

SENATE COMMITTTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
SUBCOMMITTEE ON OVERSIGHT OF GOVERNMENT MANAGEMENT, THE FEDERAL WORKFORCE, AND THE DISTRICT OF COLUMBIA

"UNDERSTANDING THE REALITIES OF REAL ID: A REVIEW OF EFFORTS TO SECURE DRIVER'S LICENSES AND IDENTIFICATION CARDS"

MARCH 26, 2007

Statement for the Record
Sophia Cope
Staff Attorney/Ron Plesser Fellow
Center for Democracy & Technology

Chairman Akaka, Ranking Member Voinovich, and members of the Subcommittee:

CDT commends the Subcommittee for holding this hearing. CDT has analyzed both the REAL ID Act and the Department of Homeland Security's proposed regulations, and we conclude that both the Act and the regulations have serious privacy and security flaws.

As we articulate below, DHS could have done significantly more in the proposed regulations to protect individual privacy and ensure security within its present authority under the Act. However, our main conclusion is that the REAL ID Act is fundamentally flawed and must be revisited by Congress, either via a wholesale repeal or substantial rewrite.

It is one thing to make driver's license and ID card issuance, as well as the cards themselves, more secure. It is quite another to create an infrastructure that amounts to a national identification system – yet that is exactly what the Act, as implemented by the regulations, would do. The end result of the REAL ID Act and regulations would be to make our nation less secure while facilitating the widespread governmental and commercial tracking of virtually all U.S. residents.

We encourage the Subcommittee to use S. 717 as a starting point from which to create a robust statutory framework that directs driver's license and ID card reform without compromising privacy and security.

I. SUMMARY

A. THE REAL ID ACT IS FUNDAMENTALLY FLAWED

CDT supports the goal of making driver's license and ID card issuance more secure and thereby making the cards more reliable identity credentials. However, DHS's proposed regulations confirm our fears that the REAL ID Act is fundamentally flawed. Both the Act itself and the proposed implementing regulations fail to protect privacy while creating serious security gaps.

CDT urges this Congress to replace the REAL ID Act with a statutory framework for driver's license and ID card issuance that expressly protects privacy and ensures security. Congress must repeal or substantially rewrite the Act if driver's license and ID card reform is to be effective. The privacy and security shortfalls found in the proposed regulations stem directly from those in the Act itself: the statutory language provides no guidance on privacy and little guidance on security. DHS states in the Preamble to the draft regulations that it has addressed privacy "within the limits of its authority under the Act."[1] The Department explains that the REAL ID Act "does not include statutory language authorizing DHS to prescribe privacy requirements," which "is in sharp contrast with the express authorization provided in section 7212 of IRTPA [Intelligence Reform and Terrorism Prevention Act of 2004], which was the prior state licensing provision repealed by the REAL ID Act."[2]

At the same time, CDT is urging DHS to make substantial changes to its proposed REAL ID regulations. We believe that the Department does have some authority to address privacy and security under the Act as it currently stands. Even given the limitations of the REAL ID Act, DHS could have done a much better job of creating a regulatory framework that does not increase the risk of identity theft nor enable widespread governmental and commercial tracking of U.S. residents. Recognizing that legislation might not move through both houses and conference, this Congress should at least use its oversight powers to encourage DHS to substantially rewrite the final regulations to protect privacy and ensure security to the maximum extent possible.

---

[1] Notice of Proposed Rulemaking (NPRM), Preamble at 10824-25.

[2] NPRM, Preamble at 10825 n.3.

B. THE ACT AND DRAFT REGULATIONS CREATE SERIOUS PRIVACY AND SECURITY RISKS

Risks to privacy and security flow from three key provisions in the REAL ID Act:

- Each state must "provide electronic access to all other States to information contained in the motor vehicle database of the State,"[3]
- Each state must "employ technology to capture digital images of identity source documents so that the images can be retained in electronic storage in a transferable format,"[4] and
- Each driver's license and ID card must contain a Machine Readable Zone (MRZ), which enables fast and easy collection of personal information by digital means.[5]

CDT's privacy and security concerns – based on the REAL ID Act as well as the proposed regulations – can be summarized as follows:

- **The Act's Requirement for "Electronic Access" Is Overbroad** – The Act mandates that each state give every other state "electronic access" to information contained in its DMV database. A nationally accessible network of government databases that contain highly sensitive personal information creates increased potential for abuse by government and identity thieves. The "electronic access" mandated by the Act is far broader than what is necessary to achieve the goal of "only one license for one driver." ***CDT recommends that the "electronic access" provision of the REAL ID Act be repealed.***

- **The Act and Regulations Are Leading to a Centralized ID Database** – To implement the "electronic access" provision of the Act, DHS proposes to build upon the system used for commercial drivers: the Commercial Driver's License Information System (CDLIS), which is managed by the non-profit American Association of Motor Vehicle Administrators (AAMVA). Even though DHS and other proponents of REAL ID have repeatedly stated that the Act would not produce a centralized ID system, that is precisely what CDLIS is: a central database that houses a small but very significant amount of personal information (including name and Social Security Number)[6] and that links to other information contained in state databases. Applying this system to all non-commercial drivers and ID card holders (i.e., virtually all U.S. residents) opens the door to the national linking of many other state and federal government databases; once a centralized identification database is established, there are no limits on what information

[3] REAL ID Act of 2005, Title II [H.R. 1268] Public Law 109-13, §202(d)(12).

[4] §202(d)(1). Subsection (d)(2) also requires states to "retain paper copies of source documents for a minimum of 7 years or images of source documents presented for a minimum of 10 years." The Conference Report on the REAL ID Act [H.R. 1268], House Report 109-72, explains with respect to §202(d)(2) that "The goal is to move all the state's records into electronic format, with each state consolidating electronic records otherwise maintained at the County level at the State level."

[5] §202(b)(9).

[6] *See* AAMVA's webpage on CDLIS <http://www.aamva.org/TechServices/AppServ/CDLIS/>.

it could point to. Both the Act and the proposed regulations fail to place any limits on the use of a central database. ***CDT recommends that a central database not be created, and instead that a system be designed that gives a simple "yes" or "no" answer regarding whether a person already holds a driver's license or ID card issued by another jurisdiction, where that information comes directly from each state and not via a central repository.***

- **The Act and Regulations Fail to Protect the Privacy and Security of Personal Data in State DMV Databases** – The Act requires states to digitally copy and store for several years all source documents, which contain highly sensitive personal information. But neither the Act nor the proposed regulations contain limitations on what personal information (including source documents) in a DMV database can be accessed, by whom, and for what purposes. ***CDT recommends that source documents and other personal data in the state databases be accessible only by DMV officials for legitimate administrative purposes, and only by law enforcement officials for legitimate law enforcement purposes consistent with existing law. CDT recommends that there be specific minimum security requirements for personal data stored in DMV databases.***

- **The Act and the Regulations Fail to Build Security into the Machine Readable Zone Technology** – The Act mandates that each driver's license and ID card have a machine-readable zone (MRZ) containing personal information, but the Act does not state what security and privacy standards the technology must meet. The lack of statutory guidance enables DHS to endorse technology with weak security. In fact, the Preamble to the proposed regulations contemplates that some driver's licenses and ID cards could contain an RFID chip so that they can be used in place of a passport book or PASS card at U.S. land and sea borders under the Western Hemisphere Travel Initiative (WHTI),[7] yet the RFID technology chosen for the PASS card is insecure. ***CDT recommends that privacy and security criteria be mandated for the MRZ technology.***

- **The Act and the Regulations Set No Limits on the Amount and Nature of Data in the MRZ** – The Act does not limit the type or amount of personal information that can be digitally stored in the MRZ, and it appears from the Preamble to the proposed regulations that DHS gave little attention to the tradeoff of putting items of personal information, such as name, in the MRZ. There is a significant risk that any data in the MRZ will be inappropriately "skimmed." ***CDT recommends that the contents of the MRZ be limited to the information necessary for law enforcement purposes, and, as we explain below, that all information be protected against unauthorized skimming.***

- **The Act and the Regulations Fail to Limit the Compilation of Travel and Activity Information by Government Agencies** – Neither the Act nor the proposed regulations prohibit REAL ID cards from being read by innumerable state and federal government agencies, which would create a vast and efficient surveillance system that enables widespread tracking of the movements and activities of virtually all U.S. residents. ***CDT***

[7] NPRM, Preamble at 10841-42.

recommends that the MRZ be encrypted or otherwise designed so it can be read and/or personal data can be "skimmed" (as opposed to the card being visually inspected) only by DMV officials for legitimate administrative purposes, and by law enforcement officials for legitimate law enforcement purposes consistent with existing law.

