DEPARTMENT OF HOMELAND SECURITY

DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE

FULL COMMITTEE MEETING

WEDNESDAY, March 21, 2007

Crowne Plaza Washington National Airport

Arlington Ballroom

1480 Crystal Drive

Arlington, VA 22202

MORNING SESSION

MS. RICHARDS: Good morning everybody. My name is Becky Richards. I'm the Executive Director of the DHS Data Privacy and Integrity Advisory Committee at least until 5:30 at which point we will be turning it over to someone else. So with this we begin this meeting.

MR. BEALES: Thank you Becky and welcome everyone to our public meeting today. If you would, please be sure your cell phones are turned off. That would be helpful to all of us. If you are interested in signing up for public comments please do so with Tamara back at the registration table by where you came in. As is our custom we'll have a public comment opportunity at the end of the meeting, but you do need to sign up.

There are meeting materials on the table in the back of the room here. There is a bound document with a cover for the REAL ID Privacy Impact Assessment. That actually includes all of the DHS-related materials. The copying company bound them all together. So it's a package deal. You have to take all the DHS stuff or nothing.

We will begin this morning by hearing from the DHS Privacy Office. Hugo Teufel is the Chief Privacy Officer, but he is testifying in front of the Senate Appropriations Committee this morning. He thought that was a higher calling than us and I can't

disagree, and so we will hear from Ken Mortensen today who's the Acting Chief of Staff in the Privacy Office. Welcome Ken.

MR. MORTENSEN: Thank you very much Howard and thank you very much to the committee. It's wonderful to see you all again and as Howard mentioned, Hugo is testifying this morning up on the Hill in front of the Appropriations Committee talking about privacy operations within the department relating to our funding. And unfortunately he sends his regrets. He would like to be here, but when the Hill calls we do like to be able to answer them as well.

What I thought I'd do is provide you with an update as to what has occurred since we last met in Miami on December the 5th and explain some of the things that have changed and also explain some of the things that were in process but have finalized since then. The first thing I would like to talk about is the structure of the Privacy Office. You may recall that Hugo mentioned that he was in the process of restructuring the office into two main functionalities: a privacy functionality and a FOIA functionality. In Miami you heard from Catherine Papoi who is the Deputy Chief FOIA Officer for the office and since we met we have brought on a full contingent of FTEs to support her, two associate directors, one that focuses specifically on the processing of FOIA requests received in by the department for headquarters operations for which we are responsible of processing those particular FOIA requests and another associate director whose job is to coordinate and manage the policy and programs both from a cross-cutting sense, for example, we may have many FOIA requests that touch many different parts of the department, will be requests for documents that will come out of different components as well as trying to unify and harmonize the policies with regard to disclosure throughout the department, one of the key things that Hugo is attempting to do. All of this is being done to establish the function so that we are able to respond better to the disclosure operations which we've always discussed in the Privacy Office as being the third pillar, the Freedom of Information Act is the third pillar of privacy which is also supported by the Executive Order 13392 in which the President asked all federal departments to look at their FOIA processing disclosure processes, and that is part of what is being accomplished there.

On the privacy side we took a look at what our organic statute required us to do. Section 222 of the Homeland Security Act has certain specific duties that are assigned to the privacy officer for the department. Those duties are ones that you are familiar with. The first one is that we have the duty to ensure that the technology used by the department sustains and does not erode the privacy protections of individuals. Second duty is to ensure that the systems and records that are maintained by the department are done so in compliance with the Privacy Act of 1974. The third duty is for us to review the impact of legislation - federal legislation and regulation as it relates to the collection, use and dissemination of personal information throughout the federal government. The

fourth one deals with doing privacy impact assessments on the rulemakings of the department to understand the impact that those have on personal privacy. The fifth and sixth ones deal with coordination with the Office of Civil Rights and Civil Liberties and our reporting functionality to the Congress on our annual report. With regard to those particular functions what we've done is we've kind of realigned although we really haven't changed the structure much in that we've looked at those in terms of what was being accomplished. We now have four major sub- functions if you will within privacy. Some of them you're familiar with. We have compliance which Becky Richards is the Director for Privacy Compliance throughout the department. We have International Affairs. John Kropf who you've met in the past is the Director for International Privacy Policy. We have technology. Peter Sand is the Director of Privacy Technology. And the new one which is the Director for Legislative and Regulatory Affairs which is Ken Hunt who you will meet later today. In addition to the duties of Subsection 4 which was the privacy impact assessments of the rulemakings of the department which Ken will be responsible for and also Subsection 3, reviewing legislation and regulation across the federal government. Ken's duties will also include being the Executive Director of your committee. So Ken will be the new Becky, although obviously will not replace her in your hearts. Ken is also going to be the Executive Secretary for the Data Integrity Board which is an official internal board required under the Privacy Act with regard to the approval and processing through the departmental matching agreements. So Ken has a very large amount on his plate. In fact he basically had a baptism of fire. As I will mention a little bit later we've had two Hill hearings and a number of briefings that we've been doing in the last month. Ken has been running around getting together all the testimony and supporting briefing materials for that. So the new structure we're hoping will also to be able to better meet the needs and our duties under Section 222 and allow us to be able to apply what we are learning to the programs within the department appropriately. And as you will hear today one of those things has already occurred with regard to the REAL ID implementation, the notice of proposed rulemaking that went out and the PIA that we promulgated and was approved by our office this past March 1 when the notice of proposed rulemaking came out. That was the exercise of our duties under Subsection 4 where we reviewed the rulemaking and we put out a privacy impact assessment on that rulemaking itself.

As I mentioned Hugo is testifying today. Today his testimony is in front of the Appropriations Committee mainly looking at budget issues, but also trying to understand the privacy operations within the department. So he will be talking specifically about some of the things that we are doing with regard to operations. Last week Hugo was in front of the Subcommittee of the House Homeland Security Committee. He was testifying with Charlie Allen who is our Chief Intelligence Officer at the department and also he was testifying with Dan Sutherland who is the Chief of the Office of Civil Rights and Civil

Liberties, and the particular topic that they were talking about was the creation of fusion centers. I know that some of you may be familiar with these particular programs, but there are a number of fusion centers throughout the country. These are run on a state and local level. The idea is to bring together different resources on those levels to allow people from first responders to law enforcement on federal, state, local, tribal and even in some cases the consideration of bringing private sector folks from critical infrastructure in in order to allow there to be situation awareness, operational information-sharing. And in that regard one of the things that we've begun to do is to look at the privacy issues associated with this collaborative environment. Obviously there are a number of issues with regard to the exchange of information and how that information will be exchanged in the processes in that vein. One of the things that we will be building upon is that the Department of Justice and the Department of Homeland Security have issued guidelines on how to implement a fusion center and in those guidelines are a number of different suggestions on how to build privacy practices into the creation of a fusion center. We would like to take that a little bit further as we move forward. This is something that we would like to provide specific guidance with regard to privacy, incorporating some of our compliance operations that we have done for the department into those operations as we move forward with that.

One last thing I'd like to mention -- some of you may be aware, but the General Accountability Office has done a review of the Privacy Office. The review was entitled Privacy Office Effectiveness. They have announced that this is ongoing and right now our understanding is that we hope to see the letter report out probably late April/early May is when we would expect that it would be finalized and available. We will certainly make that available to the committee when it comes out for you to be able to review that. I will say just generally I think GAO had good views about us, but were constructive in some of the criticisms that they had, and we're hoping that this will be something that we can use to build upon what we've accomplished so far and to understand what the gaps are in the mission as we move forward. Thank you very much Howard.

MR. BEALES: Thank you Ken. Are there questions for Ken?

MS. MCNABB: Thank you. Ken, could you tell us a little more about what kind of amplification to the privacy practices regarding fusion centers that you're contemplating?

MR. MORTENSEN: Certainly. One of the things that we are involved in that's related to the fusion centers is the information-sharing environment. Hugo is the information-sharing environment privacy official. If you recall some time ago we may have discussed the information-sharing environment in general. There were back in December I think about the time our Miami meeting was the information-sharing environment program manager, Ambassador McNamara released a number of different guidelines looking at different functionalities. There was something called Guideline 5

which was the privacy guidelines with regard to the information-sharing environment. The original group set up to handle that was chaired by Alex Joel who was the Civil Liberties Protection Officer of the Office of Director of National Intelligence and it was co-chaired with Jane Horvath who is the Chief Privacy and Civil Liberties Officer at the Department of Justice. We also participated in that. And that created a framework from which the information-sharing controls and privacy protections were to be built upon by each agency. Out of that there is a specific area dealing with state, local and tribal which relates to the fusion. Hugo was asked to chair and has accepted to chair the working group for state and local with I'm going to forget the gentleman's name from the FBI, but the FBI and DHS Privacy Offices will be looking at the particular issues to develop specific guidance so that that can tailor and combine in with the guidelines for the standing up of a fusion center. So what we're going to do is look at things such as how if any changes would be necessary for privacy impact assessments. You know, when would you apply a privacy impact assessment. Are there any particular issues that are process issues that need to be addressed while you're standing these up that would impact privacy going forward? So we're hoping that sort of in terms of a development phase that as they are developing it they think about the privacy issues as opposed to just reviewing them at the end once the centers are stood up.

MS. MCNABB: And would they be consulting any state and local people in this development process?

MR. MORTENSEN: I believe we will be and I certainly hope that we would. I do know that Hugo would like to reach out and talk to various different folks and certainly DHS does have a very active state and local office that does reach out on a regular basis and we are working with them, have worked with them in the past.

MR. BEALES: Any other questions? All right, thank you very much Ken. With that we will move to our consideration of REAL ID which is our subject for the two morning panels. We will begin with a rulemaking overview. I should note at the beginning that Joanne McNabb is recusing herself from the discussion and deliberation on REAL ID because of her position with the California State government. We'll miss you. With us today for our first panel is Jonathan Frenkel who's the Senior Policy Advisor in the Department of Homeland Security. Mr. Frenkel is the Director for Law Enforcement and Information Sharing Policy. He oversees policy development for issues involving the DHS law enforcement agencies as well as intelligence and information-sharing policy. He also leads the department's work on a number of identity-related programs including REAL ID, the Western Hemisphere Travel Initiative and the department's work with HHS on minimum standards for birth certificates. Mr. Frenkel has been with DHS since its creation in March of 2003. So Mr. Frenkel.

MR. FRENKEL: Thank you, good morning. Thank you Mr. Chairman. I'd also like to thank Hugo in absentia, to Ken, Becky, Toby Levin and the rest of the DHS Privacy Office. I think sometimes those outside the department are - may find it hard to judge the work of the Privacy Office, but from someone who works with them closely I can tell you and everyone else in the room that they are very forceful advocates for privacy positions. Sometimes I agree with them, sometimes I disagree with them, but they are always very forceful advocates and do an extremely capable job of representing those interests within the department.

I think as you all know on March 1, 2007, DHS released a notice of proposed rulemaking concerning minimum standards states would need to follow in order to issue driver's licenses and identification cards that could be accepted by federal agencies for official purposes. The NPRM was published in the Federal Register on March 9 and all members of the public are able to file comments for DHS to consider in the drafting of the final rule. As a side note I want to make clear that any exchanges that may take place here today are not official comments for DHS for purposes of the docket. If you have something you want DHS to consider for the rulemaking you have to follow procedures set forth in the NPRM for filing a comment so that it's visible on the docket, a concept I think you would all endorse, the transparency of the exchange.

There was a significant amount of misinformation about the REAL ID Act and the NPRM leading up to the release and publication of the NPRM. Some of that misinformation continues to be circulated. Earlier this week for example a Missouri legislator was quoted as saying that the NPRM, quote, 'Could result in a Big Brother kind of system with a government able to track a person's every move through a computer chip,' end quote. That is utter nonsense, wrong on so many fronts that it's hard to know where to begin. As ill- informed as that legislator is about the Act and the NPRM, we recognize that the Act in our proposed implementing regulations raised privacy issues worthy of serious debate and consideration, and we ask you and everyone who has something to say about the privacy issues relating to the REAL ID Act to engage on that level. Some, and you may hear it even on the next panel, want the Act repealed. That is beyond the power and authority of the Department of Homeland Security to do anything about. You're entitled to that view, everyone is entitled to that view, but what will help us the most obviously is constructive suggestions working within the NPRM about how to address the privacy issues that are implicated. That's why we consulted with privacy experts both within the government and outside from day one. DHS included both its Privacy Office and our Office of Civil Rights and Civil Liberties in all REAL ID meetings and also included privacy experts from the government including the Department of Transportation in the development of the NPRM. We also met with and listened to the perspectives of the privacy community including some here in the room today. DHS held long listening sessions in the winter of 2005 with a variety of representatives from the

privacy community. DHS also had discussions with privacy experts in several key states as part of the development of the NPRM.

Let me address some of the primary privacy-related criticisms that we have heard to date. First, the REAL ID Act turns a driver's license into a national identification card. It does not. The NPRM establishes common standards for states to follow when they're issuing licenses that comply with the NPRM. The states, I think as you all know, have the right or the ability to issue non-compliant licenses and the NPRM has very little to say about those non-compliant licenses. Federal government is not issuing the licenses, it's not collecting information about license- holders, it is not requiring states to transmit information to the federal government that the government does not already have, such as a person's Social Security number. Most states already routinely collect the information required by the Act and the proposed regulations. This leads to another common and incorrect assertion that without a REAL ID license or identification card a person will not be able to get onto an airplane or into a federal facility. The NPRM does not require anyone to have a driver's license or a state-issued identification card or carry it with them at any moment of time. In addition, the NPRM does not limit the documents that can be used to board an airplane or enter a federal facility. By the way, this helps eviscerate the fantastical proposition I mentioned earlier that the government will somehow use REAL ID licenses to track a person's every move. Since no one is ever required to carry a REAL ID, it makes no sense that even if it wanted to, which it most certainly does not, the government would choose to track something that no one has to carry. What the NPRM does say is that if an individual seeks to use a driver's license or identification card for those official federal purposes specified in the NPRM, then that license or identification card must comply with the REAL ID Act in implementing regulations.

Third criticism is that the NPRM creates a national database of all drivers. Again, this is simply not accurate. As they do now, states will continue to maintain and store the data about drivers in their state. The NPRM does not require that this information be sent to the federal government or anywhere else to be stored or collected and does not give the federal government access to this information. What the NPRM does enable is the ability to query the information that is contained in the database as my colleague Selden Biggs will talk a little bit more about this. This really should not be a controversial proposition. My understanding is that such an arrangement takes place already in Canada and the Canadian Privacy Commissioner has fully authorized such activity.

Fourth criticism is that REAL ID increases the threat of identity theft because DMVs will have more information about individuals than they do now. DHS believes that the REAL ID NPRM is highly likely to lead to a decrease in overall identity theft since individuals will no longer be able easily to obtain identification documents in your name or alter genuine identification documents to fit their name of choice. I'm going to defer

further discussion on this point because I understand that Assistant Secretary Stewart Baker may address this issue in his remarks later today and that may be a better forum to concentrate on that issue. I should note that there was an article yesterday that North Carolina issued some 27,000 licenses where the Social Security number was either invalid or belonged to a deceased individual and that would not happen if our REAL ID NPRM regulations were in effect. A national problem requires a national response. Piecemeal approaches where one state improves its license issuance procedures a little, another state improves them a lot and yet another state delays action for a later date will not enhance our national security and permit those who profit from obtaining false identity to continue to do so. I'm sure that many of you may have comments or questions so I'll stop now, but I think it may make sense to hear from my colleague Selden about some of DHS's thinking about implementation issues relating to the NPRM before we open it up for discussion. Thank you

MR. BEALES: Thank you very much and I'm sure we will have a lot of questions, but people haven't started turning up their tents yet. But we do want to hear first from Selden Biggs who is here replacing Darrell Williams the Director of the REAL ID Program Office. Mr. Biggs is the Deputy Director of the REAL ID Program Office in the Office of Policy. He joined the department in December of 2005 and before that has two decades of experience in the private sector in software development and in systems analysis. He's also taught political science at Harvard University and the Universities of California and Montana. He's the co-author of a graduate textbook on the practice of American public policy- making which doesn't always go the way it says in textbooks, but thank you very much for being here today.

