

>> Moderator: Because although you cannot see her, I am reminded that we need to leave this space and time to allow time to set up for the press conference at 1:30. They need to get the room set up for that. We need to move quickly around here. But we're really ex quizz Italy positioned because so far this morning, we've been talking about strengths and weaknesses of different approaches in a meta sense in a large theoretical sense of how we deal with identity. And this panel will speak more specifically about how those challenges have been addressed and dealt with or the challenges that they still present in existing systems that have been implemented or that are being planned to be implemented from birth certificates to passports to drivers' licenses to private industry authentication issues. And so let's just get right into it. As with all the other panels, it's quite a distinguished group of participants. Our first speaker is Garland Land who is the executive director of the national association for public health statistics and information systems. He has been at NAPHS since 2005 and actually he fought from the frontlines when he was a state registrar for vital records in the state of Missouri. Our next speaker will be Patti Cogswell. And she is on temporary assignment of the acting associate director for the screening coordination office at the Department of Homeland Security. And her portfolio includes harmonizing policies and investments for identity management and people screening activities. Our third speaker today is Toby Levin who is perhaps the highest credential that she's for merely of the Federal Trade Commission, and it's wonderful to have her back. Toby is also if the Department of Homeland Security. She works in the privacy office advising the chief privacy officer and internal and external privacy matters and she's very much involved on the privacy issues related to real ID. David is a director of the general services administration. Now this is a difference between government and the private sector. Will you ever have anyone at your bank

with a title that long? But he's going to talk to us this morning about government implementation of HSPD-12, which has to do with the standardization of federal credentials and how that is coming along. And again the challenges that we see in that respect with the whole authentication univers And also is John Byrne from the bank of America. He recently joined the bank of America after spending 22 years with the American bankers' association. In 2007 he became regulatory relatio executive. Very nice. Elegant. And is responsible for working with if he had ran Allstate agencies, nonindustry organizations on o various regulatory and risk issues. We thank you for being here.

We have two other participants we call our discussants. Sheldon is with AMVA. He's on the front page. Seldon, he's the Vice President of law enforcement for the American vehicle administrators.'s e related to the implementation of real ID and general authentication issues. He also probably brings a perspective on the need in certain contexts for a centralized database because his background is law enforcement. He is an integral member of the team here and our approach on identity management. Our second discussant is Ari Schwartz. He is the deputy director for the center for democracy and technology here in D. C. He's active in expanding access to government information via the Internet. As we heard in our first panel with Simon and Gus, probably the largest issue that we deal with in developing appropriate identity or authentication approaches has to do with privacy. So he will be a key stakeholder and we're looking towards his insights on the issues that have been discussed so far.

So the sequence of our panel is first Garland will speak, then Patty, Toby, and David and John. The Final Four have PowerPoint presentations that talk about some of the high level issues in their authentication issues, and then we'll have Ari and Seldan speak. You will notice that I'm the only one that doesn't have an identity. So as people

get up, I will take their identity.
identity?

>> GARLAND LAND: I'd like to give you a little bit of a background on the vital statistics in the nation, some of the changes that are going on. Some of them are automated activities and some are other changes. The state vital statistics for the United States is a state system. It's not a national system. Not a federal system. It's governed by 57 jurisdictions, all the states, the territories and D. C. and New York City. And those are where birth certificates are registered. There are over 6400 local jurisdictions in addition to those 57 that issue birth certificates. What kind of holds that system together is there are model laws and model regulations that the states have passed that are somewhat similar from one jurisdiction to another but not exactly the same. The birth certificate has been labeled as a greater document because if you have a birth certificate or have one, you can get a passport, you can get a Social Security card or you can get a driver's license. And that basically is what establishes, for the most part, identity to some extent in the United States.

The 9/11 commission realized that there are serious problems with the birth certificate system in the United States, and there have been two federal laws now that have passed that are trying to address some of those issues. One is the intelligence reform and terrorism prevention act and those regulations are going to come out in the fall of this year. And those relate directly to vital statistics operations. And the other is the real ID act and those regulations just came out this last month and there will be speakers talking about those. But they also impact our operations.

There's basically two ways in which birth certificates are used to create false identities. One is a falsifying of the birth certificate itself. The other is to use somebody else's birth certificate for false identity purposes. So let me talk

briefly about each one of those, how those occur. And there's many other ways in what I'm going to talk about but just to kind of give you an overview. The first is that some people create a new birth certificate all on their own that looks identical to a state-issued certificate. And if there's not a careful adjudication process going on, they are accepted by the agency as a valid birth certificate. Or some people obtain a birth certificate and alter it. Change the name. Change the date of birth in some ways and they're getting very good at this. And so it creates a whole new record by altering a valid record that was issued. Another way is in some cases people don't have a birth certificate. They were born at home or their birth certificate was never registered. Very small percentage of the population but it does exist, particularly for older people. So there's a process that all states have where they will create a delayed birth certificate where the person has to provide basic information to establish the facts of birth and then a new delayed certificate's created. Well some people have figured that process out and create false-- provide false information to create the delayed birth certificate. So those ways and probably many others are ways in which fraudulent records have been created in the. There's also ways in which people obtain someone else's birth certificate and use it for false identity purposes. Probably one of the best known is they'll look in the obituaries, find a person who just died, particularly an infant that hasn't created an identity yet, and then they will apply for that birth certificate on that infant and then assume that person's identity. An open record state, we have about a dozen states in which it's perfectly legal for you to go into that state, request anybody's birth certificate and they will give it to you. And then you have that person's birth certificate and then you can use it for whatever purposes that you want to. Obviously that's a serious issue. But it does go on in a lot of documented cases of people assuming other people's identity through an open record sta