- **The Act and the Regulations Contain No Protections Against Skimming by Third Parties** – Neither the Act nor the proposed regulations prohibit the cards from being read and personal data "skimmed" by businesses or other non-governmental third parties to create profiles and fill databases with information about the activities and preferences of millions of U.S. residents. ***CDT recommends that the MRZ be encrypted or otherwise designed so it can be read and/or personal data "skimmed" (as opposed to the card being visually inspected) only by DMV officials for legitimate administrative purposes, and by law enforcement officials for legitimate law enforcement purposes consistent with existing law.***

- **The Nationally "Unique" Identifier Can Become the New Social Security Number, With All the Risks of the SSN** – The proposed regulations refer to a "unique" card number and require that it be included in the MRZ. It is unclear whether this number would be unique nationally or state-by-state. A nationally unique number could be abused as happened with the Social Security Number. ***CDT recommends that the driver's license or ID card number not be standardized and unique across states, and that its use be expressly limited.***

All of these issues relate to those parts of the REAL ID Act and the proposed implementing regulations that go far beyond what is needed to make driver's license and ID card issuance more secure. These provisions create a *national identification system* by mandating "one person – one license/ID card – one record" supported by greater collection, centralization and sharing of highly sensitive personal information. The key point is that the more personal information is collected, centralized (even if in a technically "decentralized" system) and shared, the greater the potential for abuse not only by government and businesses, but also by terrorists, identity thieves and other criminals.

Neither the Act nor the proposed regulations control what information may be collected or accessed, by whom (i.e., state and government agencies, business, and other third-parties), and for what purposes. The Act does not mandate privacy and it barely addresses security, and DHS has failed to fill the gaps left by the statute despite an extensive discussion in the Preamble. Thus CDT concludes that the Act must be repealed or substantially rewritten to include mandates that protect privacy and ensure security. And whether or not corrective legislation passes both houses of Congress, Congress must use its oversight authority to ensure that DHS does everything in its power under the law to protect privacy and ensure security.

C. A MUCH DIFFERENT APPROACH IS NEEDED TO MAKE DRIVER'S LICENSE AND ID CARD ISSUANCE MORE SECURE

All of the privacy and security concerns raised above stem from elements of the Act and the proposed regulations that are not necessary to make the issuance of driver's licenses and ID cards more secure, thereby making the cards themselves a more reliable means of identifying individuals in special contexts. CDT supports the goal of making driver's license and ID card issuance more secure. Indeed, for years CDT has urged attention to the security flaws in the issuance of driver's licenses due to theft from DMV offices and insider DMV fraud.[8] And security in the issuance of driver's licenses and ID cards was the focus of the recommendation of the 9/11 Commission.[9]

Driver's license and ID card issuance can be made more secure without significantly compromising privacy, or weakening security in other ways. Measures to improve the security of the issuance process include verifying that a person is who he says he is, and that he is providing accurate and current information. Such measures also include ensuring that access to information and supplies used to create driver's licenses and ID cards are strictly controlled, and that the cards themselves are resistant to tampering and counterfeiting. Additionally, as already occurs under the Problem Driver Pointer System (PDPS)/National Driver Register (NDR), states should be able to be sure that they are not issuing a driver's license to someone whose license has been revoked in another jurisdiction. While such measures may raise questions about cost or practical implementation, they are reasonable reform measures that are likely to be effective and pose no risk to privacy or security.

Congress must revisit the REAL ID Act and create a statutory framework that addresses both privacy and security. CDT supports the bills introduced by Senator Akaka (S. 717) and Representative Allen (H.R. 1117). These bills would repeal the REAL ID Act, but they also recognize the need for driver's license/ID card reform and aim to create a framework to do it right.

---

[8] *See* "Unlicensed Fraud: How bribery and lax security at state motor vehicle offices nationwide lead to identity theft and illegal driver's licenses" (January 2004) <http://www.cdt.org/privacy/20040200dmv.pdf>.

[9] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, Authorized Edition, at 390.

II. KEY PRIVACY AND SECURITY ISSUES

Privacy and security are fundamental to any system that deals with vast amounts of personal information. Privacy and security are interrelated: threats to privacy can create security risks, and vice versa.

A. "ELECTRONIC ACCESS" IS RISKY AND IS UNNECESSARY TO ENSURE "ONLY ONE LICENSE FOR ONE DRIVER"

1. The Statutory Language is Overbroad and Should be Repealed

According to the legislative history, the purpose of the "electronic access" provision of the REAL ID Act is to ensure that there is "only one license for one driver."[10] While this is a legitimate goal, mandating that each state give every other state "electronic access" to "information" contained in its "motor vehicle database" goes far beyond what would be appropriate to achieve only one driver's license or ID card per person, and instead creates enormous privacy and security risks.

This provision contemplates a national network of government databases that contain highly sensitive personal information. The greater centralization of personal data mandated by the Act creates increased potential for abuse by government and by identity thieves, especially given that the Act and the proposed regulations fail to place limits on authorized access and fail to mandate specific security measures to guard against unauthorized access. If one point in the network is compromised, the entire network will be compromised. And even if DHS were to amend the proposed regulations to interpret this provision narrowly now, the Department would be free to interpret it broadly in the future.

Furthermore, in the short-term, states are not at the same level (and will not be for some time) in terms of implementing highly secure issuance procedures and ensuring data accuracy within their own statewide systems. Until individual state databases are accurate and complete, it will be difficult to reliably check whether someone already holds a driver's license or ID from another jurisdiction. Granting electronic access to incomplete and inaccurate data will not improve security.

> **Recommendation to Congress:** Repeal the language of the REAL ID Act that requires each state to "provide electronic access to all other States to information contained in the motor vehicle database of the State."

2. The Proposed Regulations Favor a Centralized ID Database, Which Could Facilitate Nationwide Linking of Multiple Databases

The proposed regulations do not specify what "electronic access" means. Instead, the rules simply state, "States must provide to all other States electronic access to information

[10] Conference Report on H.R. 1268, House Report 109-72, at 184.

contained in the motor vehicle database of the State, in a manner approved by DHS pursuant to this regulation."[11] As a matter of transparency and accountability, this is inappropriate. It is incumbent upon DHS to be specific and transparent regarding how the multi-jurisdictional check will take place.

The Preamble, however, states that DHS is contemplating a system similar to (if not exactly like) that already in place for commercial driver's licenses: the Commercial Driver's License Information System (CDLIS).[12] CDLIS includes a central database with "pointers" or links to state databases. Therefore, DHS is *blatantly misleading* when it asserts that "the recommended architecture for implementing these data exchanges does not create a national database, because it leaves the decision of how to conduct the exchanges in the hands of the states."[13]

CDLIS, moreover, is not simply a " one license for one driver" system.[14] Rather, it is a "one person – one license (or ID card) – one *record*" system. In the REAL ID context, this is even more of a concern given that there are no statutory or regulatory limitations on what information may be in a person's "record," who can access the information, and for what purposes. Because this system would also include ID card holders, the "record" might not simply contain driving history. And, as the Privacy Impact Assessment for REAL ID explains, "CDLIS maybe subject to more limited privacy protections" because CDLIS – which is managed by the non-profit AAMVA – is not a federal "system of records" under the Privacy Act.[15]

---

[11] NPRM, Proposed Rules §37.33(b).

[12] The American Association of Motor Vehicle Administrators (AAMVA) manages a central database that includes basic identification information for holders of commercial driver's licenses. A person's "pointer" record within the central database includes the individual's name, alias information, date of birth, Social Security Number (mandatory), and current State of Record (the issuing state). The State of Record, after issuing a person's first CDL, must report the person's basic identification information to CDLIS, which becomes the individual's "pointer" record. AAMVA's central database does not contain a person's commercial driving history; this information is housed in the database of the State of Record.

If person applies for a CDL is another state, the new state will check CDLIS (by inputting basic identification information), which will then "point" to the person's commercial driving history in the State of Record's database. If the person's commercial driving history is good, the new state will issue a new CDL, become the new State of Record, and transfer the person's commercial driving history over to its own database. A person cannot have more than one commercial driver's license (nor can a person have a non-commercial driver's license at the same time) and his commercial driving history follows him from jurisdiction to jurisdiction.

[13] NPRM, Preamble at 10825. *See also* Renee Boucher Ferguson, "DHS Issues Proposed Regulations for Real ID Act," *eWeek* (March 2, 2007) (DHS Secretary Chertoff said, "We at the Department of Homeland Security in the federal government will not build, will not own, and will not operate any central database containing personal information. The data will continue to be held at the state level as it has traditionally been since they began to issue driver's licenses.") <http://www.eweek.com/article2/0,1895,2100036,00.asp>.

[14] Ensuring one-card-per-person, possibly using a CDLIS-type system, should be distinguished from states linking to federal databases to **verify source document information** (e.g., birth certificates, Social Security Numbers, passports, etc.).

[15] Privacy Impact Assessment, DHS Privacy Office, at 11 <http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_realid.pdf>

The Act and the proposed regulations place no limits on the number and type of state or federal databases that could be nationally searchable via the "pointer system" once it is created. Under the centralized pointer system apparently contemplated by DHS, the risk for "mission creep" – linking new databases to the pointer – is enormous. Such centralization of personal data would also create a greater security risk, especially since the proposed regulations fail to include any specific security mandates for a CDLIS-type system.

When balancing the potential security benefits of a "one person – one license/ID card – one record" system (e.g., keeping track of driving "points")[16] against the privacy risks (i.e., a nation-wide identification system used to track people for purposes other than administering driver's licenses), it becomes evident that such a system should not be implemented. In any case, a CDLIS-type system for all U.S. drivers is largely unnecessary to ensure driver safety across states given the existence of the Problem Driver Pointer System (PDPS)/National Driver Register (NDR).[17]

To enable states to determine whether an applicant already holds a driver's license or ID card in another jurisdiction to achieve the goal of one-card-per-person, CDT recommends against creating either a central database or central identification records. Instead, a truly decentralized system should be architected that simply gives a "yes" or "no" answer regarding whether a person holds a driver's license or ID card issued by another state.