MR. BIGGS: Hello and thank you for the opportunity to speak. I'm representing Darrell Williams who is the Director today. He's on travel. I'd like to cover two topics today. First of all a brief overview of the REAL ID Program Office, what our charter is, and secondly a brief discussion of the data verification systems as presented in the NPRM. The REAL ID Program Office was stood up in December 2006. It's been located in the Office of the Secretary, the Office of Policy, specifically to focus the resources of the department upon REAL ID and its implementation. The idea is that following an 18-month or 2-year deployment of the program the actual administration of REAL ID will be moved to a component as a regular exercise. So we are really in the process of creating a program and implementation policy. Currently we have a staff of five on board, a program manager, a deputy program manager, two analysts. We have in addition a senior advisor from a state DMV with experience to help us work with the state DMVs to find out their situation, to help them transition to a REAL ID, and we also have additional staffing in progress. The goal of the office is fairly simple, to deploy REAL ID and to do this there are roughly four objectives we view in the near term. First is to support the completion of the REAL ID rulemaking process that's been involved with the publication

of the draft in March. Second is to issue standards or benchmarks to guide state compliance plans and implementation. We're beginning to do the research to flesh out the details of the rule and to help states progress step by step towards compliance. And we are soliciting comments on this from the states and from individuals, whatever information would help us to fill out the implementation. Third, we will be reviewing requests for extensions or compliance plans as they're submitted and certification packages in the future. Finally, our task is to support and expedite funding for technology initiatives and REAL ID implementation through department grants and other mechanisms such as may come about.

The schedule for REAL ID if you're familiar with the NPRM is roughly the following. Through October 1 of this year states have the opportunity to file for an extension to the May 11 deadline, May 11, 2008 deadline. Six months after these requests are approved, and these requests will be approved in almost all cases, states will be required to submit a compliance plan to detail their plan for implementing REAL ID and we will work very closely with the states to help them devise these plans and to evaluate these plans. In February 2008those states that seek to comply, in other words believe they are ready to comply with REAL ID will be submitting compliance packages as specified in the rule. On May 11 of 2008, the original target deadline for the statute, states that have not complied or have not filed for an extension will be - their citizens, those REAL IDs - their IDs may not be accepted at that point. Our target is to get the states that are close, and there are a number of states that are reasonably close to implementing the requirements of the statute, REAL ID- compliant as fast as we possibly can and to help them make progress. Finally on January 1, 2010, all states would need to be issuing REAL IDs and then by May 11, 2013, all states would need to comply with all requirements of the rule and the regulations. This is a phased process that allows states a variety of means to complete and we - our office has been set up to help those states work through this process.

Second topic would be the data verification systems involved with REAL ID. First of all, data verification is the process whereby the data that an applicant brings in is verified against reference databases. Data verification is not the sole verification process in checking someone who's bringing in - applying for a license. There are also two other processes. You have to authorize the document and there are methods available for that, testing to see if the document has been altered and also checking to see if the person holding the document is actually the subject of the document. That's authentication. And for instance everybody goes through authentication when you type in a password on a computer system. So data verification is just one of three pieces of the verification process and does not carry the whole weight, and the rule is very balanced in looking at all three processes and not focusing on one to the exclusion of the others. So when we talk about data systems we have to recognize that this is not the whole ball of wax, this is just one

part of a very complicated and complex set of procedures to help improve the security of licenses issued by the states.

The three components of data verification in the proposed rule are the following. First, data presented by the applicant, identified data items need to be verified against federally sponsored data verification systems. These systems are reference databases and when an individual brings in for instance a Social Security card with a number, that Social Security number and its associated data needs to be verified against a reference database to see if it's valid. As in the case that Jonathan talked about, this has proved - there are many instances in the states of invalid Social Security numbers and other kinds of fraud perpetrated. The rule identifies four different systems for data verification.

The first is a Social Security system. This has been up and running for years. Forty-seven states now verify this data already. The system is in place. There maybe some work that needs to be done, but by and large this system is operational as are the verification requests. The second system is the SAVE system run by the Department of Homeland Security. This verifies lawful presence and again, 20 states now send queries to SAVE. This system is already in place. Again, these systems do need work, they need improvement, but the system is in place. The third system is the EVVE system run by NAPHSIS. EVVE is a system for verifying birth certificates. The EVVE system is partially in place. There's a pilot in place, but again, and states need to join EVVE to implement EVVE and data needs to be cleaned up. But again, the EVVE system is in place, the system of queries is there, it's a known entity that people have been operating for now I think something like two or three years. And the final system is one that's yet to be built by the Department of State, but it's a method of verifying the data on passports. And to some extent this is quite easy because passports are coded so it's possible that a state DMV could simply slide a passport against one of the machines and verify it that way, or you could check the data on passports or other documents.

So the point is the federally sponsored systems by and large are there. They need development, they need work. It is the department's priority to - first priority to get these systems up and going to support the states. The second piece is what you might call middleware. It's how do you communicate with these systems. Again, the communications for most of these systems are already in place. States can directly access for instance the Social Security database or the SAVE database, but there's also a mechanism for what we call a federated querying service that would allow a DMV as part of its business process to access – to query all of these systems at one time. Parts of this system are already in place by DMVs who can send queries out to the Social Security Administration and other agencies. So the idea of a federal querying system - or federated, excuse me, is that this would enable states to do this more efficiently. This querying system however is an option for the states and it's a system that would be

governed by or set up through state-run agencies. The states would participate in this and by and large there are systems like this already in place and operating today. So we have models of how to proceed here. Again, the states have a choice whether to access directly as they do in some cases now or operate through this kind of system. Third is the state-to-state data exchange in the rule and this is the exchange of data among states, particularly state DMVs. The new requirement in the rule is quite simple. It simply asks that a state verifies with all other states that an individual applying for a license, a REAL ID license, does not have a REAL ID license in another state. This is a very small requirement compared to the existing requirements in the Department of Transportation systems for checking license applicants as they go through the process. There is an existing system of data exchange built up over decades involved and the requirement for REAL ID is really a very minor addition to the existing system. We are currently exploring alternatives on how to implement the data exchange requirement in REAL ID, but again it will be built upon or in relation to existing systems in place that do far more extensive data exchange among states. By and large REAL ID will not change the existing system established by DOT, it will simply add an additional requirement to check for REAL ID licenses.

The bottom line is that the REAL ID rule will not significantly change existing systems for querying federal databases. The only new system involved or query would be for passports and this could be done in the same manner as it's already done for other federal systems. And again, the states can choose how to communicate, how to query these systems. And secondly, the state data exchange will not change it significantly. The new requirement is in addition to existing system requirements for DOT systems and the department is actively exploring with DOT alternatives for implementing the requirement. And finally, it is the department's priority to make these systems available as soon as possible to expedite the verification process to make it easiest for the DMVs to verify the information some of which they already do verify, but to add the additional systems so state verification of driver data can be done quickly and effectively. Should we have any questions?

MR. BEALES: We have many questions.

MR. FRENKEL: If I may, let me just add one thing to elaborate on what Selden said. There's again an impression of wholesale data moving throughout the states and that's simply not the case. What you're really talking about are red light/green light systems, so one state, I'll just name a state, Georgia, cannot go into the Arizona DMV database and decide they want to look at all birth certificates that have been scanned into Arizona. What will happen in Georgia is if an individual walks in, is applying for a license and Georgia discovers that they have a license that - you know, they send out the query and it turns out they may have a license in Arizona, that they then get a notification

in essence that a license for this person may exist in Arizona and then they would follow up with Arizona. It's not - it's just, again there seems to be an impression that the data is searchable everywhere, every way, every how. I mean Selden was talking about passports. Passports similarly. It's not that the state DMV is going to get access to your passport file. If a person comes in with a passport as their identity document, they would send a query to the Department of State saying do you have this information in your database, yes/no. If the answer is no there could be a problem. If the answer is yes that's really the end of the exchange data. It's really a query system meant to sort of have a yes/no, green light/red light type answer and then if there are discrepancies that's when follow-up has to take place. But it's not that the State Department passport database now becomes open and widely searchable by DMVs. It's not even that one DMV's database becomes searchable by the other DMVs. So I just wanted to add that clarification to what - or elaboration to what Selden had said.

MR. BEALES: I appreciate that. We do have a number of questions. As you said we are interested in filing a comment on behalf of the committee and we have a subcommittee that is hard at work at that task and we're looking for more information today to facilitate that. If I could ask just a really narrow questions. How many of the driver's licenses today - I know all commercial licenses go through the DOT system. How many other licenses go through that system, or do we know?

MR. FRENKEL: I'm not aware that any do. There may be some. Actually, I don't know if - I guess Ms. McNabb has recused herself. I don't know if she would know the information or not. But there's certainly no requirement for any state to do that. And as a routine matter, when you're not applying for a commercial driver's license the states are not doing those queries. The only kind of information that goes between states, the only thing they're really searching is whether you appear on something called the National Driver Registry or NDR. There's also something called the Problem Driver Pointer System which is related and that's essentially to see if you have drunk driving convictions, whether your license has been revoked or suspended, but so I think they do run those queries on all drivers, but that's really the extent of any kind of routine query that is made by DMVs for non-commercial drivers.

MR. BEALES: Thank you. Lisa Sotto.

MS. SOTTO: Thank you Howard and thank you gentlemen very much for joining us. We've had really robust discussion among the subcommittee and I look forward to hearing our committee's questions to you. I'd like to just explore a narrow issue. You made the statement which makes a terrific sound byte, but I'd like to probe a little bit further that this will lead to a decrease in ID theft. It's a facile statement and it sounds really good, but it sounds to me as though what it will lead to is better verification and authentication of documents, but it doesn't sound like there's any move toward for

example preventing retailers from taking driver's licenses as IDs which - whose systems can be hacked and those driver's licenses sucked out, or - and you tell me. Is there a move toward increasing the security around the databases where the driver's licenses are maintained even within the DMV so that authorized users who can get access may in fact misuse the data. So I'd like to understand a little bit better the reduction in ID theft statement.

MR. FRENKEL: Sure. And again, I think Assistant Secretary Baker will talk a little more about that this afternoon, but really there are two primary ways and I think you've identified both of them and then I'll talk about the retailers after that. The first is it simply makes it harder to obtain false documentation. Right now it's extremely easy for those perpetrating identity theft to go get identity in your name or in anyone's name. And as you noted, what the NPRM and the REAL ID Act will do is it will make it measurably harder, not to say impossible. I'm sure there are ways to beat any system that people design, especially you know the one thing that's almost impossible to design around is corrupt insiders. You can have every law on the book, you can have all kinds of procedures and the best that really happens is those procedures catch people after they've done it. It doesn't necessarily mean they've stopped someone who's really committed to doing it. So it certainly - we're not saying that it eliminates for all time the ability to obtain a license under false pretenses, but it will make it extremely hard to do so because you simply just can't get multiple IDs in multiple states. I mean right now whatever state you're licensed in someone can get if they have the right identity documents for you, they can get a license in another state and now you have two Lisa de Sotto's out there, one who's the real person, one who's not. So that's how the REAL ID Act and NPRM are really tightened down on identity theft, the acquisition - false acquisition of identity. There is protection in the NPRM for the databases that the DMVs maintain in the whole data exchange between the states. Right now it's really left within the NPRM. This is certainly the subject I'm sure others can have different views on, but really call for a comprehensive security plan by the states including for them to detail what their data security is. So presumably there are differences in the states. So you could certainly imagine a scenario where the rule says no, here is the data security standard, you will all meet it. That's certainly a possibility. What that may inhibit, and again these are just sort of -certainly room for disagreement about and discussion, is whether if you do set that as a national standard and say point to that, whether that inhibits some states like California and I can't think of the other state off the top of my head right now who have gone a lot further with certain protections. So you might say well people - that will not just be the floor, that will be the ceiling and we're trying to give states flexibility so you can have states go beyond just the minimum standards. The retailer question is an excellent one. It's one - I know Barry Steinhardt's in the room and when there was a negotiated rulemaking committee before REAL ID was passed and repealed, the negotiated

rulemaking process, that was an issue Barry brought up and it's an excellent issue. We struggled with that a lot in our deliberations internally in the creation of the NPRM. The best we are able to do on that front, and we recognize that as you said there are certain - that it's a potential vulnerability for identity theft and privacy violations and elsewhere is to talk about encryption as a possibility. And the NPRM, the DHS says we essentially favor encrypting information on the licenses, but need to know what that effect will be on law enforcement. And we need to weigh that balance carefully. We don't know what that answer is and that's what we're hoping we will get good information during the public comment period so that when we make an evaluation for the final rule we'll really have the right information in front of us and can sort of make a decision about whether to encrypt, and if we're going to encrypt how much information to encrypt. But I mean those are the exactly right points that you're asking.

MR. BEALES: Richard Purcell.

MR. PURCELL: Thanks. So many questions, so little time, but I will leave it to my colleagues to help follow up on this. I'd like to ask one again narrow question and it has to do with the identifier itself, the license number. It's not clear to me in reading the regs or the proposed rules. Is there a standard format requirement for the license number itself? Today 56 jurisdictions, they all use different formatting, alphanumerics, lengths, different things. So first of all is there a standard format that has to be abided to by all 56jurisdictions in the format of the number itself, of the license ID and secondly, is that license ID to be unique? It is to be unique by the rules. Is it to be unique across all 56 jurisdictions or is it to be unique within each of the 56 jurisdictions only?

MR. FRENKEL: The answer to the first question is no. There's no intent in the rule to say there's one standard format for that unique identifier number. It's essentially a way for the state to be able to track its licenses to make sure that the state isn't inadvertently issuing license - the same license number, the same unique number to two people. So it's a way for if you would query the license and say we have license number ABC124, does that correspond to Lisa de Sotto in the State of Texas. Texas could say yes it does, or no that's not the number we issued to that person, there's a problem that needs further follow- up. So I think that also goes towards the second question. We're not anticipating a system like Social Security where you have a unique number for each individual. Assuming you know, if all 50 states wanted to issue a license ABC1234, as long as that's to a different individual that should be okay under the NPRM because the question isn't you know how do we find you anywhere, it's you know you should have, if the system works you will have one and only one valid driver's license. And when you present that driver's license and if it's validated against the state that issued it, if that doesn't correspond to the unique number used by that state there's a problem.

MR. BEALES: John Sabo. .

MR. SABO: Thank you. The point you made about flexibility. A lot of us in information security and privacy questioned why the proposed rule took the approach it did on baseline security. If you look at the Privacy Act, FISMA, Computer Security Act, even HSPD-12 and the FIPS, the Federal Information Processing Standards that flowed from that there's been a huge amount of work done by NIST and a huge thrust in the federal government to take the approach that security risks need to be mitigated and to build a framework for assessing the risks, identifying the controls and basically at least setting out minimum standards. And the comment that you're not trying to stifle innovation is a good one, but the whole federal government including the current work on implementing HSPD-12 for federal credentials is focused on a set of controls that have been vetted working with industry and expected to be implemented for federal employees and contractors. So I guess I'm just puzzled why the department, especially given the timeframe in which REAL ID needs to be implemented, why the department chose to basically say well, we're leaning towards encryption, but it might be hard to implement and so we won't mandate that, or we don't want to set at least baseline controls. So you know. Could you just explain the rationale, especially given the timeframe, for not utilizing at least in a proposed rule baseline security recommendations that all the states would follow. And one reason I say that is because if you look to each state to have different levels of security controls without a common baseline standard at a minimum it just seems to me as a security professional you're exposing the whole program to a weakness for attack by a determined adversary. It isn't mom and pop and the kid trying to skirt getting a driver's license without the REAL ID license. The whole purpose of this was to assist us in protecting homeland security from terrorists. The determined adversary will look for the weak link. So I guess it's a long diatribe, but I'd like you to at least indicate why you chose that approach, especially given the work that's already in place for minimum security controls.

MR. FRENKEL: Sure and we certainly considered that. I mean, we're certainly aware of that and thought about whether we should prescribe security standards or not nationally. That was one area where again the decision was made. I'm sure you will hear from David Quam in the next panel about how much of this is you know the federal government telling you this is what you have to do, this is what you have to do, this is what you have to do. That was an area where again you've certainly raised a good point, but it was one where we wanted to see let's see what the states have. Now it doesn't mean by seeing what the states have that the requirement that submit a comprehensive security plan means that we just sort of check the box and say okay, we received the plan now we're done. If we see that there are gaps, then that would be something you could work on with the state. But that's also not to say that in the final rule we wouldn't consider having a national standard. I mean part of the disability we were working under is we're not - the Department of Homeland Security is not experts in Department of Motor

Vehicles. So we didn't have - it's not that we knew exactly what every state was doing. Right now we could say, you know what, we think 46 states are already there, very, very close to this standard. We think if you impose this standard that's something that states won't be able to meet within a realistic timeframe. So you know we went with the method that we've proceeded, but again that doesn't mean in the final rule we wouldn't use those kinds of established standards, but that was the choice that was made for the NPRM. .

MR. BEALES: Tom Boyd.