There is-- if you go into my former vital records office in Missouri and if you know enough information about me, my mother's maiden name, my date of birth, my name, where I was born and so forth and

fill out the registration form, you can get my birth certificate. And that occurs also sometimes. Where if you just have enough information about somebody else, even if it's a closed record state, they will issue a copy because there's no way for them, particularly through the mail, to identify who you really are. Birth certificates of course are stolen. There's a known ring between Puerto Rico and New York City where birth certificates are stolen and sold in New York. People sell birth certificates. They sell the children's birth certificate because they need the money.

They are actually giving away the identity of their own family members.

So as you can see, the problem's complex. It's not a simple issue. If we just do this one little thing that we can solve the problem of identity theft with birth certificates.

With the intelligence reform act, we made several recommendations of how to close some of these loopholes. All I can speak to is what we have recommended. The regulations come out this fall a we'll find out to what extent those regulations are implementing what we had recommended.

One is that we feel that all states should be restricted states. There shouldn't be closed records-- they should be closed record states.

You should only be able to get your birth certificate for yourself or for your immediate family member.

We think that there needs to be birth death matching. So if you request a birth certificate, it's noted in the database that this person has died, if they died, and then that birth certificate would

not be issued. If it is issued, it will be indicated that this person is deceased.

That goes on to some extent now, but not totally in all states.

There's recommendation in terms of security papers. Some have very good security paper standards. Some have basically plan paper that they issue the birth information on. So I'm sure there will probably be some standards coming out in terms of security paper.

This 6400 issuing locations I talked about earlier, we think that's a vulnerability of the system. The more people who are issuing at a local level makes it much more difficult to assure that there's consistency throughout the United States. We can say that there should be one at the local level.

The final area that I want to just briefly speak about is our electronic verification of vital events. They're auld ef very.-- Evve. This is developed several years ago for the Social Security Administration. It was piloted with Social Security Administration. It's been piloted with about half a dozen drivers' license bureaus.

Basically the system operates in this manner. You walk into

let's say Social Security Administration or into a driver's license bureau or any other adjudicating agency, but those are the two that we've worked with up until now, and the individual gives them a birth certificate. They don't accept that birth certificate on face value. Theysen-- they then enter two key pieces of information from that birth certificate. Name, date of birth or state number or the date the record was filed in the state. Those-- three of those four pieces of information are entered into a web-based application. A message is then sent to the state where the

person was born. And then there's a 1 to 1 match to see if that person's record is indeed on file.

And if all of those pieces of information match up, it is sent back to the adjudicating agency indicating yes, this is a valid birth certificate.

If there's any of that information does not present back, it will give them a hint that says check out the date of birth. Maybe you've transcribed it wrong and then they can try-- we don't give new information back to the agency. They just

have to see if maybe they made an error or something. So that's the system that's mentioned in the Real ID Act. That in the future when people get their driver's license, they will have to present a birth certificate. That will then have to be validated. We are also working with passport and we're working with the office of personnel management, federal office of personnel management and we're working with the Social Security Administration.

We have about half a dozen states who have Evve-- have been implemented with Evve with funding that we expect to roll that out to all the states. And then any agency that has an agreement with us, we will allow them to have access.

So whether or not that's a centralized system or decentralized system, I guess you have to debate that. It's not a centralized system in the sense of a database in the sky or the Federal Government but there are these 57 jurisdictions I talked about that have the birth certificates that are recorded in their jurisdiction. And if tapping in to see if that birth certificate is on file in the particular jurisdiction.

So, in closing, I think there's a lot of barriers to improving the systems out there. These are governed by state laws. And so whenever there's inadequacies, we have to go state by state to effect change at the state level as opposed to one federal law.

There's inertia, of course, in any government enterprise. And we've always done it that way as a big problem. And so making changes sometimes are difficult because of that.

And then obviously there's costs involved in any of these changes. The Evve system is actually pretty cheap to install in comparison with a lot of other systems, in compared to what the Real ID cost, Evve is cheap, but still it does take money to implement and other changes that I talked about. So those are things that are affecting our states right now that we're trying to work through. Very conscious for the need for change. And very supportive of trying to make changes that are necessary.