Recommendation to Congress: Prohibit the creation of a central database.

Recommendation to DHS: Architect a system that does not have a central database and that, instead, simply gives a "yes" or "no" answer regarding whether an applicant already holds a driver's license or ID card in another jurisdiction.

---

[16] *See* NPRM, Preamble at 10834 ("the primary purpose of State-to-State data exchange is driver safety – to ensure that drivers are not holding multiple licenses in multiple jurisdictions to avoid points from dangerous driving").

[17] When a driver in a state has his license revoked or suspended, or when he is convicted of a serious traffic violation such as a DUI, the state DMV is supposed to report this to the NDR. The NDR is a central database managed by the Department of Transportation, but it does not contain driver history information. Rather, what a state adds to the NDR is basic identification information including name, date of birth, gender , driver's license number, and reporting state. Social Security Number is optional; the state need not submit it to the NDR.

If the person tries to get a driver's license in another state, the new state will check the NDR (by inputting basic identification information), which will then "point" to the person's driving history housed in the original state's DMV database. The new state will decide whether to issue a new license based on this information. If a person is licensed in more than one state and has had those licenses suspended, for example, he will have more than one "pointer" record in the NDR. The purpose of the PDPS/NDR is to prevent a bad driver from evading his punishment or putting others at risk by getting a new license in another state.

B. PRIVACY AND SECURITY OF PERSONAL INFORMATION IN STATE DMV DATABASES

The Act and the proposed regulations have left unanswered key privacy and security questions related to the collection and use of personal information: What information may be collected and accessed, by whom, and for what purposes? How is personal information contained in the DMV databases going to be protected from unauthorized access?

Neither the Act nor the proposed regulations limit what information may go into a "motor vehicle database" (i.e., be part of a person's record). The Act merely requires states to include at a minimum "all data fields printed on drivers' licenses and identification cards issued by the State," and "motor vehicle drivers' histories, including motor vehicle violations, suspensions, and points on a license."[18] The Act also requires states to digitally copy and store for several years all source documents, which contain highly sensitive personal information (birth certificate, passport, Social Security card, utility bill).[19]

Yet neither the Act nor the proposed regulations contain limitations on what personal information in a DMV database (including source documents) can be accessed, by whom (i.e., state or federal agencies, businesses or other third parties), and for what purposes. The Privacy Impact Assessment frankly states that "DHS cannot rely on the DPPA [Driver's Privacy Protection Act] to protect the privacy of the personal information required under the REAL ID Act."[20] This is especially relevant if a DMV databases are linked or a CDLIS-type system is created, as greater electronic collection and centralization of personal information would facilitate government access to such information, as well as create a "target rich environment" for identity thieves.

> **Recommendation to Congress:** Pass statutory limitations on the use of personal data stored in DMV databases, including source documents. Specifically, limit access to personal information to DMV officials for legitimate administrative purposes, and to law enforcement officials for legitimate law enforcement purposes consistent with existing law. Write legislation to secure personal data held in DMV databases against unauthorized access.

With or without clear privacy and security mandates from Congress, DHS should craft meaningful regulations to protect the privacy and security of personal data held in government databases. The Preamble includes various assurances that the REAL ID system will not afford the federal government any greater access to information than it already has,[21] but there are no

---

[18] §202(d)(13).

[19] §202(d)(1)-(2).

[20] PIA at 12.

[21] The Preamble asserts that "neither the REAL ID Act nor these proposed regulations gives the Federal Government any greater access to information than it had before. Moreover, there is no information about a licensee that the Federal Government will store that it is not already required to store." NPRM, Preamble at 10824.

limitations on federal government access in the proposed regulations themselves. Moreover, the proposed regulations simply require that each state, as part of its certification process, develop a "privacy policy regarding personal information collected and maintained by the DMV."[22] This is entirely insufficient. DHS should at the very least specify in the regulations criteria against which DHS will evaluate a state's privacy policy. The Preamble states that the state privacy policies should follow Fair Information Principles (FIPs): openness, individual participation (access, correction, redress), purpose specification, data minimization, use and disclosure limitation, data quality and integrity, security safeguards, and accountability and auditing. DHS should write these into the regulations, along with more specific criteria for certification, consistent with the FIPs. Failure to do so will result in states having no guidance as to what is acceptable to DHS, and there will be 56 different privacy policies with different levels of protection.

CDT commends DHS for interpreting the "physical security" provision of the Act[23] as also contemplating database security.[24] The proposed regulations themselves require that states, as part of the certification process, develop "standards and procedures for safeguarding information collected, stored, or disseminated for purposes of complying with the REAL ID Act, including procedures to prevent unauthorized access, use, or dissemination of applicant information and images of source documents . . . ."[25] However, DHS must be more specific. Arguably, the only specific database security requirement in the proposed rules is internal audit controls.[26]

> **Recommendation to DHS:** By regulation, limit access to personal information, including source documents, to DMV officials for legitimate purposes related to the administration of driver's licenses and ID cards, and to law enforcement officials for legitimate law enforcement purposes consistent with existing law. Write specific privacy criteria – consistent with FIPs – against which the state privacy policies will be evaluated. Write specific security criteria against which the state security plans will be evaluated.

---

[22] NPRM, Proposed Rules §37.41(b)(5).

[23] §202(d)(7).

[24] NPRM, Preamble at 10826.

[25] NPRM, Proposed Rules §37.419(b)(8).

[26] NPRM, Proposed Rules §37.419(b)(7).

C. PRIVACY AND SECURITY OF DATA IN THE MACHINE READABLE ZONE (MRZ)

The Act requires that each driver's license and ID card have "a common machine-readable technology, with defined minimum data elements."[27] It is not clear why it is necessary to federally mandate a machine-readable zone in state driver's licenses and ID cards. Neither Congress nor DHS have clearly explained what the benefits are or whether they outweigh the privacy and security risks. It seems that the choice of whether to include an MRZ on each card could be left up to the states.

> **Recommendation to Congress:** Consider whether federally mandating a Machine-Readable Zone on state-issued driver's licenses and ID cards is appropriate; specifically, whether the benefits outweigh the costs.

However, the main issue with regard to the MRZ is the collection and use of personal information digitally contained on the card. The Act falls short in four specific ways related to this issue:

- Not requiring privacy and security criteria for the chosen MRZ technology;
- Not requiring technological security features such as encryption;
- Not limiting the amount and type of personal information contained in the MRZ; and
- Not limiting who can "skim" data from the MRZ and for what purposes.

Failing to explicitly address skimming opens the door to using the REAL ID card as a key component of a vast and efficient surveillance system that enables widespread tracking of the movements and activities of virtually all U.S. residents. Similarly, businesses and other non-governmental third parties could create profiles and fill databases with the activities and preferences of millions of U.S. residents.

1. Privacy and Security Criteria for the MRZ Technology

The Act mandates that each driver's license and ID card have a machine-readable zone, but the Act does not state what privacy and security standards the technology must meet. The lack of statutory guidance enables DHS to endorse a technology with weak security. In fact, the Preamble contemplates that some driver's licenses and ID cards could contain an RFID chip so that they can be used in place of a passport book or PASS card at U.S. land and sea borders under the Western Hemisphere Travel Initiative (WHTI),[28] yet the RFID technology chosen for the PASS Card is insecure.

> **Recommendation to Congress:** Establish minimum privacy and security criteria for the MRZ technology.

---

[27] §202(b)(9).

[28] NPRM, Preamble at 10841-42.

Recommendation to DHS: Prohibit the use of long-range or "vicinity read" RFID technology in driver's licenses and ID cards at this time.

2. Technological Security Features for the MRZ

A technological security feature such as encryption would help prohibit unauthorized "skimming" of personal information from the MRZ, both by government agencies and businesses compiling databases of movements and activities, and by identity thieves. Only state DMVs and law enforcement officials should have the ability to read the contents of the MRZ in clear text.

The REAL ID Conference Report explicitly contemplates that personal data would be "stored securely and only able to be read by law enforcement officials."[29] However, the Act itself fails to address privacy and security of personal data stored in the MRZ. Thus Congress should make technical protection, through encryption or other means, a clear statutory requirement.

DHS has stated in the Preamble that it "leans toward recommending that States protect the personally identifiable information stored in this 2D bar code by requiring encryption."[30] DHS has asked for public comments on the cost and feasibility of encrypting the MRZ: "DHS leans toward an encryption requirement if the practical concerns identified above [key infrastructure] can be overcome in a cost-effective manner."[31] CDT plans to offer more technical advice in the comments submitted to DHS prior to the May 8 deadline, but it seems that DHS has shirked its responsibility here. It is the Department's obligation to provide the public with a detailed analysis of the cost and feasibility of an encryption scheme, especially given Congress' clear intent that the MRZ be secure and that only law enforcement officials have access to the personal data contained in it.

Recommendation to Congress: Statutorily require that the contents of the MRZ be protected by encryption or other technical means.

Recommendation to DHS: Require by regulation that the contents of the MRZ be protected by encryption or other technical means. Conduct an analysis of the cost and feasibility of implementing an encryption scheme.