MR. BOYD: Mr. Frenkel, I appreciate that the wisdom of the REAL ID Act or lack thereof depending on what point of view is really not within your capacity to address at this point, but I am curious about the cost on the states and other jurisdictions on this legislation. The range that I've seen in the materials is from $11 billion to $23 billion which I assume to be in 2007 dollars and the National Conference on State Legislatures in its testimony indicates that they think it should extend another eight years before compliance is possible. Of course those are in inflated dollars. So can you give me a sense as precise as you can what the cost is going to be in real dollars, (a), and (b), in addition to some future potential federal funding which may assist, how are the states supposed to raise these funds?

MR. FRENKEL: Yes and let me say unfortunately I wasn't the one involved in doing the cost analysis. I'm not able to sort of give you necessarily precise I think the cost is this.

MR. BOYD: Is there someone who can?

MR. FRENKEL: Presumably our economists who worked on it would be able to give you a better –

MR. BOYD: Could you provide that?

MR. FRENKEL: - different discount rates and things like that.

MR. BOYD: Could you provide that please?

MR. FRENKEL: I think there is in the NPRM there's –

MR. BOYD: Twenty-three billion.

MR. FRENKEL: No, right, but I mean there's a whole economic analysis that's laid out which is some I think 150 pages or so. So that really represents the economic analysis that the department did. Now remember that even those costs are not necessarily accurate because what those costs are primarily based on was a survey that AAMVA did of the states and information that the states provided to AAMVA. So those costs may or may not be inflated. They may not - they may be underrepresented. It's just hard to

know. As we've gone around the country a little bit after the NPRM you hear states saying they can do it for a lot less than some of the numbers that have been reflected. I think what the Secretary said in his announcement on March 1 is that when you- the expectation is, and again I can't tell you this is real dollars, how inflation has been accounted for, but the estimate is that about $20 per additional license would be the cost, the additional cost imposed by REAL ID to the states.

MR. BOYD: And how much does that add up to?

MR. FRENKEL: I mean you have 240 million license-holders approximately, 240 - 250 million, so if you do that times $20. MR. BOYD: And how would the states be expected to raise these funds?

MR. FRENKEL: Again that's one of those things where we've always said that this is a joint responsibility and that Congress has responsibility in this area too. I think for those of you who have read the Act and are familiar with it you know that Congress appropriated such sums as - I'm sorry, authorized such sums as would be necessary and then appropriated $40 million for grants.

MR. BOYD: Well that $40 million is just startup, isn't it?

MR. FRENKEL: That's right, that's right. It's clear - well I mean that was all Congress appropriated.

MR. BOYD: Right.

MR. FRENKEL: So you'd have to you know - if you're able to penetrate better the congressional thinking, but right it was basically grant funds to the states. So you know I think at this point it's fairly clear that $40 million is not a sufficient amount of money for the states to be able to implement. It is certainly a question of discussion how much of the cost should be borne by the federal government, how much of the cost should be borne by the states. I think it's certainly the department's view that it is a shared responsibility and the department does not believe that 100 percent of the cost of REAL ID implementation should be borne by the federal government.

MR. BOYD: How much of the time that you allow for implementation will be - will hinge on whether Congress provides appropriations? In other words you're making it a mandate that requires expenditures of funds based on shared funding responsibility in the future which may or may not materialize in the necessary levels, and so to what extent will that become a factor in allowing states to have more time to bring themselves into.

MR. FRENKEL: Within the rulemaking proceeding it probably will not be a significant factor.

MR. BOYD: Okay, thank you.

MR. BEALES: Mr. Frenkel, thank you very much for being with us today. I know we all have a lot more questions, but we also have another panel that we want to hear from. I hope we could ask you if we could follow up either with written questions or with an inquiry from the subcommittee as we try to understand better sort of where we are in the rulemaking in order that our comments might be as informed as possible. If we can - then we'll sort of figure out at the end of our meeting I suspect what's the most effective way for us to follow up. If we could do that we'd really appreciate it because this has been a very helpful session I think. All right, thank you very much.

Our next panel is Outside Perspectives on REAL ID. What I want to do is to introduce the speakers in turn. Each of the speakers has five minutes to make a statement and then what I want to do for the committee is after all of the speakers have made their statement then save our questions until the conclusion because that will allow us to get different perspectives on a particular question from different members of the panel. Our first speaker will be David Quam who's the Director of the Office of Federal Relations of the National Governors Association. He leads the association's legal and advocacy processes and analyzes what the federal government is doing to the states on various issues. He works closely with governors' representatives here in Washington and also with the NGA's standing committees on their legislative priorities. Before joining the NGA he was the Director of International Affairs and general counsel of the International Anti-Counterfeiting Coalition and he was the majority counsel for the U.S. Senate Subcommittee on the Constitution, Federalism and Property Rights for the Committee on the Judiciary. Welcome Mr. Quam and you have five minutes.

MR. QUAM: It's a pleasure to be here and to address you today and talk about an issue that really is a priority for governors and has been for some time. Let me point out a few things to start with. There is no governor who is not for increasing the security and integrity of the driver's license processes. Every governor is a security governor and several states were in the process post-9/11 of already improving these systems when the discussions started at the federal level. It is ironic and unfortunate that really we had this issue solved with the negotiated rulemaking first time around with the Intelligence Reform Act. I believe if that process and the negotiated rulemaking that was involving states had been allowed to go ahead we'd be done. We'd be done right now because the stakeholders would have weighed in, you'd have states invested in this process and we could have come up with some national solutions to what really - driver's license has been a state issue for well over a hundred years. That's not where we are. Instead we have REAL ID. REAL ID poses a real problem for states and it has been an increasing problem as states have been waiting for the regulations because the regulations really - the devil's in the details when it comes to these very complex systems. I think as you all recognized and as the speakers already indicated this is not an easy problem to solve. Fifty-five different state and territorial systems governing 245 million driver's license and ID cards.

This is not going to be easily solved in the near term. Because of that governors have taken a stance that is let's mend it. We don't have to end it, let's just fix it to make sure it works because only if we have a system that works can the states implement and can we move forward and get this done.

We've set forth several recommendations that came out in a report in September attempting to estimate the cost based on the information we had. The cost estimates to the states at that point in time was over $11 billion over five years to implement. I think a lot of those numbers were both used by DHS but also reflected in the cost estimates that are in the regulations that were just released. The three areas where our recommendations are most pertinent - well, they fall into these categories. Number one, you've got to give states enough time to do this. These are complex systems, they're going to rely on databases that do not currently exist. A couple of them exist, but they have to be enhanced. That's going to take time to both build them, to populate them with data, to secure that data and have a governance system to make sure they're going to work. So the states are going to need time. Number two, the states are going to need money. I think the questions that were asked are absolutely pertinent. There is no meaningful federal funding for REAL ID at this point in time. The only way you can evaluate both the regulations and the statements that we've heard thus far is that this is going to have be a fee-based system moving forward to pay for REAL ID. That is going to be a problem for citizens as the cost of these cards and the cost of driver's licenses go up. Lastly, flexibility. Because you have several different systems, it is not a national system, different states have different requirements and they need the flexibility to build off their legacy systems to get to a point that makes sense to meet REAL ID. That's going to require different states to take different steps in the process. I think you heard DHS say that some states are close. That's absolutely true when it comes to the card and the driver's license itself because a lot of states were already doing that work. It is unfortunate that with REAL ID some states had to stop their improvement programs in anticipation of these regulations coming out because why make major investments if changes are going to have to be made. That being said, most states were already in the process of approving these. I think several states are close with regard to their own card and their own state systems, but the question really is the national systems. I will say this. Until the regulations came out, the states really had no clear sense of whether all the recommendations and several had been made by NGA, NCSL, the Conference of State Legislatures, and AAMVA, the Motor Vehicle Association, working together as the primary stakeholders. Hundreds of recommendations were made to DHS. It was unclear as to whether all of that information had been heard until the regulations came out. I will give DHS its due in that some of the flexibilities in the regulations suggest a real understanding of how complex this is and the role the states are going to have to play in solving it. I am perplexed, however, that recognition of those flexibilities and those complexities is not then mirrored completely in

an extension of time. I think the timeframes that have been laid out frankly remain unrealistic and the funding issue overlays all of it because without the money ultimately I think - I heard a congressman yesterday say you know a mandate without funding is a hallucination. And that could be where we're at.

I know this committee is also very much concerned with privacy and I think that is a 900-pound gorilla when it comes to this particular issue. REAL ID would be driven, whether it can be successful and whether it can be implemented by the states in a meaningful way will depend on the existence and workability of the electronic systems. Those systems have to be up and running and manageable and protected if citizens are going to buy into this system, trust it and states are going to be able to make it work. My reading of the regulations, and again I think a lot of different groups both at this table and around the country are going to weigh in with regard to the privacy angle, is that states have taken several steps within their states and state laws to protect privacy. Those should be allowed to apply. But we are going to have to work out those governance and conflicts of law issues moving forward. Federal government has some protections in place. The way the systems are built can provide additional protection. The privacy is a very real concern. At this point in reading the regulations if I had to characterize where we currently stand on privacy it's kind of like an NFL team who's had trouble moving the ball all game and you get down and it's third and 1 and you decide whether to go for it and ultimately you do what we're really good at in Washington, D.C. and that is punt. Punt it to the states, the states will solve it. I am concerned that there are assumptions made within the regs that these systems will exist in the timeframes that are provided. I think it's unrealistic. Time will tell. NGA will be asking Congress for assistance both with funding, but also with changes to the statute. This is a tough statute to implement. The regulations reflect a true effort on behalf of DHS to listen to the states and try to meet some of those requirements, but a lot of work remains to be done. I'd be happy to take questions as we move forward. .

MR. BEALES: All right, I'm sure we will have them. Thank you very much. Our next speaker will be Barry Steinhardt who's the Director of the Technology and Civil Liberty program at the ACLU. He served as the Associate Director of ACLU between '92 and 2002 when he became the inaugural Director of the Program on Technology and Liberty. He was chair of the 2003 Computer Freedom and Privacy Conference and is a cofounder of the Global Internet Liberty Campaign which is the first international coalition that's concerned with rights of internet users to privacy and free expression. He's the member of an advisory committee on the U.S. Census and on the Blue Ribbon Panel on Genetics of the National Conference of State Legislatures and he was a member of the U.S. delegation to the G8 Tokyo Conference on Cybercrime. Mr. Steinhardt, thank you for being with us.

MR. STEINHARDT: Thank you for the opportunity to be here today. Actually let me add one thing to the brief bio that you read and Jonathan Frenkel mentioned it which is that I also was a member of the ill-fated negotiated rulemaking process that was set up by the Congress on driver's licenses. And I say that both to tell you that I've been in the weeds on this one as many of us have been, looking at many of the details, but also to tell you that that was a process that made sense. You had all the stakeholders in the room, National Governors Association, National Conference of State Legislatures, AAMVA, privacy advocates, domestic violence - people concerned about domestic violence issues, law enforcement, judges, and if we learned anything I think during that process it's that this is dauntingly complex and it can - and this is not a problem that could have been solved by the kind of statute which in fact the Congress passed which DHS - and I give them credit here for attempting both to comply with the statute and deal with all the complexities here which DHS through the regulations is attempting to implement now and I think has probably done a fairly good job of implementing the statute. What they haven't done is a good job of building a national driver's license system that protects privacy, that enhances security, that is affordable to the states, all things that it needs to be.

In preparation for this testimony we distributed three documents to this committee. The first is what we're calling the REAL ID scorecard. This is a section- by-section analysis of the Department of Homeland Security's proposed regulations and which we've attempted to assign a score looking at pass, fail, or incomplete on a variety of issues, not just privacy issues but issues of cost and states' capability to actually implement. In our scorecard we found DHS got about a 9 percent out of a possible 100 in meeting the various concerns that have been raised by the various stakeholders here. Again I say that without being too critical of DHS. I'm not sure this is their fault. They've been attempting to implement a very difficult statute.

The second thing that we gave you is a map that shows the activity in state legislatures across the country on REAL ID. And the remarkable thing about this map if you look at it, and we've color-coded it, is that this is not the blue and red map that we're all familiar with from elections of Republicans and Democrats. This is a map that shows that literally across the country, from Maine to Washington State, state legislatures have passed resolutions or statutes either in one house, in a couple of the states now in both houses so that their actions are complete, asking that REAL ID either be repealed or revisited. What it reflects is a firestorm really that exists across the states at the grassroots level among state legislatures reflecting an acknowledgment and a notion that this statute cannot be implemented. It fails all the tests, both privacy, security, do ability. Remarkably since we've distributed the documents to the committee at the beginning of the week there have been actions now in four states which were not reflected on the original map, Oklahoma, Missouri, Arkansas and New Hampshire. And that reflects the

fact that this is - that this movement is accelerating across the country. In fact it has been accelerating since the regulations came out. You also see the third document that we gave you which is a list of those states that have acted since the regulations came out, since March 1. And this reflects that the rebellion is both growing and accelerating.

So I understand from the original comments today that the committee intends to file comments in response to the NPRM and I applaud you for that. I would urge you to give DHS one piece of advice that I think makes the most sense here. REAL ID is a real nightmare. It cannot be implemented in a manner that protects privacy which I know is something that is your primary concern. It's unworkable, it's unaffordable. DHS should be supporting efforts that are now ongoing in both houses of Congress to revisit and reform the law. We can have a more robust driver's license system. I say that as someone who did serve on the negotiated rulemaking and I think Jonathan Frenkel will be the first to tell you that even though those of us who came from the quote 'privacy community' unquote went in with a good faith belief that the driver's license system could be made more secure, more robust, but at the same time we could protect privacy. You can't do it under the REAL ID statute. Simply not possible.

I want to highlight one or two items with respect to privacy issues and the REAL ID scorecard which we distributed to the committee and which is available - will be available here on the desk for anyone who'd like to look at it goes through a whole series of issues, many of which are probably not the direct concern of this group. But I want to highlight a couple of issues that were mentioned earlier. One is this question of whether or not REAL ID is in fact going to become a national identification card. The reality here is that REAL ID will become a de facto national ID card. We're talking about a driver's license that will be held by the vast majority of adult Americans, in fact the vast majority of Americans over the age of 16. It will be backed up by a distribute database and whether or not that database sits in Washington in one big database or whether or not you have a database which is 50 or 56 separate databases across the nation, but everyone can query it, it's effectively one database. The computer professionals on the committee and in this room know that in reality. And most significantly there is this machine-readable zone to be placed on this national driver's license, on this REAL ID card. As Jonathan Frenkel said, we urged very strongly that the machine-readable zone be encrypted. DHS has punted on that issue. Not clear to me why they punted on that issue, it seems to me so clear that it should have been encrypted. The result is that everyone out there, particularly in the private sector if it is not encrypted is going to be reading that machine-readable zone, is going to be harvesting the information and it's all the information in the system, the front of the license and it's much of the information that sits in these databases that there have been a lot of discussions this morning about protecting, going to harvest it and it's going to duplicate it. The fact is that the information is going to be harvested by every retailer you go to and every retailer is going to want it. Every bank, every 7-

Eleven, every airline, everybody's going to want it. They're going to sell it off for pennies on the dollar, that information, to data warehouses and data aggregators like the ChoicePoints of the world and they're going to recreate it. And all the effort that has gone in on the part of the states and the federal government to protect the privacy of driver's license information as embodied in the Drivers Personal Privacy Act will go, will simply vanish. All that effort will go for naught because the private sector will be capable and certainly will create a parallel database to the database that now exists in the 56 jurisdictions. So thank you and I'm happy to answer any specific questions, but I want to make this point again that I think that this committee could be doing the country a great service and everyone a great service by recommending to the Department of Homeland Security that they support efforts to modify the Act. Thank you. .

MR. BEALES: Thank you Mr. Steinhardt. Our next speaker will be Anne Collins who's the Registrar of Motor Vehicles for the Commonwealth of Massachusetts. She was appointed by Governor Mitt Romney. In her job she sets policy and leads an agency of over 800 employees with 39 offices. In Fiscal Year 06 they served 3.6 million customers in branches with an average wait time of 10 minutes. They served 1.2 million customers over the telephone and 4 million on a website. The Registrar of Motor Vehicles collects over $1.2 billion annually in revenue and has an operating budget of $57 million. Before becoming Registrar Anne was the Director of Professional Licensing for Massachusetts, licensing over 500,000 licensings in more than 40 professions ranging from architects to veterinarians and I guess there's not a Z profession that gets licensed.