3. Limiting the Contents of the MRZ

In CDT's view, encryption or other technological means are clearly the best way to protect information on the MRZ. If Congress and DHS do not require encryption or other technological means of protecting MRZ data, this information can also be protected by policy and law. That may include narrowly limiting the information in the MRZ.

---

[29] Conference Report on H.R. 1268, House Report 109-72, at 179.

[30] NPRM, Preamble at 10826.

[31] NPRM, Preamble at 10838.

In the Preamble to the proposed regulations, DHS suggests that states should store "only the *minimum* data elements necessary for the purpose for which the REAL IDs will be used. DHS requests comments on what data elements should be included . . . ."[32] However, the proposed rules themselves currently require nine data elements: 1) expiration date, 2) full legal name and all name changes ("name history"), 3) issue date, 4) date of birth, 5) gender, 6) principal address, 7) unique driver's license or identification number, 8) revision date, (9) inventory control number of the physical document.[33]

The Privacy Impact Assessment also discusses data minimization, a Fair Information Principle: "Good privacy policy supports limiting the data in the MRZ to the minimum personal data elements necessary for the intended purposes of providing access to law enforcement personnel."[34] Consistent with data minimization and because law enforcement officers are to be the intended beneficiaries of the MRZ, CDT believes that the only personally identifiable information that should be included in the MRZ is the number associated with a driver's license or ID card – especially if the MRZ is not encrypted or otherwise secured. The PIA recognizes that less information in the MRZ would make "skimming less attractive to third parties."[35]

CDT believes that Congress should make this a statutory limitation so that the required contents of the MRZ cannot be easily changed by regulatory action. But CDT believes that it is within the Department's present authority under the Act to further limit the contents of the MRZ.

> **Recommendation to Congress:** If there are no technological protection requirements for the MRZ such as encryption, Congress should statutorily limit the contents of the MRZ, and in particular should consider the risks of including name in the MRZ.
>
> **Recommendation to DHS:** If there are no technological protection requirements for the MRZ such as encryption, DHS should limit by regulation the contents of the MRZ, and in particular should consider the risks of including name in the MRZ.

4. Prohibiting by Law the Unauthorized Skimming of MRZ Data

The Conference Report on the REAL ID Act explicitly contemplates that the MRZ should "only be able to be read by law enforcement officials."[36] However, neither the Act itself nor the proposed regulations include this specific limitation. The PIA states, "the REAL ID Act does not contain any statutory language to address the downloading, access and storage by third parties of the information in the MRZ."[37] In the Preamble to the draft regulations, DHS recognizes that

---

[32] NPRM, Preamble at 10838 (emphasis added).

[33] NPRM, Proposed Rules §37.19.

[34] PIA at 17. *See also* NPRM, Preamble at 10826.

[35] PIA at 17.

[36] Conference Report on H.R. 1268, House Report 109-72, at 179.

[37] PIA at 14.

downloading from the MRZ is a serious concern, but it claims that it is powerless to address the problem:

> The ability of commercial entities and other non-law enforcement third parties to collect the personal information encoded on driver's licenses or identification cards raises serious privacy concerns. However, while cognizant of this problem DHS believes that it would be outside its authority to address this issue within this rulemaking.[38]

CDT believes that Congress should explicitly prohibit non-DMV or non-law enforcement third parties – including state and federal government agencies, and private businesses and other entities – from "skimming" personal data from the MRZ. Moreover, Congress should mandate that the MRZ be designed to prevent skimming.

Additionally, CDT disagrees with the Department's assertion that it is powerless to address the skimming problem. DHS could require security features in the MRZ to prevent "skimming" for non-DMV or non-law enforcement purposes and also require states to outlaw unauthorized skimming as a condition of certification.

While collection of personal data off the MRZ is already possible in a number of states, CDT believes that it is the responsibility of both Congress and DHS – given the REAL ID federal mandate – to address this serious national problem in the next generation of driver's licenses that will emerge as a result of REAL ID.

> **Recommendation to Congress:** Statutorily limit the collection of personal data from the MRZ to DMV officials for legitimate purposes related to the administration of driver's licenses and ID cards, and to law enforcement officials for legitimate law enforcement purposes consistent with existing law.

> **Recommendation to DHS:** Require states, as part of the certification process, to pass laws that limit the collection of personal data from the MRZ to DMV officials for legitimate purposes related to the administration of driver's licenses and ID cards, and to law enforcement officials for legitimate law enforcement purposes consistent with existing law.

[38] NPRM, Preamble at 10837. *See also* PIA at 14.

D. CONCERNS WITH A "UNIQUE" IDENTIFIER

The Act requires that the face of the driver's license or ID card show "the person's driver's license or identification card number."[39] While the Preamble echoes this language, the proposed regulations themselves refer to a "unique" number and require that it be included in the machine-readable zone. It is not clear whether the draft regulations require a number that would be unique state-by-state or nationally.

Significant privacy and security risks – most notably, the enhanced ability for tracking – would exist if the driver's license or ID card number were unique nationally, rather than within a state. The Privacy Impact Assessment assumes that "unlike a SSN, a person's driver's license number may change over time if the person moves from one state to another."[40] But neither the Preamble nor the proposed regulations say so.

Recommendation to Congress: Mandate that the driver's license or ID card number not be standardized and unique across states.

Recommendation to DHS: Mandate by regulation that the driver's license or ID card number not be standardized and unique across states.

Additionally, even though the PIA assumes that a REAL ID number will not be nationally unique, the document rightly notes that "if retailers, healthcare providers, financial institutions, insurers, and other private or government entities were to collect the credential and record the ID number whenever individuals engaged in a transaction, the REAL ID's unique number could pose the same, if not greater, risks as experienced in the use of the SSN."[41] Thus, "The only way to prevent misuse of any identifier is to establish enforceable restrictions at the time any REAL ID identifier is introduced."[42]

Recommendation to Congress: Carefully consider how use of the REAL ID identifier can be limited.

Recommendation: Carefully consider how states, as part of the "privacy" certification process, could limit the use of the REAL ID identifier.

---

[39] §202(b)(4).

[40] PIA at 6.

[41] PIA at 6.

[42] PIA at 7. The issue of using the card identifier as an anchor to access lots of other personal information is distinguishable from using the REAL ID card as a physical credential that verifies a person's identity for "official purposes" such as entering a nuclear power plant. *See* §201(3).

III. CONCLUSION

CDT supports driver's license and ID card reform by making the issuance process more secure, thereby making the cards a more reliable means of identifying an individual in a given context. However, the privacy and security shortfalls of both the REAL ID Act and the Department of Homeland Security's proposed regulations are many. Moreover, deficiencies in the regulations stem directly from fundamental flaws in the Act.

CDT urges Congress to create a robust statutory framework that achieves driver's license and ID card reform but that also protects privacy and ensures security. CDT also urges Congress to exercise its oversight powers – whether or not the Act changes – to ensure that the Department of Homeland Security addresses privacy and security within its implementing regulations to the maximum extent possible under the law.

State of South Carolina

Office of the Governor

MARK SANFORD
GOVERNOR

POST OFFICE BOX 12267
COLUMBIA 29211

March 26, 2007

The Honorable Daniel Akaka
Chairman
Subcommittee on Oversight of
Government Management
United States Senate
Washington, DC 20510

The Honorable George Voinovich
Ranking Member
Subcommittee on Oversight of
Government Management
United States Senate
Washington, DC 20510

Dear Messrs. Chairman and Ranking Member,

I would like to thank you for holding today's hearing on the implementation of the REAL ID Act (PL 109-13). These hearings will, I believe, offer Washington a chance to see how this far-reaching legislation will impact the lives of citizens around the country.

While we are committed to enhancing security measures, we need to make certain that the financial impacts - and all effective alternatives - are considered before implementing the REAL ID Act.

We have carefully evaluated how this Act will impact the State of South Carolina and I wanted to share those concerns with you today. I also ask that these comments be included in the written record for this hearing.

Unfunded Mandate to States

Currently, REAL ID is a costly unfunded mandate imposed on the states. The implementation and operating costs for REAL ID would be well in excess of $36 million for South Carolina. At this point, it appears that no cost considerations have gone into the proposed implementation of this plan. In my first term in the U.S. House of Representatives, Congress enacted the Unfunded Mandates Reform Act, which was intended to stop Congress from passing the costs of programs onto the states. REAL ID clearly violates the spirit of that law. Congress should only be willing to pass legislation it is willing to pay for and not simply pass the bill to the states.

Give States the Mission

The proposed process is entirely too prescriptive for states. General George S. Patton was quoted as saying, "Never tell people how to do things. Tell them what to do and they will surprise you with their ingenuity." The federal government should be more focused on outcomes and less on processes. If the intent is to establish a higher security level, give that mission to the states and let them meet it as they see best.

There are inherent risks associated with the drivers' license card security process that have not been factored into the federal process. The physical security of the actual drivers' license is only one segment of the overall licensing process for states. For instance, mandating a single set of card security features and card materials could create a serious security risk. Such a directive significantly reduces a state's ability to address security concerns with better technologies that are sure to be developed in the future.

Finally, states must be allowed to address customer issues with greater flexibility. For example, policy should allow for exception processing at the state's discretion, reporting exceptions as part of a self-certification process. Also, the time period to enroll citizens in the REAL ID program should coincide with the expiration date of their current license or identification card.

Security Concerns

A single set of security features allows a single, but fraudulent, production method to be effective at counterfeiting the drivers' licenses and identification cards of all states. We applaud the Department of Homeland Security's agreement to use adversarial testing to ensure a higher level of security for credentials. We would encourage them not to impose testing standards so restrictive that they mandate a specific technology or card stock.

In addition, our initial concerns over privacy of information have been addressed by the proposed regulations of the Department of Homeland Security. We would ask Congress to watch carefully to ensure that a federated database is not implemented and, instead, the pointer system, as is currently proposed, is maintained in the final rules.

Federal Accountability for Human Costs

The hurdles government creates have a cost in human terms that is rarely considered. In the case of the Department of Motor Vehicles, the impact of these rules will require more of each citizen's time - standing in long lines - wasting man hours that can be spent in a host of other ways.

The five-year implementation is expected to increase the number of in-office visits by 1.9 million here in South Carolina over a five-year period. These regulations will require us to choose between funding a growth in the number of employees to handle the additional workload or leave our citizens standing in endless lines. This is simply unacceptable.

If Washington officials do not provide the funds necessary to comply with these burdensome regulations, they should at least come and account for the cost on human lives in each state around the nation.

Again, thank you for your leadership on this issue. We hope that you will hold additional hearings to more carefully consider the impact of this program on the people of this country. We stand ready to work with you and your colleagues on any front to better address a reasonable and practical approach to implementing REAL ID. Take care.

Sincerely,

Mark Sanford
MS/se

cc: Marcia Adams, South Carolina Department of Motor Vehicles

STATE OF CALIFORNIA - BUSINESS, TRANSPORTATION AND HOUSING AGENCY ARNOLD SCHWARZENEGGER, Governor

OFFICE OF THE DIRECTOR
DEPARTMENT OF MOTOR VEHICLES
P.O. BOX 932328
SACRAMENTO, CA 94232-3280

April 9, 2007

The Honorable Daniel Akaka
Chairman, Homeland Security and Governmental Affairs Subcommittee on
Oversight of Government Management
141 Hart Senate Office Building
Washington, D.C. 20510

Dear Senator Akaka:

On behalf of the California Department of Motor Vehicles (DMV), I am writing to you and the Homeland Security and Governmental Affairs Subcommittee on Oversight of Government Management to clarify California's position relative to implementation of the federal REAL ID Act.

In truth, since the Act's inception, we have continually voiced concerns about California's ability, or any state's ability, to comply with the Act, under the proposed regulations (see the attached three-page document that we have repeatedly used to outline our critical issues and cost estimates). If the intent of the Act is to assure a national "one-driver, one record" system, then we are all for that.

We believe it is time for the Department of Homeland Security (DHS) to focus on a different implementation approach. To that end, DHS should consider a phased, prioritized process for REAL ID compliance. In lieu of an onerous recertification process with all its inherent challenges, the DHS should acknowledge and recognize states that have developed secure, front-end, initial issuance systems.

The California DMV has been verifying Social Security Numbers and Legal Presence Status for license issuance for many years, using the SSOLV and SAVE national databases. We have required digital images on our licenses for years and all the security provisions outlined in the Act will be incorporated in our new driver license and identification cards, including a biometric verification process. We would argue that the systems we have in place do, in fact, meet the intent of the Act, and that the DHS should so find. The first phase for meeting REAL ID compliance would be for states to show that they meet this level of front-end security.

The second phase of compliance acknowledges the evolution of the national implementation process, but does not hold compliance in abeyance. As additional national electronic verification systems would come online, they would be incorporated into the issuance procedures and would subsequently enhance system security provisions and further underscore the intent of the Act.

If DHS were to find that our existing systems and our new driver license and identification card security enhancements would meet compliance requirements for the Act, then the projected costs for implementation would be significantly reduced. We had initially estimated costs for REAL ID

implementation in the $500 million range, over the proposed five-year period. Obviously, we continue to be concerned about funding plans from the DHS that do not take into consideration California's needs.

In response to the Committee hearing testimony of Assistant Secretary for the Office of Policy Development Richard Barth of DHS, I would also like to clarify the scope of California's involvement with DHS in the development of the proposed REAL ID Act rules. California, Iowa, Massachusetts and New York have been working with DHS and the American Association of Motor Vehicle Administrators (AAMVA) on a limited information technology connectivity issue. That is, the development of a "federated" approach to create an interstate verification system for driver license information "pointer" system linking state databases. While we have also engaged in other workgroup sessions at DHS, the efforts of the four states in regular phone calls and meetings with DHS, referenced by Assistant Secretary Barth, were limited to the federated pointer system project.

California driver license and identification card issuance and recertification provisions incorporate the fundamental features proposed in the REAL ID Act. We would hope that the DHS would see and acknowledge that, and not overly focus on provisions in the proposed regulations that would be an undue burden and a challenge for all states.

Our proposed phased approach speaks to the importance of establishing a base line level of security which all states can achieve within a reasonable period of time. Once that phase is completed, all states would then move together to develop the highest security platform that can be achieved so that we have a national standard.

We would be most happy to discuss this phased approach in more detail with your staff. Please feel free to contact me at your convenience at (916) 657-6941.

Sincerely,

GEORGE VALVERDE
Director

Attachment

cc w/att.: Dale E. Bonner, Secretary
Business, Transportation and Housing Agency

Matthew Bettenhausen, Director
California Office of Homeland Security

Dennis A. Kamimura, Licensing Administrator
Customer Services Department

REAL ID Act -- Critical Issues for California

Gov. Schwarzenegger supports the REAL ID Act's goal of preventing terrorists from obtaining driver's licenses and identification cards (DL/ID cards) and California continues to work with the Department of Homeland Security (DHS) to implement the REAL ID Act. As DHS continues to develop regulations and Congress begins its work on appropriations, the following key aspects of the implementation should be considered:

- *Lack of Federal Funding*

Federal funding to the states through an appropriation from Congress to support implementation and ongoing program costs is essential to successful implementation. California's estimated costs could approach $300 million to $500 million over the next five years.

- *Re-credentialing of Current Cardholders from May 2008 to May 2013*

"Re-credentialing" all existing card-holders would require an in-person visit to a DMV field office and presentation of required documentation. This would require California to suspend its renewal by mail and Internet programs adding 2.5 million field office visits per year.

- *Lack of National Verification Database Systems*

The four national verification database systems required by REAL ID either do not currently exist or need significant enhancement. The Systematic Alien Verification for Entitlements (SAVE) system and the Social Security Administration Online Verification system, will require modifications prior to the implementation of the Act. Neither the Birth Record Verification Database nor the 50 State Cardholder Pointer System currently exists.

- *Information Security Safeguards*

Given the size of the databases and the number of users, information security and privacy and creation of fraudulent identification documents are of paramount concern.

- *Mandated Card Security Features*

California feels strongly that DHS rules should provide states with the maximum flexibility to utilize cards that meet accepted standards for security features and card materials. California estimates that certain proposed requirements could increase card costs by up to $250 million.

- *Implementation Timeframes*

There is simply not enough time to fully implement an effective, secure, reliable, state-administered, national drivers license and identification card system capable of verifying identity, residence, and legal presence, as envisioned by the Act prior to May 11, 2008.

- *A Phased, Prioritized Approach*

The looming specter of another terrorist attack necessitates that we do what we can now to improve the issuance process for driver's licenses and identification cards. This requires an approach to phase in implementation of the Act. We feel such a phased approach to certifying state's compliance efforts would allow DHS to insure all states meet a basic national standard for DL/ID cards by May 11, 2008, and to provide additional layers of security as they become available.

Additional Questions for the Record
For Richard C. Barth, Assistant,
Secretary for the Office of Policy Development,
U.S. Department of Homeland Security

Question#:	1
Topic:	Alternatives
Hearing:	Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers Licenses and Identification Cards
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: In response to my question on alternatives to REAL ID for individuals in Hawaii for inter-island travel, you said that the Department of Homeland Security (DHS) is looking at alternative documentation, such as a passport. Please elaborate on the alternative documentation that DHS is considering. What sort of documentation or verification process would those individuals have to go through to be able to board commercial airlines? What sort of privacy and security measures are in place on those cards?

Answer:

Neither the REAL ID Act nor the proposed implementing regulations published in the Federal Register in March 2007 determine what type of documents will be acceptable for commercial air travel inside the United States. The NPRM proposes that the boarding of Federally-regulated commercial aircraft be considered an "official purpose" for purposes of the Act. Both the Act and the NPRM are clear that a driver's license or identification card issued by a State that is not complying with the REAL ID Act could not be accepted as the individual's identification to board the aircraft. The types of alternative documentation that could be accepted is outside the scope of the rulemaking, which sets minimum standards for State-issued driver's licenses and identification cards.

The Transportation Security Administration (TSA) currently accepts a number of other documents, including a passport, which could still be used to establish an individual's identity for purposes of Federal-regulation of commercial air travel.

Question#:	2
Topic:	WH Privacy and Civil Liberties
Hearing:	Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers Licenses and Identification Cards
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: In response to my question as to whether the White House Privacy and Civil Liberties Board reviewed the regulations, you said no. Will you brief the White House Privacy and Civil Liberties Board on the proposed regulations? Will you share their comments and suggestions with my staff?