MS. COLLINS: Exactly right. We went for the zoologists, but we were rebuffed. Thank you so much for having me here today. I think one of the best outcomes of the REAL ID Act is actually some focus on practices within the motor vehicle community and the work that is done there. Aside from being the butt of everybody's jokes, now people are actually coming to realize the complexity of the operations of issuing the driver's license and IDs. I'm going to speak from my prepared remarks because I really want to focus on the issues that you are directly dealing with on privacy. At the outset I also want to clarify that my comments here today are not intended to express a commitment by Massachusetts to comply with the REAL ID Act. In fact, like many states we are actively engaged in a thorough cost-benefit analysis ourselves to look at whether the incremental increases in security and safety of our citizens can be balanced against the tremendous costs and complexity associated with implementing this law.

Second, while I really appreciate the lens of privacy being applied to the REAL ID Act and indeed to the practices of the motor vehicle agencies today before the REAL ID Act, I really want to temper that with the notion that you can have tremendous policies, but without an eye towards efficiency those policies will be quickly given short shrift. The continuing pressures on motor vehicle agencies to do more with less is creating an

untenable situation for implementing even the current privacy protection laws as front-line employees are called upon to do more and more with less and less resources. If the operational considerations on the cost are not specifically addressed, I love the line about the hallucination, but we're really talking about when you put together systems in too short a timeframe, the systems will be under-designed, the staff will be under- trained and the execution of the protections will be directly at risk by having too few people doing too much. Each element of the program is only as important and reliable as the resources that are dedicated to carrying it out. If I were to declare a theme for my remarks today it would be to co-opt the theme of my favorite movie the Field of Dreams. If you build it, they will come. So both the title of the movie and the reference of its main theme are directly relevant to the REAL ID Act. It is just the absolute truth that each system that is designed expands. As the system becomes a reality, the uses for that system expand. Just look at the driver's license itself. At one point it was actually evidence that someone knew how to drive. In Massachusetts right now we are trading off things like the technology to give the learner's permit exam and the funding for giving the road test exam because we are busy spending resources on the identity side of the house. I can get funding for things like a biometric in a facial recognitionanti-fraud device, but I cannot get funding for the technology to administer the license exams themselves. You build it, they will come.

So whatever the intended implementation of the REAL ID Act and any assessment of the individual vulnerability that is included in it, you've got to quickly look at the fact that over time it will change. The best privacy that we can come up with now will be built into the program, but over time that will change. You look at the Social Security card, you look at the driver's license, any other system, over time our priorities change from privacy to security to efficiency.

My background was given and I wanted to highlight just the fact that this is a constant tension in government. We're constantly balancing the public purpose with the respect for the individual needs. And when you get that balance right you have support and programs that work, but as you go along if you've got that out of balance, and I think this is what the prior speaker was addressing, you have accelerated withdrawal from the process. And that is something that has got to be borne in mind or we will produce a situation where the lack of universal compliance actually produces something that is of less value than what we have today. Specifically one element that I just learned of on Monday is that in the final or the draft of the proposed rulemaking, one of the elements that has been a prime focus and frankly one of the elements that adds the most value for the REAL ID Act was something called the one driver-one record. That's the notion that your driving record should follow you wherever you go. So if you move from state to state, you will actually be accountable for your driving behavior. This is - and to answer one of the questions that was raised too Mr. Frenkel, this is one of the ways in which identity theft can in fact be prevented by virtue of - the number one committers of identity

theft or identity fraud in the driver's licensing business are drunk drivers and people looking to avoid accountability for their child support payments. Both of these things are policed by the driver licensing department. When we implemented facial recognition in Massachusetts those were the number one and two number of people who were trying to get a different identity. They're trying to avoid the consequences of their past behavior. Not to commit identity theft and go off and steal money, to avoid the consequences of their behavior. In the regulation as it was put out in the notice of proposed rulemaking, we are now no longer looking at a one driver-one record system. That piece of it has been lost and what I suggest will now result is a doubling of cards, identity cards and driver's licenses that are out there because states like Massachusetts will be looking at a way in which we can become compliant with a REAL ID and the requirements are so onerous as to the fact that we're going to have to offer a two-tiered system, those people who can't find their original birth certificate, who don't want to pay extra to come in to change their address in person for example will choose to have the lesser standard driver's license. And the complexity that will ensue by creating a two-tiered system in multiple states will I suggest really increase the threat of homeland security rather than decrease it. So there needs to be a very practical approach to what can be done by the states in order for this to add any value at all.

In Massachusetts one of the values that we have been able to add, I think I would stake our 10-minute wait times up against any of my fellow jurisdictions. And I think one of the ways we've been able to do that is by diversifying our points of doing business. Like many other businesses we're looking at developing natural systems. Meet the customer where they are, provide the service that they want where they are. So if for example you buy a car in Massachusetts, you get your plates - you register your vehicle at the car dealership. If you're buying insurance and because you've moved you've changed your address, your insurance agent can do that. This creates over 600 private business partners that have access to our data. We have not had major breaches of privacy with that data. We have an auditable system. We require Driver Privacy Protection Act training for anybody who uses our data. But we will face really serious changes in our business practice if we have to pull back from our vehicle titling and vehicle registration programs because of the REAL ID Act's limiting access to data.

I wanted to speak specifically to some of the principles of privacy that were - are championed by the states now and are championed to DHS, will be in our comments, and again notice that there needs to be a tempering in the expectations. We can't simply blindly assume that because we have a stated principle that that will be what ends up in the actual execution of the policies. The notion of openness, that everyone should know what information is being collected, why and how it will be used is certainly appropriate, but as a practical matter unless you are prepared to live without a driver's license or state-issued identification card it is almost impossible for that notice to have any real value. The

individual simply can't act upon it. They need the license so they will surrender the information. This is not new because of the REAL ID Act, this is the practical reality of driver's licenses today. The principles of restricting collection and disclosure of data to that limited to the official need and the stated purpose, also very worthwhile. In this case the ability to use the principle to maximize individual privacy requires on the smallest possible systems to store the information and the exchange of the least amount of data possible to complete the necessary validation. For example, there has been much discussion about the use of pointer systems to meet the needs of the REAL ID Act. Such systems rely on data stored by the issuing agency or the state. This helps compartmentalize information, a natural protection. However, the pointer systems must also exchange sufficient data to minimize the problems associated with false matches. False matches are highly disruptive to customers and frequently cause customers the anxiety of believing that their identity has been stolen when in fact they have simply been wrongly identified. Neither is comforting, but the misidentification is more easily resolved. This is a difficult tension to resolve, exchanging enough but not too much. The current systems that have been spoken to in terms of the states like Massachusetts that have long used the Social Security online verification system and CDLIS, the Commercial Driver Licensing Information System, and a reference was also made to the Problem Driver Pointer System. The number one problem that we face is false positive matches and these are relatively small systems. When we go to a245 million person match and you're matching things, the full legal name which was never designed into any of these systems, you're just asking for trouble. Each of these agencies that are participating, every state and every federal agency as well as the networking agencies have to be prepared to keep these systems up and online while customers are standing in front of front-line clerks. They need to be staffed with ombudsmen offices to be able to respond to the false matches and to allowing the customers to correct the data. Right now in Massachusetts one of our other most frequent problem is someone who has a parking ticket. They get a parking ticket in a city or town and they find out about it when they're at the registry because they forgot, they didn't pay it, you know, Junior had the car and they may owe that ticket to - on New Year's Eve day I worked at the branch counter myself and I had a nice guy who drove up from New York to renew his driver's license only to find out that he owed a parking ticket in Provincetown from the previous summer. When he can't solve that problem in my branch because he can't pay me the parking ticket, the cities and towns want that themselves, he’s stuck there. He's stuck there in my face, he’s angry, he's upset and we have no solution. What we're doing here is pouring gasoline on the public and saying to them in the Registry of Motor Vehicles offices, the motor vehicle offices throughout the country we're going to just sit there and wait for a match to be lit because we are asking for millions of people to face situations that they cannot resolve in that motor vehicle office. You can't change your Social Security name or address of record in my office. And without giving me the tools to make those changes you're giving me the

opportunity of confronting customers with problems and no ability to solve them. Limiting access to the current stated -.

MR. BEALES: Ms. Collins, if I could ask you to just wrap up because we do have –

MS. COLLINS: I'm sorry.

MR. BEALES: I would love to have more time, but we don't.

MS. COLLINS: The if you build it they will come issue is really the other you know gargantuan issue that we're facing. We're already seeing in side comments, in jargon people saying oh well, you know, how soon can we troll that data. In conversations that I've heard - the Department of Homeland Security there is a very definite, real and intended use to expand access to state records. I think that where there's a given law enforcement threat there is already access to that, but I think that there really needs to be expressed tempering on what the desired uses of this information are going forward. Thank you for your time.

MR. BEALES: Thank you very much. Our next speaker will be Sophia Cope who's a staff attorney and Plessor Fellow at the Center for Democracy and Technology. Ms. Cope works on internet free expression and the privacy implications of government ID programs, also RFID and the Fourth Amendment's application in the digital age. She received her BS from Santa Clara University and her JD from the University of California's Hastings College of Law. Ms.Cope, welcome.

MS. COPE: Thank you very much and God bless you for saying that last bit because I am going to actually address that. So on behalf of CDT thank you committee for inviting me here today to speak. I'm actually going to echo a lot of what Barry said. I think we didn't want to have too much overlap so that we provided you with a broad range of meaningful input, but the fact is that the Act and the NPRM sort of unavoidably elicit the same response I think from the privacy community.

As Barry said we believe that the Act as it is now is unimplementable. There of course are the costs and practical considerations to consider, but really the privacy and the security concerns really are incredibly enormous and we believe that the Congress must go back and revisit this Act. As Barry said, I echo what Barry said. CDT encourages this committee to give recommendations to the Secretary of Homeland Security to in turn give recommendations to Congress about how they can amend this Act. And of course we also encourage this committee to give DHS recommendations about how they can improve the regulations assuming that the Act doesn't change.

CDT believes that the issues surrounding REAL ID really fall into two broad categories and we really think that this distinction is very, very important. The first set of issues revolves around making the driver's license or identification card issuance process more secure, so that way it is more reliable. This includes verifying that a person is who

he or she says he or she is, that he is providing accurate and up-to-date information, that the information and supplies used to create driver's license or ID cards are strictly controlled and of course that the cards themselves are resistant to tampering and counterfeiting. These sets of issues really are not that controversial. Again there are costs and practical considerations to keep in mind, but really we feel like this was the intent of both the 9/11 Commission and to some extent the former Congress when they passed the Act, that these issues were at the core of the concern.

And I want to make a point to piggyback what Barry was saying. A lot of privacy advocates have been talking about repeal. One thing that we want to emphasize is that we're just not talking about repeal to repeal and that's it. Barry was on the original negotiated rulemaking committee. There is a concern, or there's a respect in the privacy community and a recognition that there are ways to make the driver's license and ID card issuance process more secure and more reliable. So when you hear about repeal in the media or whatnot, it's not just repeal and nothing. It's repeal and let's do this thing right. And CDT has been supportive of the bills that are in Congress now that really try to go back to the beginning and really do this thing right.

The second set of issues which have been more controversial in our mind go far beyond what is necessary to make the driver's license or ID card issuance process more secure and more reliable. These set of issues revolve around two main provisions in the Act again that Barry mentioned which is the electronic access provision which requires that all states give every other state electronic access to the information in their motor vehicle databases. Now I know that Mr. Frenkel said that there's - the intent of DHS is not to allow the sort of open, widespread data-searching, but the fact is that the Act has this broad language and the NPRM is in our opinion frankly has been - is quite vague as to how that's going to happen. The other provision in the Act is the machine-readable zone and the requirement each card be able to be digitally read and contain a significant amount of personal information.

These provisions together in our mind do create a national identification system. Now it's not a national ID card that people are required to carry with them wherever they go. It's not a 'Papers, please' situation, but it is a nationalized identification system. We must call a spade a spade and be honest about the implications of the infrastructure that we are creating here. These provisions of the Act and how DHS has chosen to interpret them, the intent is to create a one person-one card-one record system and these provisions call for greater collection, centralization and sharing of highly sensitive personal information. This includes the copying of source documents such as birth certificates, Social Security cards, passports, even your utility bill. And there are absolutely no statutory and for that matter regulatory limitations on what information can be collected, what information can be accessed, by whom, like for example for other government

agencies beyond DMVs, third party businesses, that was already brought up, and of course for what purposes. CDT's perspective is that there needs to be statutory limitations and to the extent that Congress fails to act very clear regulatory limitations that personal information both the databases and the machine-readable zones are limited to DMV officials of the issuing states for legitimate DMV purposes and of course to law enforcement officials for law enforcement purposes consistent with the existing law.

And it should go without saying, but CDT's perspective is that the greater collection, centralization and sharing of personal information, particularly without clear statutory or regulatory controls, actually does create greater risk for abuse by government, businesses, but also criminals, ID thieves, terrorists and whatnot. There has been talk about the DHS regulations basically punting to the states. CDT completely agrees with that and calls - the NPRM simply calls for each state as part of their certification process to have a privacy policy that follows the Fair Information Principles, but beyond that DHS provides absolutely no standards, how - CDT, we want to know how are states supposed to get certified. Against what specific, clear, objective criteria, how are their privacy policies going to be certified by DHS. And that goes for the security policies too. They're supposed to have this comprehensive security plan, but there are absolutely no clear, specific, objective criteria or standards against which state security plans are supposed to be certified. In our mind this is going to create 56 different privacy policies and 56 different security policies and that system is going to have a weak link somewhere undoubtedly.

So again on behalf of CDT I want to emphasize that we encourage this committee to give recommendations to the Secretary to in turn give recommendations to Congress about how this Act cannot just be repealed and nothing, but actually how the driver's license and ID card system can be meaningfully reformed. And then again to the extent that Congress fails to act, there are ways that DHS can significantly improve the proposed regulations. And I will provide this committee with written testimony probably later today. So again thank you for the opportunity to speak.

MR. BEALES: Thank you very much and we'll look forward to the written statement. Our next speaker is Melissa Ngo who is staff counsel and Director of Identification and Surveillance Project at the Electronic Privacy Information Center. Ms. Ngo focuses on federal and state identification proposals including REAL ID and their impacts on citizens and immigrant communities. In addition her work includes Spotlight on Surveillance, a monthly evaluation of federal and state surveillance programs. She worked previously as a journalist at USAToday.com and the Washington Post and she continues to examine First Amendment issues. Ms. Ngo, welcome.

MS. NGO: Thank you for having me here today. I actually have prepared written statements I have submitted to the committee and they're available at the back of the

room as well, but I'd like to take this opportunity to respond to some previous testimony. Some of my panelists have already responded, but I really need to reiterate that it is not ridiculous to say that REAL ID will create a national identification system that will allow people to be tracked. REAL ID is ostensibly voluntary, but that just isn't true. The ubiquity of driver's licenses and state ID cards, 245 million IDs and licenses across the nation, the federal purposes, plus the regulations contemplate a universal design. This means that people without REAL ID cards will be easily found. This means that they will be looked upon with suspicion. We already see that states that have rejected REAL ID implementation, states that are criticizing REAL ID and others who are criticizing REAL ID have been labeled as anti-security. It is not anti- security to reject a national identification system that does not add to our security protections.

The technology considered in the regulations will allow for clandestine tracking of individuals. The unencrypted machine-readable zone, we have already heard of the many uses that can be made of that. The fact that there is long-range RFID technology contemplated in the regulations. This takes control of a person's personal information away from the individual and gives it to whoever can grab this information. Now the regulations and Secretary Chertoff have contemplated expanding REAL ID to the point where it will do, quote, 'double or triple-duty.' This expands the use of the card and access to the state records. One centralized system does not create a secure system. Several layers of security, several identification cards set out for specific purposes will increase security. Now, if you want more security it is just common sense to have several different cards such as you have several different keys, your house, your car, your safe deposit box. All of those are not opened by one single universal key and there should not be one single universal card to create security for the nation because it just will not. Mr. Frenkel admitted that it will be possible to circumvent the REAL ID system. This does not increase security, it makes it easier for identification theft and easier for terrorists and other attackers because they only need to forge and break the security of one card. Now, the theory that the REAL ID Act will prevent terrorism is predicated on the belief that only outsiders have an intent to harm the United States. Bruce Schneier, security expert and member of the EPIC Board of Directors has explained this misconception. In theory 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 evil-doer. This is impossible because you cannot predict intent based on identification. There are threats from both sides. Terrorist acts have been committed by U.S. citizens. You need only look at Oklahoma City bomber Timothy McVeigh and the Unabomber Ted Kaczynski. Even though standards for employee background checks are set out in the proposed regulations, this does not solve the insider attack problem because there are insiders without previous ties to criminal activity. A recent case illustrates this point. According to court documents, a few weeks ago in Florida two men entered restricted areas, bypassed security screeners and carried a

duffle bag containing 14 guns and contraband, drugs, onto a commercial plane. They avoided detection because they are airline baggage handlers who used their uniforms and their legally issued identification cards. Both men had passed federal background checks before they were hired. The men were only investigated and caught after police received an anonymous tip. If the airport had identification-neutral security systems such as requiring all flyers to go through metal detectors then the men could not have walked blithely past security. But the identification-based system allowing some flyers to skip screening because they are presumed to have no evil intent failed and the men transported weapons and contraband onto a commercial flight.