Answer:
DHS has generally discussed the REAL ID program with the Privacy and Civil Liberties Oversight Board and has offered to brief either the full Board or its staff at their convenience. In addition, the Privacy Board has discussed this program with the DHS Data Privacy & Integrity Advisory Committee, an advisory committee to the DHS Privacy Office.

Question#:	3
Topic:	Budget
Hearing:	Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers Licenses and Identification Cards
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: The DHS FY 2008 budget request for REAL ID is only $1.3 million. However, the proposed regulations estimate the cost near $14 billion. Why didn't DHS ask for more money to implement REAL ID?

Answer:
Congress appropriated $40M in grant funding to the States for REAL ID implementation under section 528 of the Department of Homeland Security Appropriations Act of 2006. $6M of the $40M was set aside to two States to begin pilot programs. DHS chose not to request additional FY 2008 implementation funding because the remaining $34M had not been awarded to the States, pending DHS submission and Congressional approval of the REAL ID Implementation Plan. DHS will distribute the remaining $34M to the States to help States comply with REAL ID requirements. DHS requested an additional $1.3M for FY 08 to provide funding for REAL ID program support.

In addition, DHS has announced that States can use up to 20% of their Homeland Security Grant Funding to assist in complying with REAL ID which makes funds almost immediately available to the States..

Question#:	4
Topic:	Databases
Hearing:	Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers Licenses and Identification Cards
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: While the Real ID Act requires states to verify information against certain databases, I understand that some databases do not exist currently and others are only in the pilot phase.
If the Commercial Drivers License Information System (CDLIS) is used to verify information from other states, when will this system be ready to include information on 240 million drivers? How much money is needed to make CDLIS ready to implement REAL ID?
What were the Department of State's comments on the REAL ID regulations, and when will the State Department's database be up and running? How much is the State Department seeking in its FY08 budget request to establish this database?
If the databases that need to be checked to have a REAL ID compliant license are not working, how helpful is REAL ID at achieving its mission?

Answer:

The CDLIS system is managed by the Department of Transportation (DOT) and is currently being upgraded to add additional capabilities. CDLIS is only one potential alternative that could be used to verify driver information from other states. DHS is also reviewing other existing and new capabilities that could also be used for states to verify information from other States. The REAL ID Program Office has established a system verification working group that will evaluate alternative solutions and the costs associated with those solutions. Once the REAL ID verification requirements are finalized, this group will make recommendations to the Secretary of Homeland Security for final decision.

As a general matter, we do not disclose comments received by another agency during the internal Federal government clearance process. All Department of State (DOS) comments received on the NPRM were resolved by DHS to the satisfaction of DOS and to the Office of Management and Budget.

The DOS databases referred to in the NPRM are already functional concerning passport holders, but that information is not available to DMVs . The primary issue DOS faces is how to make this existing information available to DMVs without compromising the privacy of the passport record holders. DHS is continuing to work closely with DOS on this important issue.

Question#:	4
Topic:	Databases
Hearing:	Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers Licenses and Identification Cards
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

The benefits of the REAL ID effort are not limited to the availability of all the necessary data verification databases. Improvements in the driver's license issuance process, the protection of personal data, and the security and integrity of the document issued by a DMV will also accomplish the goals and purposes of the REAL ID Act.

The NPRM solicited comments on data verification related to REAL ID, including comments on the availability and status of databases required for verification of customer identity documents by DMVs. Based upon comments received, DHS will issue a Final Rule and Certification and Compliance Guidelines that will address the issues of database availability and functionality for data verification under REAL ID.

Question#:	5
Topic:	States
Hearing:	Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers Licenses and Identification Cards
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: Under the regulations, a state is required to submit a certification document to DHS and a comprehensive security plan detailing how the state will protect the privacy of the data collected. What do states need specifically in their comprehensive security plan to be approved by DHS?

: Section 37.41 of the NPRM proposes that States provide a comprehensive security plan that includes:

- *Physical security for DMV facilities;*
- *Document and physical security features for the face of the card;*
- *Employee identification and credentialing, including background checks;*
- *Periodic training requirements in fraudulent document recognition;*
- *Privacy policy regarding personal information collected and maintained by the DMV;*
- *Emergency/incident response plans.*

DHS anticipates receiving comments concerning these proposed requirements and will review and consider these comments before finalizing the information that states shall be required to provide as part of their security plans.

Question#:	6
Topic:	Other uses
Hearing:	Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers Licenses and Identification Cards
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: Although the list of official purposes for using REAL ID is currently limited, it is possible for DHS to expand that list in the future. I have already heard some discussion of using REAL ID for purposes other than those currently listed in the REAL ID Act.

What are some other purposes where DHS believes the REAL ID card may be used? In light of the potential for widespread use of REAL ID, how do you respond to concerns that REAL ID will, in practice, become a national identification card?

Answer:

The NPRM does not prohibit states, nor agencies, from expanding the use of the REAL ID. There are many possible purposes and situations where a Federal Agency might want to require a secure form of identification, like a REAL ID, for official purposes. In the preamble to the NPRM, DHS noted that it considered including the acquisition of Federally-issued identification documents, such as a Transportation Worker Identification Credential (TWIC), military Common Access Card (CAC), U.S. passport, or PASSport card within the proposed definition of "official purpose." To do so would have been consistent with the concept of strengthening the reliability of identity documents, one of the primary objectives of the Act. However, since no state would be required to fully implement REAL ID driver's licenses and identification cards until May 2013 to participate in the program, DHS concluded that it would be premature to require Federal agencies to accept only REAL ID driver's licenses and identification cards during the phase-in period and that the imposition of such a requirement could inhibit individuals from obtaining these necessary forms of Federal identification. However, once implemented, DHS will carefully reconsider whether to further expand the definition of "official purposes" to possibly leverage the security benefits of the REAL ID Act across a multitude of programs.

REAL ID is not intended to create a national identification card. Rather, it is designed to establish minimum standards for state-issued drivers' licenses and identification cards that Federal agencies would accept for official purposes as defined by the rule. There will be no interconnected repository of records as a result of the implementation of REAL ID. Neither the REAL ID Act nor the NPRM creates a national database of information on individuals who will possess a REAL ID-compliant document. The operation and control of both the state data query of Federal databases and the state-to-state data exchange will be left to the states. Appropriate standards will be in place to ensure the integrity and privacy of personal information. Additionally, there is no Federal requirement that everyone in a state possess a state-issued driver's license or identification card.

Question#:	7
Topic:	Privacy
Hearing:	Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers Licenses and Identification Cards
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: The proposed regulations state that DHS sought to provide for privacy and security to "the extent of its authority." However, the regulations ask for comments as to whether the privacy protections are adequate. Please detail the privacy laws and principles that DHS had to follow in issuing the proposed REAL ID regulations.

DHS is very cognizant of the importance of protecting privacy in connection with implementation of the REAL ID. In drafting the NPRM, DHS considered a number of current Federal privacy protections, including the Driver's Privacy Protection Act (DPPA) and the Privacy Act of 1974, and the extent to which they would or would not apply to the personal information related to REAL ID information that is held by the States. A discussion of the scope of the DPPA and its limitations was included in the Preamble of the NPRM. The NPRM did not discuss the Federal Privacy Act, however, as the NPRM contemplates that the information collection and data verification network to implement REAL ID would remain a State-controlled and operated process. The NPRM section on Privacy Considerations, however, does emphasize the importance of States developing appropriate privacy protections, including security safeguards based on the Fair Information Principles, which are the basis of the Privacy Act as well as numerous State privacy laws and private sector codes of practice. In developing the Final Rule, DHS may consider providing additional guidance to the States regarding the protection of the personal information collected and maintained related to REAL ID implementation as part of the certification requirement for a comprehensive security plan. The NPRM sought public comment on the nature of the protections that should be included in the security plan and will consider those comments in drafting the Final Rule. In addition, DHS may consider using principles such as those contained in the Privacy Act and Federal Information Security Management Act (FISMA) as models to help State's protect information quality.

Question#:	8
Topic:	Costs
Hearing:	Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers Licenses and Identification Cards
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: As part of the concern over the cost of implementing REAL ID, many states and localities are concerned that they will be charged by the federal government or other states for validating information from the various federal and state databases. Will states be charged for verifying information against federal and state databases?

DHS does not own or operate most of the databases that might be used for data verification under REAL ID and cannot provide information about costs or fees for using these databases. However, DHS does own the SAVE system, and electronic immigration verification service operated by U.S. Citizenship and Immigration Services (USCIS). Through SAVE, Federal, state, and local agencies and organization are able to verify immigration status in order to determine eligibility for Federal, state, or local benefits. Costs for queries to SAVE are currently minimal, with a fee of approximately $0.20 per initial query. As part of USCIS' ongoing effort to ensure that fees are set at an appropriate level to recover costs, USCIS has initiated a new fee study for the SAVE program.

Question#:	9
Topic:	NGA/NCSL
Hearing:	Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers Licenses and Identification Cards
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: The National Governors Association and the National Conference of State Legislatures both testified as to the need for an extension on the deadline to complete reenrollment, a transition to requiring states to comply with electronic verification, and for flexibility for states to waive certain segments of the population from the requirements of REAL ID and encourage state innovation. What is DHS's response to each of these suggestions?

Answer:

These issues have been raised several times during DHS outreach efforts, and we would expect that these proposals will be raised in the comments on the NPRM that are filed in the public docket. DHS will give every comment, including those filed by the National Governors Association and the National Conference of State Legislatures, careful and appropriate consideration in developing a Final Rule.

Question#:	10
Topic:	Budget
Hearing:	Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers Licenses and Identification Cards
Primary:	The Honorable George V. Voinovich
Committee:	HOMELAND SECURITY (SENATE)

Question: Dr. Barth, DHS estimates that it will cost $23 billion to implement REAL ID throughout the country. To date, Congress has appropriated only $40 million to assist states with the implementation. The President's FY2008 budget request did not include any funding for states to implement the requirements of the Real ID. Do you think it is possible for states to implement and sustain REAL ID within the current timeframe without an annual appropriation and grant process?

Answer:
DHS believes that it is possible for States to implement REAL ID within the proposed time frames. It is important to note that some States have made significant investment and progress toward REAL ID compliance are far better positioned to meet the time frames than those that have not. DHS has announced that States can use up to 20% of their Homeland Security Grant Funding to assist in complying with REAL ID. Also, DHS will use the remaining $34M appropriated by Congress to help States become compliant.

Question#:	11
Topic:	WHTI
Hearing:	Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers Licenses and Identification Cards
Primary:	The Honorable George V. Voinovich
Committee:	HOMELAND SECURITY (SENATE)

Question: Dr. Barth, as you know, the Administration is also moving forward with implementation of the land portion of the Western Hemisphere Travel Initiative. I want to ensure ample consideration is given to creating interoperability among the various screening tools and identification documents. Has DHS given thought to accepting REAL ID compliant licenses for use at the land border with Canada? Has DHS considered allowing a waiver for individuals who have been through a federal government vetting process -- such as an individual with a security clearance or a military ID card?

Answer:

DHS has given careful consideration to the potential overlap between REAL ID and the Western Hemisphere Travel Initiative (WHTI). There are significant differences between the REAL ID Act and section 7209 of the Intelligence Reform and Terrorism Prevention Act of 2004. A WHTI-compliant document must denote a person's citizenship. There is no such requirement in the REAL ID Act. Congress specifically provided that non-citizens lawfully present in the U.S. may obtain a REAL ID-compliant driver's license or identification card. Thus, a REAL ID-compliant license would not, by itself, satisfy crucial WHTI requirements. In addition, DHS and the Department of State are seeking to incorporate technologies that facilitate the legitimate movement of travelers through ports of entry in WHTI-compliant documents. States can fully comply with the REAL ID Act without incorporating the type of radio frequency identification (RFID) technology that DHS and DOS are seeking to use in a WHTI document. However, States may wish to develop identification cards that go beyond what is mandated by the REAL ID Act and include features required by WHTI. For example, Washington State and DHS have executed a Memorandum of Agreement through which Washington will issue an enhanced driver's license that can serve as a WHTI-compliant document.

DHS is continuing to examine how other documents might be used and will review this in the review of comments filed during the public comment period.

Question#:	12
Topic:	Cost burden
Hearing:	Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers Licenses and Identification Cards
Primary:	The Honorable Ted Stevens
Committee:	HOMELAND SECURITY (SENATE)

Question: Mr. Barth, I do share a concern with many of my colleagues about the cost. I am also concerned that the only source of funding DHS is providing to states is through their homeland security grants. These grants are already stretched thin. Does DHS have any other grant proposals states could apply for to aid in the enormous costs associated with Real ID?

DHS does not anticipate using other grant proposal categories as a way that States could seek to comply with REAL ID. States, can, of course, build REAL ID compliance costs into their overall State homeland security plans and proposals to DHS.

Question#:	13
Topic:	Remote renewal
Hearing:	Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers Licenses and Identification Cards
Primary:	The Honorable Ted Stevens
Committee:	HOMELAND SECURITY (SENATE)

Question: Mr. Barth, I am pleased to see that DHS will have a remote renewal process. This is particularly important in a state like Alaska where so many Alaskans live in remote villages, accessible only by air. As a mater of fact, there are areas of Alaska where they currently issue driver's licenses without a photo. These are called "valid without photo I.D.'s" and are given to rural residents not located near a state DMV office.

It is important to make sure that all Americans have reasonable access to obtaining these I.D.'s since they will need them for boarding planes and entering federal buildings, among other things. It is equally important that they be able to renew as easily as possible. What do you plan to do to accomplish this?

Answer:

DHS has proposed that, once a person has obtained a REAL ID, a State should be able to renew that license through whatever remote process the State chooses to use – as long as the State establishes an effective procedure to confirm or verify a renewing applicant's information, as required under the REAL ID Act, and can ensure that it is actually renewing the license of the person who obtained the REAL ID. DHS has not sought to limit the flexibility of the States on how to provide remote renewal services, and believes that State DMVs will use a wide variety of approaches that best serve the residents of their States.

NATIONAL CONFERENCE of STATE LEGISLATURES

The Forum for America's Ideas

Leticia R. Van de Putte, R. Ph.
State Senator
Texas
President, NCSL

Stephen R. Miller
Chief, Legislative Reference Bureau
Wisconsin
Staff Chair, NCSL

William T. Pound
Executive Director

May 25, 2007

The Honorable Daniel Akaka
Chairman
Subcommittee on Oversight of Government
Management, the Federal Workforce and the
District of Columbia of the Committee on
Homeland Security and Governmental Affairs
Washington, DC 20510

Dear Chairman Akaka:

Thank you for the opportunity to answer your follow-up questions regarding the March 26, 2007 hearing—*Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers Licenses and Identification Cards*.

Question 1: *Your testimony listed several recommended changes to the proposed regulations and the need for federal funding. Do you believe legislation is needed to address your concerns about Real ID or do you think DHS can make changes through regulations alone?*

Congressional action is needed to "fix and fund" the Real ID. It is within the department's rulemaking authority to "fix" the Real ID by adopting some of the recommendations made in my testimony. However, based on meetings with Assistant Secretary Barth, we are not optimistic the final regulations will reflect a 10-year, progressive reenrollment period or exempt certain populations from the Real ID process. These two recommendations, if adopted, would significantly reduce the cost to implement the Real ID.

Because it is not within the department's rulemaking authority to "fund" the Real ID, congressional action will be needed in this area. NCSL has urged the House and Senate Budget and Appropriations Committees to include at least $1 billion in FY 2008 for state start-up costs.

Question 2: *In response to my question to Assistant Secretary Barth about what legislative changes he would recommend be made to Real ID, he said Congress should consider increasing penalties for Department of Motor Vehicle employees who steal personal information. What is your view of this recommendation?*

Congressional action is not needed to address this issue because all 50 states have laws regarding identity theft, fraud and bribery, which carry with them requisite charges and penalties—civil or criminal—depending on the crime. There is no need to federalize these areas of very well developed state criminal law.

Denver
7700 East First Place
Denver, Colorado 80230
Phone 303.364.7700 Fax 303 364 7800

Washington
444 North Capitol Street, N.W Suite 515
Washington, D C 20001
Phone 202 624 5400 Fax 202 737 1069

Website www ncsl.org

Question 3: *There has been a great deal of discussion over the sharing of data or verifying of data with various databases. Which databases do Texas licensing and ID programs tie into currently?*

Texas currently utilizes the American Association of Motor Vehicle Administrators' network to access pointer information on commercial drivers as well as problem drivers. When a pointer (identifying a record in another state) is identified, then a state to state connection is utilized to gain more information about the individual record. In response to verification of data, we currently communicate with the Social Security Administration to verify Social Security Number information.

Thank you again for the opportunity to testify. NCSL is encouraged that you and other federal lawmakers recognize the challenges states face in implementing the Real ID. We look forward to working with you to "fix and fund" the Real ID. For additional information, please have your staff contact Molly Ramsdell (202-624-3584; molly.ramsdell@ncsl.org) in NCSL's Washington, D.C. office.

Respectfully,

Leticia Van de Putte
Texas Senate
President, NCSL

Additional questions for the Record
For Mufi Hannemann, Mayor, and
Dennis Kamimura, Licensing Administrator,
City and County of Honolulu, Hawaii

1. Your testimony listed several recommended changes to the proposed regulations and the need for federal funding. Do you believe legislation is needed to address your concerns about REAL ID or do you think DHS can make changes through regulations alone?

RESPONSE:

DHS has continuously indicated that jurisdictions must pursue funding through the congressional representatives. As such, the funding issue requires legislative action.

Aside from funding, the majority of our recommended changes could be implemented with DHS' publication of the final rule. However, we are concerned that the number of changes that are being recommended by the jurisdictions may not be reflected in the final rule. We recommend that a second NPRM be issued by DHS for the jurisdictions to have another opportunity for comment.

There are several provisions of the Act that are of concern to Hawaii:

(a) The Act requires that the states must capture digital images of identity source documents so that the images can be retained in electronic storage in a transferable format. States must retain paper copies of source documents for a minimum of seven years or images of source documents presented for a minimum of 10 years. This is a massive amount of storage space and a tremendous burden on Hawaii. We question the necessity of retaining copies of documents especially since all documents that are presented must be verified by the issuing agency. Retention of these personal documents creates unnecessary privacy and security risks resulting from compromise or theft. For purposes of law enforcement or any future clarification of data, we could require the applicant to present the original documents upon demand or the applicant's license could be canceled. We recommend that this section be repealed or amended by allowing the jurisdictions the flexibility to determine what documents, if any, will be retained by the jurisdictions.