Legislation to repeal REAL ID has been introduced in the House and Senate. Maine and Idaho have passed regulations - resolutions rejecting the implementation of REAL ID and 27 other states are debating similar legislation. The Data Privacy and Integrity Advisory Committee should use its authority to advise the Department of Homeland Security that these proposed regulations do not solve the fundamental problems inherent in this national identification scheme. I appreciate the opportunity to be here today. I'll be pleased to answer your questions and also if you have follow-up questions I will be happy to submit and augment to my written testimony that has already been submitted.

MR. BEALES: Thank you very much. We appreciate that. Our final speaker on this panel will be Robert Burroughs who is the Assistant Chief at Driver's License Division at the Texas Department of Public Safety. Mr. Burroughs coordinates the field operations and fraud investigative units of the Driver's License Division. He serves on various committees of the American Association of Motor Vehicles Association. Prior to his current position, Mr. Burroughs was a Major in the Texas Highway Patrol. He managed and coordinated activities of the Vehicle Inspection Program and the Information Service of the Texas Highway Patrol Division and he served as a trooper and supervisor in various locations throughout Texas. Mr. Burroughs, welcome. I wasn't really going that fast.

MR. BURROUGHS: Thank you. I appreciate it. Thank you for the introduction. We appreciate the request today for the - to get the states' perspective on the REAL ID and on the implementation of the REAL ID. I was asked to speak about what it would take for a state to implement the regulations as we understand them and I will speak from prepared comments from that perspective.

In Texas currently the bills have been proposed and are being considered by the state legislature to modify Texas legislation to be compliant with the REAL ID Act and the provisions of the Act so that Texas can be compliant. Once again that's still in the legislative process so we're not - all I can tell you is we're working on getting there. Secondly, I want to say that the implementation of the Act is going to be significant for the

driver licensing agencies much as what Anne had spoken of. State of Texas has approximately 4.2 million licensed drivers coming into the driver's license offices throughout the state, about 334offices throughout the State of Texas, with an additional about 1.4 million drivers who renew or duplicate their licenses online or through mail-in processes. The first year of the Act our belief is we'll be required to process 7.2 million in-person transactions with REAL ID licenses. Obviously that's an increase of between 65 to 70 percent per year and then couple that with the processing time is going to at least be doubled by having to now image the documents and - you know, everyone thinks that minor things such as data entry of numbers and data entry of names. If I have a data entry on a birth certificate, I've got to put down the birth certificate number. We've got to put down the Social Security number, things that aren't in the data systems now, they just take time and they add time to the process. And so as they add time to the process and then they collapse time of the 5-year implementation on a 6-year licensing we've got to bring in 20 percent of our drivers additionally each year. And so the stress on the state licensing system then is compounded and we have of have additional personnel and additional offices and extended hours. Currently our belief is through our planning process is we'll need about 507 additional license-issuing technicians. Currently we have around 1,100, so you're talking about an increase of about 50 percent. Quite a significant undertaking.

We are I think in a fortunate position in the State of Texas compared to other states in that four years ago our legislature approved a driver's license reengineering project and funded that project for us. And it's a full business process reengineering, moving us off of a 25-year-old legacy system to a modern PC- based, internet-based communications system. We currently also have been approved an image verification system with a one to one verification of the person who's attempting to obtain a driver's license in our office compared to the previous photograph on file. And then in cases where there's a - because we are a law enforcement agency also there are cases where there's a non-match, then we have the ability to investigate that with a one to many search of the person to detect identity theft and to obviously deter criminal activity.

The imaged documents in the State of Texas, we have really two processes in the new process. The photograph, signature and thumb prints that we currently take will be transmitted in real time to our host database in Austin and an overnight batch upload of the REAL ID documents that have been imaged that will be housed on a local server and then updated overnight and then deleted from that local server after the update is confirmed. All images of course are stored at our DPS headquarters within the state police - within our state DPS facility and we meet the CGIS security requirements for all of our databases and all of our communication infrastructure. Utilize ADS encryption over the infrastructure. Our cards are issued from a central location. The card production facility is in the basement of our building. All materials are brought in and inventoried

there. We send a work order nightly to the vendor who then processes the cards, then verifies through the agency the cards that have been produced and then destroys that file for the creation of the driver records and then we mail the driver's license to the address indicated by the license-holder.

Some of the issues with REAL ID, I think they've been covered here quite well in the last couple of hours. The data exchange for the exchange of data or verification of data of documents of birth records, Social Security records and other identifying documents. It would be our preference not to have to build data interfaces to 54 different jurisdictions and to obviously four or five additional federal users or federal databases, but that the federated system where a single query could be run from one single query then disbursed to the various databases and it's I think Mr. Frenkel stated a green light-red light indication that the person is - that the record matches the request of the record is what we would like to see.

The issue that Mr. Frenkel I think hit on earlier about the accessibility of driver records. You know, currently law enforcement has accessibility to drive records through the NLETS system who then basically can go get a complete driver record and determine what actions to take in the event of a - especially a DWI. You look at the history of an individual to see if they've had a previous DWI for enhancement purposes of what charge to file. The data exchange between states from the law enforcement and from the driver licensing perspective is we want to know if that person was a safe and competent driver in their previous jurisdiction before we license them in Texas. You know our driver licensing goal is that the person is who they say they are and that they are a reasonably safe risk on the roadway and that they're not trying to commit a fraud. So we believe that you know obviously one of the requirements of the Act is that a person terminate their driver's license from their previous state and when they do that, wanting to be able to verify with the state that they've only had one driver's license, they've had it in only one jurisdiction and that they are currently still qualified to drive in that jurisdiction. The data pointer used in CDLIS has served the states well for the commercial driver's license information system. We don't advocate sending driver records to a central location or sending driver data to a central location or personal data. Only enough data to be able to identify that each person is individually who they say they are can be verified as licensed in another state. The transfer of records from state to state once again is a part of the Act, is to support the one driver-one record-one license concept and that is when a person leaves my state, they go to Arkansas, their driver history, their driver record and their identity record follows them. That's what we believe the intent of the regulation is and that that needs to be obviously performed in a secure manner so that a person’s identity is not compromised during that transfer, that those documents and records aren't compromised to be intercepted or in any way could be stolen or misused.

The last thing I want to speak to is the card security on the.

MRT, the machine- readable technology. The PDF417 obviously has been requested as a part - or has been prescribed as the proposed rule and from a law enforcement perspective and from doing the police law enforcement for the highway patrol for the last - for three or four years prior to the current job I'm in, we've seen over the years that the previous machine-readable technology that was commonly used was of course the mag stripe and in many cases it was encrypted by the states. Well, in the Highway Patrol Division we're trying to - we came up with mag stripe readers for a handheld computer for our troopers to use. The problem was we had 13 states that encrypted their mag stripes and refused to give us the decryption codes, even to law enforcement. And I believe that if we do encryption on PDF417, I'm totally for the privacy and security side of this. The issue we have to determine is how do we manage the decryption keys and how are they made readily available to law enforcement. And I mean readily available to law enforcement as a whole, not to just the federal agencies who want to read the driver's license at the airport, which is going to be an issue if we have to deal with encryption and encryption keys. Once again the reason for that is it increases officer safety. Officer is not having his nose in a computer while he's having to type out a ticket. Most of the data that's on the back of the driver's license is readily movable then to the courts through electronic systems that didn't exist 15 - 20 years ago. We're seeing officer safety - court efficiencies and officer efficiencies increase with the machine-readable technologies that are currently on the driver's license whether they be the PDF417 or the mag stripe. So those are the issues that I'd bring before the committee. Obviously we do support security, we do support privacy, but we also realize that there's practical implications on both sides too and the regulations need to speak to those issues.

MR. BEALES: I want to thank all of you again for being here with us today. I know we have many questions and our first question will come from Jim Harper.

MR. HARPER: Thanks all of you for being here and presenting. I think it's a very special day. Maybe the earth is spinning off its axis a little bit when the Electronic Privacy Information Center comes and talks more carefully about security than the Department of Homeland Security did. That's a fascinating development. But I think Melissa has her eye on the ball in asking what if anything does REAL ID add to the protections that we currently enjoy. Very important question, not well addressed in the NPRM and unfortunately we didn't hear anything about it this morning. Maybe we'll get some information on that from Assistant Secretary Baker this afternoon.

But I want to ask a sort of question of Anne Collins, and I appreciate the fact that you carefully couched your statement, you're considering what the State of Massachusetts is going to do. I'll note that the Boston Globe editorialized this week as you probably know calling REAL ID unrealistic and saying that the REAL ID law should be scrapped.

That echoes a statement made by Chairman Lieberman of the Homeland Security Governmental Affairs Committee two years ago when he called it unworkable. You talked a little bit about identity theft and those kinds of issues and doing careful analysis of the REAL ID Act and so I wanted to learn perhaps from you what you've been able to learn from DHS in terms of identity theft protections. In response to a question that Lisa Sotto asked this morning, Jonathan Frenkel said that identity theft would be measurably harder thanks to the REAL ID Act and I wonder if you have access to the results that they got. Did they express their results in dollars, in percentage terms and did they consider counter-measures that might be taken, corruption, fraud, hacking and things like that. So what result did they get in their analysis of how REAL ID would prevent identity fraud?

MS. COLLINS: Well, and I think that may be something that's better channeled to Secretary Baker when he's here, but from my perspective as a motor vehicle administrator, I don't want some of the real values that can be added by the REAL ID Act to be lost in the concerns about cost and practicality. I mean clearly without those, the time and the money to do this, we don't move anything forward, but specifically in terms of preventing identity theft I do think that as all states get a digital image and something that's not actually called for in the regulations but will be a necessary corollary to executing the verifications, there will be a digital image exchange that goes on between the states. This is something we were already contemplating and working towards specifically so that if you present me a Texas driver's license and the card - the clerk can look and see if that card matches the person who's there, but I can also then verify is that also the image that Texas has on file. So that if it's not, if someone is trying to create a new identity on someone else's name they're going to have a more significant barrier in getting there. Again, it's not necessarily included in the notice of proposed rulemaking, but because we're going to be dealing with so many false positives in the matches when we have you know people, Anne Collins, my own physician has eight different Anne Collins's that go to her. You know you're going to have to have to some tools that are available and by mandating that all states have a digital image that can then be exchanged I think that will be a movement forward. If we don't lose the one driver-one record piece, and I reference that because I think the notice of proposed rulemaking now talks about only being one REAL ID that is going to be matched. You're only allowed to have one REAL ID. But we know that a lot of states are going to have two-tiered systems and that they may have multiple - you may have a license and a REAL ID for example in a single state. If we lose that notion that there's only one record, driving record, we lose that measurable improvement towards identity theft prevention. I also think the fact that states are going to go to the digital image as required by the Act will mean that the states also add the facial recognition biometric as Massachusetts has done which is in fact helping us erode some of the fraudulent efforts to get false identification.

MR. HARPER: So the drop in identity fraud will be X percent or X dollars? What's the result?

MS. COLLINS: I don't have that number. They - Jonathan indicated that it was a measurable number. It's probably included in their economic evaluation, but I don't have that.

MR. BEALES: Ana Anton.

MS. ANTON: So thank you to all of you for coming today. My remarks also are for Ms. Collins. So first I'd like to commend you because there's more discussion of the FIPS in your testimony than I saw in the NPRM. So thank you for that. One thing I did notice in your testimony though was that you mentioned the pendulum shifting from privacy to security to efficiency. And as a software engineer we view these things as properties of a system and we don't view them as mutually exclusive, and the minute they are viewed or treated as such then our systems become vulnerable. So I appreciate your concern with practical operational considerations, but privacy is an operational consideration and I'd like to urge you to press for the resources that you need in order to be able to treat it as such. And the cost will be far greater if we don't design it in from the onset and so I urge you to consider that.

And a question that I have for you is in the NPRM it states that the states are going to have to provide a comprehensive security plan and I'm wondering whether you feel that you know what kind of guidance or guidelines or what do you need from DHS to be able to produce that and produce a good security plan?

MS. COLLINS: Well, it's interesting too when we talk about, and some of the other panelists spoke about a single point of failure. I mean one of my concerns about there being a sole place where all security plans for all states where all vulnerabilities are exposed being amalgamated in one place is in fact a threat to security. So that's kind of interesting. I know that post-9/11 all state agencies have gone through some threat assessments, some security planning. I don't think it is a bad idea to continue to put - shine the light on that and to focus especially in different areas. I mean in some cases we're talking about the physical threat. When the Democratic National Convention was being held in Boston there was a specific threat evaluation that went on and preparedness drilling. Looking at this from a privacy threat I think is a new take on some of the work that agencies have done when they're talking about homeland security. So the idea that there would be an outline and some guidance as to what elements should be focused on is certainly helpful. Motor vehicle - I continue to talk about doing more with less. You know we do not suddenly get a privacy officer and a security officer and a REAL ID compliance officer assigned to the agency as new mandates come down the pike. Rather, you pull the guy who was the state trooper who knew how to design a driver licensing system and you know say can you stay up nights and weekends and read up and learn

about this. I mean this is really how these systems evolve so any guidance that's given from a you know preparedness level is helpful. I hope that it's not just an open-ended set of questions that you know then does take off in 56 different directions.

MR. BEALES: Renard Francois.

MR. FRANCOIS: Thank you for your time and being here and Ana stole a little bit of my thunder with the comprehensive security plan. Mr. Frenkel said that they didn't want to prescribe a particular set of factors because it provided states maximum flexibility. And I think that kind of - it's one - I have one question to ask you, whether you all on the panel have a sense of kind of where states are with the security practices for the databases that already exist. Are they all over the map? Are they kind of similarly situated? Because in my view that if the state has a short timeframe and limited resources to kind of implement the REAL ID project, they are going to do what they continue to do and in the comprehensive security plan without any guidance they may think that what they're doing is sufficient and submit that. Mr. Frenkel said that it strikes me as a little passive that DHS will receive the comprehensive security plan, review it, look for gaps and then approach the states about filling the gaps when you could have 42 different gaps. Whereas if you kind of proceed from the same vantage point with kind of these factors that can evolve with security standards and security technology that you may have gaps, but at least you will have uniformity in the gap or gaps that you have to resolve. And I'd just like to get your thoughts on that.

MS. COLLINS: I think states really are all over the place in terms of how their systems were developed. A lot of us are going through mainframe replacements, legacy systems that are written in COBOL that are not you know forecasted to last forever or at least to have the staff to continue to program them. So and I can really only speak for Massachusetts in understanding sort of how technical security protocols get dictated. And it's really from the central ITD, the central information technology division of the state. And I find that very often the protocols lag the development of technology. So you've got people, sort of similar to the COBOL situation, you've got folks who were trained in one way of doing business, one way of thinking and even though technology is moving ahead, the person now on the state side haven't kept up. So I think it is great to put out best practices, but there's got to be flexibility in terms of understanding how the states can progress on all of these different fronts. One of my primary points of suggestion has been the fact that there really needs to be sort of a point system assigned and the things that the federal government thinks are the most important should be made clear because we can't do all of the things that are required under the Act at the same time. We will never get that much money in a single year, nor will we have the talent to execute all of the items on the menu at one time. So there really needs to be some - when you talk about phased and flexible implementation, there needs to be also some guidance

as to what is the most important elements. I think security - security and audit ability is the other piece that really needs to be enforced, and again it doesn't help - I can tell anybody who has access to any data field in my database. I don't have a lot of time to do that so I need to have some ability to prioritize where the threat is and where the risks are. I hope that was responsive.

MS. NGO: Was that question to the whole panel because I would like to answer as well? We know that there are a variety of security practices at the state level in different DMVs and that was why the Electronic Privacy Information Center and other groups want - believe it is completely necessary to have baseline minimum security standards that the states must meet, that the states can build upon. Do not have this be a ceiling. Have it be a floor. Because the states and the state DMVs are under attack. We have insider license for bribe schemes. We have in Las Vegas a couple of years ago a truck rammed through the wall of a DMV, grabbed the hard drive and got the information of 9,000 people. I mean therefore we definitely need to make sure that the security standards meet a minimum that we can keep working on and adding to. Because Mr. Frenkel said earlier that after the fact you can go back and find out who these people are. That doesn't help us really after the fact because the damage has been done. Because identification - sorry - because identification does not prove intent and that is why we definitely need increased security protections. Thank you.

MR. BEALES: This table is a little too long.

MR. QUAM: I think the microphones indicate that technology alone will not solve this problem. It's always more complicated. You know one of the questions I think Jonathan Frenkel actually mentioned my name with regard to the flexibility and flexibility is critical. From states' perspective and governors' perspective, one of the reasons for that is the ability to just get this done. I think you know having targets are vital so you know what you're aiming at. But having the ability to decide how to get there, states and companies and others can innovate a better mousetrap and the better mousetraps will come and states are going to need the ability to move and implement those to hit those targets. I thought one of the recommendations that was put out by some of the state groups for instance on security technology was a performance standard and that's echoed somewhat in the regulations. And the reason for that was the basic premise if you mandate a single security standard or tool or technology then it's kind of like putting the same lock on everyone's door. It might work that year, but as soon as somebody breaks it then you can get into everyone's house. Instead, let the states innovate and choose what works best for the systems they have. And states are coming from different levels. Some states are much further along on modernizing their systems. Some states are much further back. Some states are more rural, others have you know massive urban centers. All those things are going to play into the ability to just get there. And flexibility has been

a cornerstone for what governors have been calling for in order to allow states to get there. Again, it's not an avoidance tactic, but it's much more of an implementation tool. And we understand that flexibility has got to be leveled against the need for some uniformity because that's going to be critical to making the systems work, but there's got to be a balance. And I think we haven't found that balance yet. I don't see it yet in the regulations, but it's going to be critical moving ahead.

MR. BEALES: Neville Pattinson.

MR. PATTINSON: Thank you. Very interesting to listen to all of you. Certainly from Mr. Quam's perspective I'm very encouraged to hear the governors are supportive of moving forward and to solving the situation. With respect to Mr. Burroughs, the machine-readable zone being accessible and available to law enforcement, I think that's a very good requirement. We hear that as a requirement rather than a complaint. The problem with a machine- readable zone though is as you expressed the lack of the ability to decode it if it's encrypted. It's not really a question of encryption, it's a question of accessibility of the data and who should get access to that data. And then when you have access to that data if it's integral, if you've got good data and obviously keeping it confidential is an essential part of the privacy aspect. Many systems exist today to take a business card and scan it through optically. You can put a driver's license today through an optical scanner such as that and pick off the information.

So the MRZ zone, unless it contains information beyond what's already printed in plain text on the card offers no significant value. We need to look at technologies that perhaps enhance that and provide accessibility to information and ensure confidentiality and integrity of the information.

With respect to Mr. Steinhardt and Ms. Cope both of you in your testimony discussed the fact that this is not achievable under REAL ID, but it can be fixed. And with respect to privacy issues, is there one or two key areas you'd like to suggest to our committee that could be done to fix let's say the usability of REAL ID or an identification card, be it driver's license, in the scope of that there will be a nationalized identity system as you describe it. What are the key issues that we need to look at from the usability? Not necessarily the enrollment and the vetting. I think we've got lots of information in the NPRM about that, but there's very little in the NPRM about the usability of this document and how we're going to preserve the privacy of the citizen and hence thwart identity theft. So I'd like to hear from both of you if you could.

MS. COPE: Thank you, Mr. Pattinson. Just I guess to reiterate what I said originally from CDT's perspective our concern in terms of the statutory language is the electronic access provision that requires that every state give electronic access to their DMV databases to every other state and of course the machine-readable zone requirement. That language is so, so, so broad, so in terms of an initial recommendation

to the committee we would say to recommend that Congress or through the Secretary, that that's something that Congress could or should change. But the real issue I think with that provision is really this - well, let me back up. One point I actually didn't get to elaborate on but actually Mr. Burroughs did touch upon is the CDLIS system, the commercial driver's license system. That system is what DHS is proposing to - as sort of the architecture or the framework to implement this electronic access provision of the Act. I feel like there hasn't been incredible sort of - I don't know if it's transparency or just sort of detailed discussion about what that CDLIS system looks like, or what it would look like for REAL ID cards. So one recommendation for the committee is really to try to get - you know sort of pin DHS down and really ask them to explain how that system would be architected. My understanding is that the way the CDLIS system works now with commercial drivers is that AAMVA holds a central database of basic demographic and other information about commercial drivers and then that database pings to state databases that have additional information regarding the commercial drivers' driving history. If that exact system is going to be applied to not just ton-commercial drivers, but ID cardholders, that really does create again like I said a one person-one card-one record system and Mr. Burroughs actually said that that record is going to follow the person around the country. What I would say to the committee is to ask both Congress and - or DHS what are the limitations of what information goes into that record, the record or the DMV databases, however you want to define it. What information is going to be in that record, is it going to - are source documents going to be in the record? Who is going to have access to that information and for what purposes? There are absolutely no limitations in both the Act or the NPRM regarding those issues of again what information is going to be in there, what's accessible, you know what's going to be accessible, by whom and for what purposes. And so I would say to the committee is to really try to get to the bottom of that.

MR. STEINHARDT: If I could respond. You know I think the important thing to recognize is, and you raised a lot of important issues here, is that these issues cannot be dealt with within the four corners of the statute as the statute was written and as the Department of Homeland Security has attempted to contend with it. That's why the statute needs to be revisited. The statute is pretty clear there has to be a machine-readable zone. Statute's pretty clear there has to be interoperability between the various states. You have all those sorts of problems and there's not a lot of flexibility in the statute. There are solutions to these problems. There are ways to make the driver's license both more reliable and robust across the country, but at the same time protect privacy. Some of them perhaps could have been addressed in the regulations. The machine-readable zone I suppose is one of those. They could have required encryption, but at the same time created a system that would allow law enforcement who has a legitimate need to get access to the data to do so, perhaps for example by having a common identifier that

would be available to law enforcement which in turn would be able to determine whether or not for example the person whose license they were looking at was subject to an outstanding warrant or had a record or whatever. Others are simply not amenable to fixes under the statute. The problem that you raise for example, the problem of people scanning, using optical scanners to harvest the data off of the card in order to both bypass the current protections under the Drivers Personal Privacy Act and also to create this sort of universal private sector database of drivers information could be dealt with for example by allowing the states to - one way you could deal with this is allowing the states to vary to some degree both what information is on the card and how it appears on the card. As a practical matter under the statute and under these regulations that can't happen. So that you're going to have a uniform card across the country. It lends itself to that kind of optical scan. It lends itself to that kind of harvesting. Those are the kinds of problems that you know when you get down into the weeds here, when you really begin to deal with the specifics of the statute and deal with specifics of this problem to which there are creative solutions. The problem that we all face at this point is that the statute doesn't allow for those creative solutions. It mandates a particular approach. It's an unworkable approach. It needs to be revisited. As Melissa said, none of us who believe that the statute has to be revisited believe that it should be repealed and then nothing should follow that. But we begin by starting with a repeal of the statute as it is now and work out a system for contending with these issues in a way that's both fair to individuals and fair to the states.

MR. BEALES: Barry if I could just ask, let's put the statute aside okay and let me focus on the substantive problem because I'm interested in this issue. I've never seen two business cards that are alike except within the same company and it doesn't do me much good to scan my colleague's business cards. So the software is able to deal with differences in format without a lot of difficulty and capture that information. And we did a comparison of the driver's licenses in a small group of us. They all have machine-readable zones on the back. They're not the same. So where's the unique risk all right in harvesting this information that stems from whatever Homeland Security does that's not already there with the existing system of driver's licenses?

MR. STEINHARDT: Well, with respect to the machine-readable zone you're talking about one set of common data which will be in a common format, it'll be housed in a common manner. You are going to have readers quickly developed across the country to harvest that information. It is the ubiquity and the uniformity of those readers. That's also going to be true of the use of optical scanner, the devices to harvest information from the printed information on the license. The fact is that sure, right now you can on a business card you can take off the name and the address, but we're talking about much more information on the face of the driver's license. Currently there's much more

complexity and more variance in order to how that information is displayed than there is on the average business card.

MR. BEALES: Who's next? Lance Hoffman.

MR. LANCE HOFFMAN: Sorry about that. The technology strikes again. Thank you all for coming and giving us your opinions this morning. Question for Mr. Burroughs. You mentioned that 13 states encrypted their data fields but did not give out their encryption keys so you could not read it I think is what you said. Could you tell me how many states did share their fields as opposed to did not and also of those that did not, did they articulate why or did you get any informal indications why they didn't do it or both?

MR. BURROUGHS: Many states, and I'll be – not able to speak specifically of which states. Many states though had specific statutes that provided that information to their local and state law enforcement only. And that was one of the barriers we came up against. And then others were - the information was deemed to be a DMV - you know in many states the DMV is not the same as the state police. It was deemed to be DMV purposes only for them to use it for auditing and tracking and they didn't - it was internal policies that they didn't release it to other states.

MS. SOTTO: Richard, did you have a question? Okay, you're all set. Kirk.

MR. HERATH: I too want to thank you all for coming here today. I was going to pose this question to our DHS panel and I'll probably pose it to him in an email, but this is for Mr. Burroughs mostly and Ms. Collins. Obviously the American Association of Motor Vehicle Administrators has a fairly mature, well-defined governance process among yourselves. And DHS discussed specifically the federated system that this is in essence going to be rather than a federal system, although there was a slip there. They also admitted they didn't have any expertise in motor vehicle licensing or how to run it. So what has your experience been with the interaction, collaboration and how do you think that this system will be governed going forward? So retrospectively how has this been governed and prospectively how do you think it will be governed? Is there a structure that's in place? And then I have a follow-up question too.

MR. BURROUGHS: The AAMVA REAL ID steering committee is putting together a governance structure sub-work group that will begin meeting. There were several states, I believe four states who participated back in the fall, started participation in putting together a governance structure for a federated system in conversation with DHS. The current system CDLIS is governed by AAMVA and basically it's the 50 states participate and it has its own established governance structure. When it began it was AAMVAnet which was an independent corporation. AAMVA has a couple of other units similar to that that do other registration like the interstate registration plan, the IRP which

is a different corporation as well as the Driver's License Agreement Corporation. And you know they basically -they set up a corporate structure, they set up bylaws, they set up standards for participation that the states agreed to and to become members and they have auditing and compliance requirements.

MS. COLLINS: Yes and I was actually one of the four states that participated with DHS in really trying to drive the decision towards a CDLIS-type matching primarily because it is a mature administrative structure and there can certainly be additional safeguards that are developed. We've had a lot of discussions about that and actually have a working draft where we've talked about the fair information practices being incorporated into the governance structure because I think that will be important as we expand the system. From the business side of the house it's absolutely critical that the federated system grow out of AAMVA. It is the only structure that exists for us to - from a knowledge base of the motor vehicle administration for us to communicate in like terms. I mean if you take something as simple as whether it's a DUI, an OUI, or a DWI we're all talking about the same thing, but we're all talking about it in different abbreviations and different codes. Since the creation of the commercial driver's license there have been hours and hours, tens of thousands of hours put together towards reconciling the vocabulary through which states discuss common business practices. And as we look to integrate the various checks that are being done while the customer is standing in front of us, Social Security, 50-state driver's license check, Department of State, SAVE, birth certificates, they have to be incorporated into a single business interface. We can't have just the hardware that you could imagine for running multiple queries at a branch location, so it has to from my perspective work through AAMVA. The states are very good at working out discipline in terms of holding each other to task. The International Registration Plan is something that you may be familiar with. If you're in my generation it made it a lot harder to play the license plate game when you're on family vacation because trucks no longer have a license plate for every jurisdiction that they drive through. You just see that one state that says apportioned. If we can trade money between each other and we do very successfully I think we will also take the same care with information and AAMVA is the right place for that to happen.

MR. HERATH: Okay. But and I know that you interact well. Do you feel that the DHS folks that are responsible for coordinating this are integrated well into AAMVA and recognize and respect AAMVA for sort of the foundational organization upon which most of this rests?

MS. COLLINS: I think we're getting there. It's not - the fact that it's not spelled out in the regulation leaves us all wondering what do they mean by federated system. Even in the course of the AAMVA Region 1, the New England and I guess from Maryland up states met with Darrell Williams on Monday and the question didn't come back with a

specific answer. I know also from other conversations that I've had that there are vendors that are continuing to talk about an outsourced, privatized solution that would ostensibly attempt to provide either an option or a competition to a centralized system. AAMVA is the states, it is the organization of the states, it is the only reasonable vehicle that I see for getting anywhere with any reasonable time and I don't think 2013 is a reasonable time, but there really needs to be an exclusive remedy there that is something that is of and by and governed for the states.

MR. HERATH: A final question and it's real quick. Have you done a gap analysis to show where the states are relative to each other based upon what you can currently define as the standards in the NPRM and so in other words which states are close to certain requirements, which states are farther away?

MS. COLLINS: That's underway right now. There's actually a centralized comment being developed on behalf of AAMVA from the states that will look at that and I think that there has been charting of a variety of the elements of the Act. You know some states are central issue already so they're beyond some problems. Some states are in the middle of legacy mainframe system replacements so they're behind in other aspects. There are as many variations as there are states.

MR. HERATH: Thank you.

MR. BEALES: David Hoffman.

MR. DAVID HOFFMAN: Thank you Howard. Once again I'd like to thank everyone for coming and sharing this information with us. This has been very informative. I want to make sure that I understand some of these issues correctly. My understanding is that the NPRM officially limits the scope of official purposes to three areas: accessing federal facilities, boarding federally regulated aircraft and entering nuclear power plants. And my understanding is, and this is in part due to the good research of Mr. Harper who's on the panel, that what this does is it sets the standard for ID that can be used to access those official purposes, but that for most of them there are secondary methods if an ID is not present that can be used to access that. For instance if you do not have an ID and you need to board a plane it means that you have to go to secondary screening as has happened to Mr. Harper I believe. And so I think there's some statements in some of the testimony that's been provided stating for instance things like people are not going to be able to travel. And I think that's likely not true. But at the same time it does seem that by the time period when the regulations will require REAL IDs that there will be a great number of people from what I'm hearing from you who will not have them for one reason or another. Could be that a state decided not to implement, it could be an implementation problem technologically, or it could be that individuals choose not to go and to get them if there's a two-tier system for example. So my question then really is that has there been a discussion of the implications of that to the individual

and in two different ways. First, the implications to the individuals who do not have the ID, specifically the privacy implications in that if they are subject to other checks beyond the regular ID checks such as a secondary screening mechanism. That actually could be more privacy-invasive because the secondary screening could cause them to have to release a lot more personal information or subject themselves to a physical search that they normally would not have to. And second, what the implications would potentially be to all people that are going through that process. I'm not an expert on what it takes to enter nuclear power plants luckily, but I'm assuming that there could be substantial implications to waiting to board aircraft if a much higher percentage of people need to go through secondary screening. And that may be a question that we also need to ask the folks from DHS, but I'm particularly interested in the folks from the states if there's been a discussion with DHS of those implications and what it means for the residents of your states.

MS. COLLINS: There has been discussion in Massachusetts about whether if a two-tier license is created, whether that creates a jaundiced eye in law enforcement when a person is pulled over and they have the non-REAL ID, will that subject customers to further profiling or harsher treatment or some greater level of suspicion. There have been question raised by the motor carrier community as to whether a federal facility includes delivering goods to - cargo, specifically in and out of federal facilities and whether that will impair the movement of cargo or increase the cost of cargo. I think there are a lot of questions. I don't think there are a lot of answers and I don't want to dominate this discussion.

MR. QUAM: I'd like to echo that. I think there are more questions than answers. You know under- it's interesting from our perspective, from governors' perspective you know the way you get around calling this an unfunded mandate is by saying it's not a mandate. States have a choice. Not much of a choice really in the end. I think you've raised some interesting questions with regard to inconvenience, the line, the privacy issues related to if you don't have a REAL ID and that's a real concern. I'd also like to point out though that although the department has restricted this to the official purposes that were listed in the statute, it has the option, the Secretary has the ability to expand that list. I'll note that just in the last Congress there was at one point an amendment floating around that would have made REAL ID necessary in order to get a voter identification card. It's pretty quickly, as REAL ID comes online the official purposes are going to expand rather quickly, whether it's done by Congress, whether it's done by the Secretary, whether it's done by states who decide hey, if we have one card here there are benefit packages. This could solve a lot of issues for a lot of different agencies, whether it's benefits, whether it's whether you get into a building, your identification, your legal status in the United States. We have to be wary of all the potential uses and we have to get this right because of the unintended consequences of moving forward. So while it's

very restricted right now and there are options for people standing in those lines, not only will the lines be affected, but I think it's where are we going to be five years from now as this comes online. We really need to take a look at that vision and make sure that we're getting things right to deal with those consequences so they're not unintended, but we actually know where we're heading.