(b) The Act requires that a noncompliant license or ID card clearly states, on its face, that it may not be accepted by any federal agency for any official purpose; and uses a unique design or color indicator to alert federal agency and other law enforcement personnel that it may not be accepted for any such purpose. If the license or ID card clearly states that the card is NOT REAL ID COMPLIANT, we question the rationale for the increased cost to develop a unique design or color indicator. Additionally, if the majority of jurisdictions will be issuing noncompliant licenses or ID cards, it would make more sense to brand REAL ID Compliant cards – "REAL ID COMPLIANT" since jurisdictions that decide to not comply with the Act do not have a statutory requirement to brand their licenses or ID cards. We recommend that this section be repealed or amended by requiring the branding of REAL ID Compliant cards.

Additional Questions for the Record

2. In response to my question to Assistant Secretary Barth about what legislative changes he would recommend be made to REAL ID, he said Congress should consider increasing the penalties for Department of Motor Vehicle employees who steal personal information. What is your view of this recommendation?

RESPONSE:

We do not agree with Assistant Secretary Barth. Department of Motor Vehicle employees who steal personal information should not be single out for penalties that are harsher than another person convicted of the same crime.

3. There has been a great deal of discussion over the sharing of data or verifying data with various databases. Which databases do Hawaii licensing and ID program tie into currently?

RESPONSE:

Hawaii driver license offices use the American Association of Motor Vehicle Administrator's AAMVAnet infrastructure for connectivity to the following verification programs - Social Security Online Verification System (SSOLV), Commercial Driver License Information System (CDLIS) and Problem Driver License Pointer System (PDPS).

Additional Questions for the Record

4. You have stated that the Commercial Driver License Information System (CDLIS) is not a central database and not vulnerable to hacking. Could you explain how this system works?

RESPONSE:

CDLIS has operated in all 51 U.S. jurisdictions (50 states and the District of Columbia) since April 1, 1992. As of March16, 2007, CDLIS has 13.2 million records, growing at an average rate of more than 40,000 new records per month. CDLIS consists of a Central Site and nodes at the Motor Vehicle Agencies (MVAs) of the 51 jurisdictions. The Central Site houses identification data about each commercial driver registered in the jurisdictions, such as:

- name
- date of birth
- Social Security Number
- state driver license number
- AKA information
- sex
- height
- Current "State of Record" (SOR)

This information constitutes a driver's unique CDLIS Master Pointer Record (MPR). Each MVA houses detailed information about each driver for which it is the SOR. This detailed information, called the driver history, includes identification information, license information, and a history of convictions and withdrawals, and remains in each individual jurisdiction—not in a central data base.

When a jurisdiction MVA queries CDLIS to obtain information about an applicant prior to issuing a CDL, the CDLIS Central Site compares data provided by the State Of Inquiry (SOI) against all MPRs in CDLIS. If one or more matches are returned, then the CDLIS Central Site "points" the inquiring jurisdiction to the jurisdictions where those matches have been found. The SOR can then provide the detailed information about the driver's commercial driving history.

In accordance with the CMVSA of 1986, access to CDLIS is authorized to only the state driver's license agencies, the Federal Motor Carrier Safety Administration (FMCSA), employer or prospective employer of a person who operates a commercial motor vehicle and federal agencies upon written request and approval by FMCSA where there is a legal basis and need to access the information commercial motor vehicle drivers who wish to review and, if necessary correct information about them in CDLIS. Access to CDLIS is provided via a secure private network operated by the American Association of Motor Vehicle Administration and cannot be accessed via the Public Internet. Each site connected to the private network has its access controlled via several security mechanisms which include:

- a network security layer which restricts each site's network access to its authorized trading partners.
- a messaging infrastructure which also restricts the network traffic to only the authorized locations, and

- finally a security table at the CDLIS central site level controlling access levels on a site by site basis.

Neither the State of Hawaii nor the American Association of Motor Vehicle Administrators (AAMVA) is aware of any privacy breaches of CDLIS since it went in production in 1989.

On August10, 2005, Congress passed the transportation reauthorization bill, the "Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users" (SAFETEA-LU), and authorized $28 million to modernize CDLIS. This effort is currently underway and is scheduled for completion by the end of 2010.

The State of Hawaii and AAMVA are recommending leveraging this project and the federal funding associated with it to expand the scope of the CDLIS modernization effort to support an all-driver pointer system for non-commercial driver's licenses and ID cards. Using the proven CDLIS architecture, this system will provide the jurisdictions with a robust driver license/ID card pointer system, designed to handle 250 million records. This system will allow the jurisdictions to enforce the concept of one person/one REAL ID document/one record mandated by the REAL ID Act.

The use of a CDLIS like system to support the REAL ID requirements will not increase the risk of data privacy breaches. In fact, when Congress passed the Motor Carrier Safety Improvement Act (MCSIA) of 1999 (Pub. L. 106–159, 113 Stat. 1759), it required that all drivers, both commercial and non-commercial, be checked through CDLIS before motor vehicle agencies issue or renew a driver's license. The thought is that if the person is allowed to have more than one license, they will spread their traffic violations across those licenses and therefore avoid driver control action and pose a highway safety risk. As noted in the DHS *Privacy Impact Assessment,* issued in conjunction with the REAL ID Notice of Proposed Rulemaking:

> As described in Section II.E of the NPRM, although the REAL ID Act poses a requirement for this state-to-state data exchange, this exchange is already required and implemented under the Department of Transportation's (DOT) existing rules and regulations governing commercial driver's licenses (CDLs). The DOT requires that states connect to the National Driver Register (NDR)/Problem Driver Pointer System (PDPS) and the Commercial Driver's License Information System (CDLIS) in order to exchange information about commercial motor vehicle drivers, traffic convictions, and disqualifications. A state must use both the NDR/PDPS and CDLIS to check a driver's record, and also check CDLIS to make certain that the applicant does not already have a CDL. Under these programs, as well as under the REAL ID Act, the primary purpose of the state-to-state data exchange is to determine if the applicant is unqualified and if the application is fraudulent rather than specifically verifying the applicant's identity.
>
> The existing state-to-state data exchange among DMVs, while focused on commercial driver's licensing, also impacts non-commercial license applicants, as states are required currently to run all license applicants against the PDPS and CDLIS, which are both pointer systems that collect limited information from each state in order to match against the incoming inquiries. Both systems offer certain mandatory privacy protections.

The all-driver pointer system, once developed and implemented, would subsume both CDLIS and the National Driver Register's (NDR) Problem Driver Pointer System (PDPS); but until an all-driver pointer system is fully implemented in all 55 jurisdictions, all three systems would continue to operate concurrently.

The states are very familiar with the CDLIS program and the all-driver pointer system would use the same principles as CDLIS; however, the technology used will be more efficient.

For further information regarding AAMVAnet and CDLIS, please contact:
Mr. Michael R. Calvin
Interim President and CEO
American Association of Motor Vehicle Administrators
Telephone: (703) 908-8262
Fax: (703) 908-2851
Email: MCalvin@aamva.org.

Additional Questions for the Record
For Mr. David Quam, Director, Federal Relations
National Governors Association
Submitted by Senator Daniel K. Akaka

1. **Your testimony listed several recommended changes to the proposed regulations and the need for federal funding. Do you believe legislation is needed to address your concerns about REAL ID or do you think DHS can make changes through regulations alone?**

Although DHS has some discretion to implement the recommendations outlined in my testimony, legislation is necessary if states are to meet the objectives of Real ID.

First, additional funding sufficient to implement Real ID can only be provided by Congress. NGA has asked Congress to begin funding Real ID by providing $1 billion in fiscal year 2008 to fund the up-front costs of developing and deploying the systems necessary to implement the program. DHS proposals to allow states to use existing homeland security grant funds for Real ID do little to offset the cost of the program and ignore the fact that such funds have already been obligated to other homeland security priorities.

Second, Congress should change the statutory deadline of May 2008 to provide states with adequate time to plan, develop and implement the statute and re-enroll their populations. DHS has recognized that the statutory deadline is unreasonable and shown willingness to extend compliance dates without direct statutory authority. Changing the compliance dates in the law would provide DHS with the authority to set reasonable compliance milestones and provide states with the certainty they need to make long-term planning and procurement decisions.

Third, Congress should clarify that states will only be required to use electronic verification systems when such systems are fully operational and deployed. Enhanced verification is the cornerstone of REAL ID. Reliance on the Secretary's discretion to waive the verification requirements is not sufficient to address broad state concerns that their ability to comply with REAL ID depends upon still undeveloped and unfunded electronic systems.

2. **In response to my question to Assistant Secretary Barth about what legislative changes he would recommend be made to REAL ID, he said Congress should consider increasing the penalties for Department of Motor Vehicle employees who steal personal information. What is your view of this recommendation?**

NGA's Permanent Policy calls on the federal government to avoid federal preemption of state laws and policies, especially in areas of primary state responsibility such as criminal justice. States have sufficient criminal statutes and penalties to address instances in which a DMV employee steals or participates in an organized effort to steal personal information. Congress and DHS instead should focus on making changes to REAL ID that will help states meet the objectives of the Act.

○