MR. BEALES: Mary De Rosa.

MS. DEROSA: A couple of you mentioned the issue of DHS increased or an appetite for expanded access to state information. And I wanted to hear a little more about that. There's so many issues here that that didn't get discussed a whole lot. A little more about what concerns there are and what kinds of limitations if any you would like to see on DHS's -what kind of checks, what kind of restrictions if there are any that you think would be useful on DHS's ability to access this information.

MR. STEINHARDT: I'll take a pass at that. Look, you know I think Ms. Collins put it very well here. Build it and they will come. I suspect we could probably spin out any number of areas where DHS has either suggested it needs data or it might want data in the future and others in the federal government and law enforcement community and in commercial sector have said that they would like access to additional data. But the reality is that if you create this system, and REAL ID really needs to be seen as an identification system. It's not simply an identification card. It is an identification system backed up by the database and including the machine-readable zone, including the card, including the whole package. People will find additional uses for this. And those uses are going to vary from the commercial sector which is going to insist on the production of the REAL ID in order to demonstrate identity so that you can do everything from rent a car to open a bank account to get a mortgage to get a lease, you name it the commercial sector is going to ask for it, to the federal government that's going to begin requiring it for all sorts of things that are not currently contemplated in the statute. And while I applaud the fact that DHS suggests in the NPRM that there are these three official purposes that are mentioned in the statute for which the REAL ID would be required, the reality here is the statute is very clear. DHS can designate anything as an official purpose. And down the road we can expect and I think we can predict that they will add to the number of official purposes for which REAL ID will be required. After all, remember the whole idea of REAL ID is that this is going to be one ID that's uniform across the country that all the jurisdictions are going to adopt. If you have one or more states opting out of this the whole house of cards collapses. You can't have a uniform system if the people of Maine or the people of Idaho don't have one of these cards. So that if I was the Department of Homeland Security I certainly would say we've got to make it more you know advantageous to the people of Maine or the people of Idaho to have this card. We've got to make it necessary to the people of Maine or Idaho to have this card and the only way to

do that is to add to the number of official purposes so that there's no way that Maine, Idaho and soon we think Utah and some other states can opt out.

MS. COPE: I agree with everything that Barry just said, but I want to make sure the distinction is made. The official purpose part of the Act and you know DHS basically just mirrored it in the NPRM is for the required presentation of the card, right? So if you want to get onto an airplane you have to show your boarding pass and then your REAL ID card. If you want to get into a courthouse you know, show your card, whatever. What that doesn't get to is access to the personal data including the source documents that are like I said earlier are going to be in a more centralized location, and as of right now without - no limitations on use or access, right? So if you read the NPRM carefully it's very interesting. It says - like I said, so the official purpose is one thing. The requirement for the presentation of the card. The NPRM very sort of I don't know quietly states that the rules do not grant or require DHS to have any greater access to personal information than they would already have. Well I frankly don't know what that means and the key point is that it doesn't prohibit DHS from getting access to the information. So again I want to make the distinction between accessing information and requiring the presentment of the card for an official purpose.

MS. COLLINS: One of the thoughts that's sort of cavalierly injected and especially more so the very first meeting that I attended at DHS there was an initial discussion about liquor stores and cigarette sellers, you know sort of this will be great because they can scan the card and they can prove that you know you're 21 or you're over 18 or whatever. And you know after there was sort of a reaction of outrage on behalf of the motor vehicle folks that kind of tapered off, but I've heard it echoed in Secretary Chertoff's testimony about the value of this. It's going to be a better tool for administration of programs such as alcohol and tobacco control. So I think that is not very far from the surface and it's not clear whether that's contemplating an electronic connection, or just the fact that because the card was better created in its initial issuance that it is more reliable, that you know kids can't tamper with the card. I - it's my impression that there was an intended electronic verification at retail settings that was at least contemplated if not explicit in the rules now.

MS. NGO: Well, I you know clearly agree with the fact that there will be expanded purposes. I mean DHS in the regulations specifically says that later on they can expand it. Secretary Chertoff has said that he wants to think about expanding it to Western Hemisphere Travel Initiative at the very least. And there's - it's like a spider web. You start in the middle. It's going to be this one national identification system and then it spreads out everywhere. For instance, there was a recent scandal in New Jersey. Nightclubs had decided to start scanning driver's licenses and downloading all of the information. The New Jersey state DMV chief sent letters to the nightclubs saying this is a

violation of people's privacy, this is a violation of state law privacy and federal law privacy and the nightclub's response was well, why would they you know have this type of technology which allows us to do this if it's not legal? So we're going to sue. We're going to keep downloading the information and sue to say that because there's technology to do it then we should be allowed. And that's just one example of how it's just going to keep expanding. Nightclubs, liquor stores, colleges will start doing it. I mean it will just keep expanding further and further.

Now you wanted to talk about concerns and limitations. Well, what we advocate is the distribution of identity or an identification meta system in which identification is confined to specific contexts in order to limit the scope of potential misuse. This reduces the risk associated with security breaches and the misuse of personal information. For example, a banking PIN number in conjunction with a bank card provides a better authentication system because it is not coupled with a single immutable consumer identity. If the bank card and PIN combination is compromised a new bank card and new PIN number can be issued and the old combination can be canceled. This limits the damage that can be done. This means that misuse is limited to the context of the information breach, whether it is a single bank account, an online merchant, or medical records. So if you have this layers of security, layers of identification then it makes it a lot less likely that the system itself will cause a huge ripple effect when it is breached.

MR. BEALES: Can I just go back to your New Jersey example because it seems to me to say, and I want to understand why this is isn't right. It seems to me to say that there is not a unique privacy problem that comes from REAL ID or anything about it. The privacy problem that may be out there is existing with current driver's licenses in current technologies and your complaint is that REAL ID doesn't fix it. Am I missing something? Is there something - where's the unique risk here? MS. NGO: You're correct that we already have this problem. And the question is REAL ID is asking and claiming to better protect people, that this is a better security system. And if it makes it easier for people to download the information through the machine-readable zone being unencrypted, if it somehow allows long-range RFID, if it allows all of these things then it takes a step backwards. It in fact makes it easier for nightclub owners, liquor stores, everybody to say okay, give me your information because it's there and I can take it.

MR. BEALES: I guess I'm not seeing the how it makes it easier.

MS. NGO: If you have an unencrypted machine-readable zone, if you have the atmosphere of -.

MR. BEALES: Which we do.

MS. NGO: For some states. If you have -.

MR. BEALES: I mean, I just don't know. Are there a significant number of states where there's not a machine-readable part of the driver's license? No.

MS. NGO: I'm talking about encryption. And what I'm talking about is the data-sharing of information. Whether we have a system where it's okay for DHS, for anyone, the states, liquor stores to say we can take your information. This is the data-sharing environment that we feel is accepted under the REAL ID regulations and we are against that.

MR. BEALES: Ms. Collins.

MS. COLLINS: I believe there are 46 states that have a machine-readable zone on their cards now. It is primarily designed for, as Mr. Burroughs said, for law enforcement to be able to quickly download that information so that they can continue to engage in a roadside stop. It's also frankly built into our business process so that in the future we can have customers who come back to us and we can populate the licensing fields to speed renewal transactions. To the extent I think you're dead on that that information is already out there, it's already in use whether it's in an optical character reader or in a machine-readable zone. That information is not the most invasive information that you find. It is the name, address, it's all the information that's on the front of the card is on the back of the card. In some cases it helps us with - for the petty fraud detection because there are - the readers in the branches will make sure that the information does in fact match front and back, so somebody who has tampered with the data on the front may not be able to as easily counterfeit the information in the machine-readable zone. .

MR. BEALES: What happens now when your law enforcement officers encounter a license from another state?

MS. COLLINS: In Massachusetts they do have a code. If they don't have a decoded machine-readable zone they would hand type in that information that appears on the front of the card and use it to match through NLETS.

MR. BEALES: Can they read the machine-readable zone of other states' cards?

MS. COLLINS: Those that are not encrypted and Mr. Burroughs probably knows more about this than I do, but it's - unless - I take on face value what he said which is if it's encrypted in general there are state laws that restrict that information so they would just have to use the front of the card, data enter and do the NLETS check.

MR. BURROUGHS: In reference to the machine-readable area, like I said before some states encrypt it and otherwise if not, as Ms. Collins said, they typically have to key it in or they have to go to a microphone and talk to dispatchers, run a check for driver check or wanted person check.

MR. BEALES: I think we have time for one last question and that's Richard Purcell.

MR. PURCELL: Moving to - from the front of the card and the back of the card to the back-end databases. We've had some conversations already from Mr. Francois and Mr. Herath's questions about the security standards that are apparently not in the NPRM. What I'm - simple question. Does AAMVA have a set of security guidelines that they require their participant organizations to comply with?

MR. BURROUGHS: The security guidelines are set up in the membership agreements. Yes, there are security guidelines in each one of the data systems and in the CDLIS rewrite and in this new governance structure that'll be an integral part of the implementation of the - when I say governance, the federation governance committee. That'll be an integral part of what they're putting together as a proposal to expand CDLIS to be the data interface, CDLIS and the AAMVA network to be the - to provide the data interface for the central record, basically a central record window to gain access to all the federal systems and other states.

MR. PURCELL: Would you promote those guidelines as being at least a minimal standard for the rules that would support REAL ID?

MR. BURROUGHS: We would, yes, because it's the 50 states in agreement that this is the standard. And there are security officials on staff at AAMVA who obviously we have security interests. You know, CDLIS has never been hacked. It's never been compromised. The new advanced - AAMVA just relet the contract for a new network and the new network security is a closed network, basically point-to-point closed loop network of only the member jurisdictions. Any edge to any other network is of course through standard firewalls and standard high-level security practices and business practices that are in, basically in place today.

MR. BEALES: I want to thank each of you for taking the time to be with us today. This has been most helpful and most enlightening about the issues that REAL ID poses and we really appreciate your time and effort to be here today. Our next speaker is the Honorable Stewart Baker, the Assistant Secretary for Policy at the Department of Homeland Security. He was appointed by President Bush and confirmed by the Senate on October 7 of 2005. Prior to his appointment as assistant secretary he served as general counsel of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction where he headed the drafting team. He was also the general counsel of the National Security Agency and the deputy general counsel of the Department of Education. He has been an associate and a partner at the law firm of Steptoe & Johnson before his government service. He clerked for Justice Stevens on the Supreme Court, Justice Coffin on the Court of Appeals for the Fifth Circuit and as an intern law clerk for Justice Hufstedler of the Ninth Circuit. He served on numerous government and international bodies dealing with national security and technology and

related topics and he was awarded the Defense Medal for Meritorious Civilian Service in 1994. Secretary Baker, thank you for being with us and welcome.

ASSISTANT SECRETARY BAKER: Thanks a lot Howard. I'll try to make the speech shorter than the introduction. It's actually a great pleasure to be here. There's so many friends on the committee I'm really sorry I haven't been able to get to see you before this. So it's great to see you all and I will save some time for questions. What I wanted to just talk about because I know you're looking at this issue already is questions about identity theft and REAL ID. We all know identity theft is an increasingly difficult problem. Whoever said that information wants to be free may not have been right about copyrighted songs, but they sure were right about our Social Security numbers and our mothers' maiden names. You can buy that probably for everybody in the room for fifteen bucks a pop off of dark net servers around the internet because it's so easy to gather that information. And identity theft is increasingly a serious problem. I think 10 million Americans were subject to identity theft in the last year and that's not a number that's likely to go down. Costs $64 billion according to most estimates and that doesn't count the amount of kind of exposure and violation that I think most people feel when they discover that somebody is running around running up bills, using credit or taking other actions in their name without them being able to stop it. So it's obviously a big problem. It's a big problem that DHS has run into quite directly, not just in cyber- security but in immigration enforcement. We have a mechanism for making sure that when people sign up for work they have a Social Security number that goes with their name. This is not a mandatory program, it's just a voluntary program and a number of employers use the program. In theory that should prevent people from getting jobs who have just made up their Social Security number and it does, but it turns out that what illegal immigrants do who want jobs at those companies is they don't make them up, they steal them. And when we raided a large meat-packing company we discovered that a large proportion of their workforce was working under a Social Security number that matched the name, it just wasn't really their name. They had essentially stolen the identity of somebody else or in some cases borrowed the identity or bought the identity of another person. But they also had run up debts in the names of the people whose identity they borrowed and caused all kinds of difficulties, and they did it because it was relatively easy to engage in identity theft. So it's obviously a hot topic. The question that I know you all are interested in is whether REAL ID is going to make it worse. And my thought is while you can never foresee the future, every indication is that REAL ID is actually going to make it less easy for people to engage in identity theft. The privacy concerns about REAL ID have always puzzled me. I'm not sure yet that I could state them with certainty without having to distort the facts, but let me state what I think the argument is with respect to REAL ID and identity theft. First, that somehow the DMVs are going to have more information about people than they do now and they're going to pool this information into a central database

that'll be accessible to hackers and to unauthorized parties who will then use those databases to steal the information and take over the identities of the people whose information they've gathered. Well, I think if those things were true you could see how there might be a risk, but they aren't true. REAL ID does not require a centralized database. It doesn't really require that states gather any more information than they already gather with the exception of probably eight or ten states that don't now actually ask for information to show that you live in the state where you're getting the license. Relatively small amount of information that is going to be gathered by a minority of states that are not gathering it now. And because of the concern that we had about being party to anything that would lead to violations of people's privacy we actually went out of our way in the NPRM to write a requirement that each state develop a privacy and security plan for the data so that - as to tell us how they are protecting it from unauthorized activity. We require background checks and security for the issuance of the licenses to make sure that the DMV process is not infiltrated. And we don't, as I said, require a central database here in Washington where everybody's records go to be looked up by whoever has access to the database. This is a federated system. That is to say each of the DMVs keeps the information that it has gathered in its own database, but I think most people here are familiar with the problem we used to have with truck drivers who would get five, ten, fifteen driver's licenses in different states and then just accumulate points on all of them so that they paid the speeding tickets and never had to worry that their license was going to be taken away no matter how tickets they got. They just pulled out a different license the next time they got stopped. That's a problem and it's not just a problem with truck drivers. We've addressed that already for commercial driver's licenses. Those are now subject to automated checks so that you can find out whether someone who's asking for a commercial driver's license in one state already has one in another state. The REAL ID Act would apply those standards as well to other driver's licenses, not just commercial ones. So the only ability to get into the information of other states' driver's license database is that a state can ask all the other states does this fellow, does this woman have a driver's license in your state because they're asking for one here. And if there's somebody who if they have a driver's license in another state, then they're going to have to relinquish that to get a new one so that people will have basically one ID. But there isn't an ability to gather information about the license beyond the question does this person have the license in another state. That federated approach is generally the approach we took in the NPRM with respect to all data where we could reasonably leave the data in the hands of another party who maintained it and have that party respond to inquiries that are limited to particular questions. That's how we designed the program. I don't think I have to do a lot of missionary work on federated database approaches with this group, but we certainly think that wherever possible it's better to leave the data where the party that gathered it and maintains it can continue to maintain it so that it's always up to date and accurate rather than falling behind in somebody else's database. So

there is no obvious place that a hacker could go to try to gather information unless they went to the places they would go today which is individual DMV databases which we hope we will through a combination of suasion and authority induce states to bring up to higher security standards over time.

The reason I think that REAL ID will actually help is that we've relied for a long time on having privacy and identity security that depends on knowing stuff that nobody else knows about us, our mother's maiden name, or a Social Security number that we don't reveal. And we've gone to some lengths to try to hide Social Security numbers from kind of casual gaze. But the fact is in this era it's just not possible to keep information like that secret for very long. We reveal it far too often and if we reveal it once in a context that's not secure then the folks who think that fifteen bucks for our financial information is a good deal for them will start selling it and trading in it. So in the long run having a secure and secret fact as the source of your identity is not going to work. We're going to increasingly have to move to tokens of one sort or another and one of the tokens that we're obviously going to rely on pretty heavily is identity documents. And those identity documents are going to have to be more secure if they become the last barrier between us and identity thieves. And what REAL ID really does is it substantially improves the security of the documents starting at the process where someone goes in to get a driver's license. If they're going in to get the driver's license of someone whose identity they're trying to steal they would have to be able to produce a birth certificate typically. That birth certificate in the long run will have to be checked against a database to show that there really was someone born on that date in that jurisdiction so that the birth certificate can't be a fake and the party is going to have to know where you were born as well as when. Then the process of issuing it will be subject to substantial security controls so that it will be hard to obtain from a friend in the DMV the license and it will be very difficult once the license has been issued for someone to steal your wallet, get your license and put a new photo over yours and present that along with your credit card and try to pretend to be you. So our assumption is that at the end of the day rather than being a risk of identity theft, REAL ID as it's integrated into the decision to accept credit cards and the like is going to be a net positive for preventing identity theft. I'll stop there and see if I can take a few questions. .

MR. BEALES: All right, thank you very much. Jim Harper.

MR. HARPER: Thanks Chairman. Stewart, nice to see you as always and thank you especially for at least making some affirmative case for REAL ID. There's been a lot of defense and defensiveness about REAL ID, but you listed potential benefits of REAL ID and that's welcome, identity theft, immigration control and truck drivers. Of course it wasn't truck drivers who knocked down the Twin Towers and I think it's important for us to keep our eye on the ball. And a very important question that underlies this committee's

considerations in our framework document we found that risk management is an important and appropriate thing for us to consider. The Secretary speaks in terms of risk management and that's all welcome and good. So the question is how and how well does REAL ID improve our security protections. And I suppose to get into that in a little more depth I wanted to get your assessment of what counter-measures might be taken by sophisticated threats to undermine the system that REAL ID would have us implement.

ASSISTANT SECRETARY BAKER: I'm not sure I want to get into all the ways that you could defeat REAL ID, but maybe you can bring that back.

MR. HARPER: You have thought them through.

ASSISTANT SECRETARY BAKER: I have - well, we have done some thinking about the risks here and - but let me start with the question of how does this make us more secure. I think it does. Almost everyone who studies things like airline security and gives us advice says you know, you can't just say you're trying to find the weapon and keep the weapon off the plane because that requires eternal vigilance. You've got a system in which basically everybody sees exactly what you're doing and exactly what you're looking for and can carefully design around your screening system as the 9/11 hijackers did and indeed as the folks who wanted to blow up the planes over the Atlantic last year did. So just looking for weapons is not really a complete solution. It's much better if you can identify people that you're worried about, let large numbers of people go through un-hassled, then concentrate your attention on the people that you're most worried about, and that's things like having a good list of the people that shouldn't be on planes and a good list of the people who ought to be looked over closely before they get on the planes. All of those systems in which you try to use intelligence and make judgments about people in advance about why you're worried about them require that you know who they are and that you be reasonably confident that the people who are getting on the plane are presenting credentials that match their real identities. And REAL ID does precisely that. It makes it harder for people to acquire fake IDs and therefore to evade systems that are designed to leave most of us un-hassled and to focus our enforcement attention on the few people that we're actually worried about. That is not a system - as I will now do what I said I wasn't going to do - that's not a system that is completely foolproof of course. Any ID system can be defeated if you're willing to work hard enough at it. U.S. currency is forged by some very talented forgers and if you are a foreign nation and you wanted to forge an American passport I'm willing to bet you could. So we'll never have a completely secure ID system, but we can make it much more difficult for people to acquire fake IDs and to use them to get on planes or to get access to government facilities. And we can catch a large number of people who may not yet have made a decision that they're going to be taking action against us, but who in a year or two choose to do that and if they've used an ID that actually allows us to identify them and to see whether they

came into a facility or took a flight before and it wasn't easy at a time when their trade-craft was not particularly sophisticated, if it wasn't easy for them to acquire a fake ID then they're likely to use their real identity. All of those things mean that our records are better and our ability to differentiate between people who are potential threats and people who aren't is substantially improved.

MR. BEALES: If I could just very briefly follow up on that. I mean I see the harder to fake, that clearly makes sense, but how useful that is depends also on the nature of the process of presenting the credential. What happens now in airports, it doesn't matter. From what I see it doesn't look like it would matter how hard the document was to fake because nobody looks at it closely enough to even think about that question. Does the name match, does the name match. Is there a more elaborate process that's envisioned here?

ASSISTANT SECRETARY BAKER: We are actually looking at the question of whether we can take over the process of checking the IDs. That actually, that process kind of to my surprise is not a TSA function, it's not a government function, it's performed by the airlines who hire somebody to stand in that part of the line. That's the one part of the screening process that was not taken over in the wake of 9/11, but we are looking at the question of whether we can't take that over and bring to bear some more sophistication about the kinds of ID forgery that people are engaged in. And some of the other observational responsibilities and techniques that would make it more likely that you could identity not the weapon, but the hijacker.

MR. HARPER: And assumedly you'd use the machine-readable zone on the REAL ID card to do this efficiently.

ASSISTANT SECRETARY BAKER: We haven't decided to do that and I'm not entirely convinced that #NAME? zone. That just gives you the information. And so if you're trying to look for security, you might be better off having a hologram checker than having a reader for the machine-readable zone.

MR. BEALES: Ana Anton.

MS. ANTON: Thank you. Honorable Baker, thank you for coming and taking time with us today. Just as a follow-up, it seems to me that relying on the form of the ID rather than the content ill inevitably lead to weaker security. So just as a point. I think when the ID is actually studied, that's when we have stronger security.

Any database presents privacy risks and when those databases are administered separately and linked, these databases can be exposed at an insecure point in any of the databases who are along the communication pathway where all the information is exchanged. The NPRM implies that there is increased security, but fails to provide specific guidance to the states. And also doesn't really provide any security policies for

sharing information in the driver's license databases. So the question I have for you and your office is what efforts have been made to create and ensure that there are security policies in place that are verifiable and auditable in these systems.

ASSISTANT SECRETARY BAKER: A couple of responses to that. I would certainly urge the states to adopt high standards for security for the data that they have, recognizing that it is data that's available many other places as well. However, the statute didn't require us to set those standards and impose them on the states, and the states have with some reason objected that this is an unfunded mandate which they estimate and we are not in a position to disagree on the order of $10 - $15 billion over the next five to ten years. And if we were to say oh and by the way we've got some other stuff we want you to do too even though it's not in the statute, I think their response would be okay, so more unfunded mandate. That said I think we are going to encourage them to do this, but ask them for a plan. We will at a minimum use the bully pulpit and we're taking comment on that and it may be that the comments will persuade us we should do more. But I'm confident the states will give us comments saying we should butt out.

MR. BEALES: Neville.

MR. PATTINSON: Thank you Honorable Stewart Baker. Thank you for coming today.

ASSISTANT SECRETARY BAKER: Thank you.

MR. PATTINSON: I'd like to question you regarding the improvements you think REAL ID will make to the identification credential. I'm really having a strong time understanding how that's achieved. Certainly the emphasis appears to be in the NPRM about looking at the process of enrollment vetting, but the usage environment when presented at a checkpoint doesn't seem to be strongly addressed according to what we have today. So there are precedents already in many of the systems of the federal government with electronic passports, CAT cards, PIV cards, TWT cards that are using identification technology which is a stronger form. I don't see in REAL ID how there is a chain of trust from the credential that's being presented to the inspection officer to really prove this is who the person really is. There's no biometrics other than a facial photograph and even today on driver's licenses they don't generally look at the person or the photograph that intensely. There's no essential ability to authenticate the document at the point of check. You've got to do a visual inspection. So my view is that we're really moving nowhere on REAL ID to improve the credential beyond what we have today and we're still going to allow the counterfeiting to take place which is rife today, completely undermining all the effort that the DMVs will take on to improve the vetting and background checking on the basis that you can go and make a fraudulent card and present it as a fraudulent identity. So I would like to hear your response if you could.

ASSISTANT SECRETARY BAKER: Well, I think - I appreciate what you're saying and I'm not sure I would disagree with all of it. It's not easy to build a complete system when you're starting with an existing system. There's a backward compatibility issue. There's a sunk cost issue. And we were struggling with a system in which the states have already decided and have often entered into long-term contracts with suppliers of the equipment they use to create the licenses and the like. So we're not writing on a clean slate and that means that whenever we said gee, don't you think that you should stop using laminates which are easy to photo-substitute and move to a different kind of cardstock the response was are you kidding? I just signed a 4-year contract, you're asking me to throw out all my equipment, you're making a big change. And so the backward compatibility issue was quite substantial. That said, I think we are pushing for improvements in cardstock. That will make it harder to photo- substitute.

And authentication of the document, I understand what you're saying that it isn't going to be as easy as we would like to be able to actually authenticate the document in the field. I wonder if that's entirely true. For at least police agencies it is possible because they'll have connections to verify that the license was issued at least by their state and very likely by others so that for police use it will be possible to authenticate the document on something other than the face of the document. If the complaint is well merchants won't be able to do that as easily, I think that's fair. But it might be better if people said we'd like to be able to authenticate these documents electronically to prevent ID theft and as soon as everybody agrees with me that REAL ID is a bulwark against identity theft we can take a look at that. Right now I think we're still struggling with getting people to see it that way.

MR. BEALES: Tom Boyd.

MR. BOYD: Thank you Howard. Welcome Stewart. Nice to see you again.

ASSISTANT SECRETARY BAKER: Thanks.

MR. BOYD: I can confess to a bias in preferring to see statutes expanded by way of a vote on Capitol Hill as opposed to an expanded regulation. And much of what we've heard this morning by way of criticism has focused on the potential expansion of the REAL ID regulations, in particular the ability of the Secretary to expand beyond the primary three purposes for which the REAL ID is to be used. What would be your reaction to limiting or eliminating that potential to expand the coverage by way of regulatory decision on the part of the Secretary?

ASSISTANT SECRETARY BAKER: We've taken a pretty minimalist approach in terms of going beyond the statute in many areas and that was certainly one of them. I'd be cautious about saying okay, those are the only uses that we want to allow. As I said, we've just recently discovered how serious the problem of identity theft can be in an

immigration context and I'm not sure I would say we shouldn't be able to say that a REAL ID license is something that people ought to present once they're available to demonstrate that they are in fact who they say they are. So I'm not sure I would want to completely give up the possibility of addressing additional problems of identity theft with the REAL ID, but you know we were pretty clear about taking a minimalist stand in the NPRM. And while I'm sure we'll get comments, I'm kind of guessing that expanding it isn't going to be the burden of most of the comments.

MR. BOYD: Thank you.

MR. BEALES: Lance Hoffman.

MR. LANCE HOFFMAN: Afternoon, Stewart.

ASSISTANT SECRETARY BAKER: Hi Lance.

MR. LANCE HOFFMAN: You've got a tough job given the hand you were dealt and the law that was passed.

ASSISTANT SECRETARY BAKER: Somehow with a start like that I think you're going to make it harder. (Laughter).

MR. LANCE HOFFMAN: No, I'm going to make it easy. I just wish you had spoken more to the question immediately asked just a moment ago because in terms of the so- called minimalist stand, especially in light of you know current events in the media, sometimes a lot of people don't believe that it's going to be a minimalist stand, although I have every respect for you and what you're saying.

I'd like to speak more to the - especially to the lack of requiring encryption in machine-readable field. That seemed to be that's an obvious thing to do, but yet not only did the department not go there in the NPRM, it didn't even go to federal standards of just anything. In essence as a couple of people who testified mentioned, in essence it was punted to the states thinking that miraculously the states are going to do better. Comments?

ASSISTANT SECRETARY BAKER: Yes. I don't know how much of this ended up in the NPRM, but we thought pretty seriously about encryption. And we're certainly not religiously opposed to it. But we have to remember that the principal reason for the machine-readable zone is so that when police encounter people on the road they can quickly and without typos and without making mistakes that could lead to people going to jail that shouldn't go to jail get that information into a central authority and back out to them with an answer, is this somebody I should be worried about. And if you impose encryption requirements that make that exchange of information difficult, you're underline, not improving, security associated with the driver's license. We don't want to do that. Now, of course there are ways to say well you have encryption but everybody

uses the same key. But we know what the problem with that is. You know if Sony can't keep their keys secret, I don't think that the DMV can do it either. And so using a single key would I think end up being compromised and then you'd have people making quasi-black market machines that use the key to read the data. We're open to encryption if it works first for the policeman who does the traffic stop and then actually provides the security that is promised. But I think there are some kind of practical questions that have to be addressed before you can decide that you've got that kind of an encryption system.

MR. BEALES: Are there federal uses that are contemplated for the machine-readable zone? Mean is the department planning to places where it would collect information that way, or to read that information?

ASSISTANT SECRETARY BAKER: No. There was a suggestion that we consider doing it at the checkpoint, but I wasn't sure that it would actually would make a difference for the job that has to be done. And I'm not aware of any current plan to try to use those machine-readable zones for federal purposes.

MR. BEALES: So from the federal perspective at least there's not any particular reason why that needs to be standard format or standard information or anything like that because there's not anything you want to get out of that information.

ASSISTANT SECRETARY BAKER: I think that's probably right. The states are interested in trying to standardize it for obvious reasons. It dramatically lowers the cost of the readers and that's you know in our interest too to have good effective law enforcement. But no, actually I don't think - as far as I know the federal government doesn't use these 2D bar code systems. Certainly DHS doesn't. We have any number of machine-readable systems for identification and ain't none of them this. So if we were picking it for federal reasons we would have chosen a different standard and then we'd be busted, but we weren't interested.

MR. BEALES: Lisa Sotto.

MS. SOTTO: Stewart thank you for joining us. It's really nice to see you again and we hope Paul is serving you as well as he served us.

ASSISTANT SECRETARY BAKER: Yes, well he's serving himself too. He's spending the week in Italy.

MS. SOTTO: Oh, nice. Well, send him our best. I'll have to catch up with him. Just to sort of add on a little bit to Lance's question and take it from a slightly different perspective. So right now we've got driver's licenses that are readable in some states and we know that businesses are using that data, keeping that data. Now we're going to have essentially more uniformity and a business that wants to have 50 states worth of data on how many, 240 million license-holders could in theory at least put together that sort of a parallel database. Barry Steinhardt used the term parallel database. I don’t worry so

much, and maybe I should, about the security of government databases. I'm one of those inherently trusting individuals, whether it's state or federal. I worry though deeply about the lack of security in corporate databases. And we've seen both government and corporate databases being infiltrated. And the hackers and the bad guys are getting more and more sophisticated. They're incredibly talented. There's no question that they're going to come up with a way of getting at this data. And it just seems to me that there is the potential at least of creating this much more robust and interesting database than has been created in the past.

ASSISTANT SECRETARY BAKER: You know, I see the theoretical risk there, but I'm not sure I see it on a practical level. Because it depends on saying if you standardize the already you know fairly common sets of machine-readable zones, businesses will be able to do a better job of collecting that information and that will lead them to collect it for 240 million people. But the fact is 90 percent of the driver's licenses you're going to see in a particular state are probably from that state. If you wanted to gather information in that state you get a reader that worked for that state and you'd gather the information and if you did business in 50 states you'd get readers that worked in each of the states that you were operating in and gather the information. But as a way of gathering this information it doesn't sound like a very cost-effective mechanism. Hell, you just go buy it. And so I'm not sure that they're likely to acquire it in the fashion or that we're going to be making that much easier. And then I'm wondering what a hacker gets if he breaks in and gets that information because it's pretty anodyne information. Now, there are people for whom this is information that has to be absolutely secure, whether it's an abused spouse or somebody in the witness protection program. But it's a relatively small number of people and I don't think you could make a lot of money as a hacker breaking into systems and then trying to sell the names of abused spouses and witness protection program participants. So given that, I am just not convinced that we - that there's a plausible way in which the things that are required by this set of regs will actually lead to insecure databases that are the subject of attack. This is information about us that's probably available in dozens of places today without much difficult because we've given it up and given it up and given it up. And once you give it up once it gets around. So for all those reasons I'm not completely convinced that we're adding to the risk in commercial databases. That said, I kind of share your concern. Commercial databases aren't all that secure most of the time and we've all gotten breach notices telling us - you probably advise the people who send them out - telling us that our data is potentially compromised. I do think the market will work on that as well, that sooner or later people will get tired of getting those notices and shift to people who can offer better protection. But in the long run we're not going to get security through obscurity of our personal data.

MR. BEALES: Stewart, I want to be respectful of your schedule. As people have more questions I'm sure, but –

ASSISTANT SECRETARY BAKER: I am past due at a meeting on the Hill, so."

MR. BEALES: All right. Well, we thank you very much. This has been very helpful. We appreciate your time and –

ASSISTANT SECRETARY BAKER: I actually am going to be rude to somebody else if I don't leave now.

MR. BEALES: Much better to be rude to Jim. (Laughter)

ASSISTANT SECRETARY BAKER: That was kind of my thinking, yes. But send me a note, I'll send you an answer. Okay.

MR. BEALES: Thank you very much. With that we're going to break for lunch. Please be back at 1:15. We will get started promptly at 1:30 with our afternoon speakers and remember if you want to make a public comment please sign up at the registration table as you leave the room. Thank you.