>> We can get through the slides next. We seem to

have John's slides next. There we go. Okay. Yea
>> PATTY COGSWELL: The first thing I want to do is set the framework and standpoint from a GHS perspective. At the end of the day, we're responsible for screening. We screen individuals in very,

very large numbers. And why do we do the screening? Number one to identify those who pose a threat. Second thing is to find individuals who are ineligible for something they're applying for third frankly is to find individuals who have violated the terms of that status, privilege or license that we have provided. In that context, you see the kind of numbers we are dealing with. frankly the different environments from which we conduct the screening opportunities. I am with the screening coordination office. I'm so new people don't know what I do. This is a quick plug who we are and why we are there. What are we doing? The first thing is really looking at creating interoperable environments. I really enjoyed some of the factors brought out by the earlier panel

and I'll talk about them a bit more as we move into the next slides but also it's talking about finding ways to take initiatives and move them from the policy perspective in its implementation enacted to the various pieces of legislation to which we are responding.

One of the first things we have done is a credentialing review. The objective is to look across a life cycle of interactions with individuals but also look across programs. We want to look at

opportunities for fewer credentials not the discussion we had earlier about why is there not every single store still issuing their own Visa card, version of a Visa card but now there is a Visa card?

We want to look at opportunities to say there should be fewer credentials, not one, but fewer, so that they make sense. We want to look for smarter vetting. And look for a way to simplify interactions of individuals with the Department of Homeland Security.

With that, we have looked creating a series of

principles associated with these activities.

These principles are really designed around a couple different key pieces. First vetting, associated with

like risks and like usage should be the same. We should look at a way to make sure frankly that at X level of risk of an encounter you supply the same information under the same type of vetting so that you frankly if you're one of those people who is subject to three different DHS programs, you can go through it once. If you are only subject to one DHS program, you only have to go through it once.

We also want to look at immigration, electronically. We see a problem with using a card, a physical piece of information, as a way to communicate amongst DHS. There is too great a possibility, frankly, that someone could try to create a fraudulent identity.

We also want to look at verifying the entitlement to a license, privilege or status using technology, the signer enrollment programs so that we can more often enroll once and reuse information where appropriate. And the last thing is really to create a good robust opportunity for redress so the individuals can come in, identify the information and make corrections where they need t

As one of the examples since I was specifically asked to talk a little bit more about the travel contracts is the USViesite programs. It is one of the most well known programs out there using biometrics. The life cycle idea. It means you expect to come in contact with an individual through multiple different ways, multiple different programs and frankly multiple different agencies. Pre

entry at this point in time is real buy the department of state. I forget who really said it at the earlier panel, the need to prevent people for re-applying, double dipping.

One of the biggest things we've seen through the creation of the bio Visa program is we've stopped individuals from shopping locations to get Visas. Individuals who applied in one context were denied

cannot go to another location with a new identity and try to get a Visa in that new identity. The second one frankly is more of that context. Making sure that we can still identify an individual across life cycles. The person we see at that preentry strag that can get that Visa, we can say you are the person to whom state department issued that Visa. This is very important because frankly one of the biggest issues we used to have is called Visa wash. Literally they take that piece paper, scrub off the photo, replace it with other information. We can now say look, in our system, we show that the person to whom this Visa was given is a woman. You're not. The name is comple different. And, gosh, she was 12 and you're 47. We have a problem that we have been able to solve through this identity management context. We also look at them and cross further. Status management. One of the biggest issues we ran into frankly that we're excited about is we're current vetting. Quite often the paradigm used to be you vetted someone at a point of encounter and only at that point of encounter. What we have is an individual may have no derogatory information at the time we captured them at the Visa application, be clear upon admission, but later they come in contact with law enforcement. And now they're wanted by pick your favorite state agency. Because we have a path and a mechanism to receive information, we can then check that new derogatory information against the enrolled population. This means that an individual who now has violated the terms of their admission to the United States, we can identify them and we can then take appropriate law enforcement act. Next I want to talk about the western hemisphere travel initiative. It is a little different context in that its focus, again as some of the other panelists have discussed, about the terrorism reform and prevention act. How do we set up an environment so that we don't have 8,000 different birth certificates and all the different things coming across-the-boarder? How do we look at making it easy to identify

people who are compliant so that there are no issues so we can focus our time and attention on those who

are come compliant? How do we find the risks?

The other piece frankly is a way to do checks.

The key is looking at an environment that will facilitate the travel across-the-boarder because t country thrives on that kind of economy and transmission between countries.

Some other things I wanted to really focus on here in particular is some of the recent contexts about the department of state's potential passport cards that we've had a recent set of regulations discussing and that the comparable DHS regulations that go along with them about what documents will be expected for border crossing.

Right now the proposal is for that card to have a machine readable zone, that lovely little thing with all the care ets you see at the bottom. And a vicinity RS. Longer range read RS. The key her is on the radio frequency is a number. The number doesn't mean anything. It's not a number that can be generated from anything in specific. It's truly a random number issued by our system. The k here is really that we are able to take that number and tie it to a record about you so that when you come across-the-boarder, there is a place you come to get into the queue to come up to the booth.

It reads that card or frankly several cards that are in a vehicle and prepositions that information so that customs topples and border protection officer. They can then see the photo, this is who was issued to. And all the information about background checks that have already been run. So that the officer can know right then and there does this person present a threat or is this no records, no issues?

That's kind of how we've been approaching it. In particular I wanted to note two items. This is the next generation of radio frequencies by the technology that we have e been using since 1995 on border.

The second thing is we intend to issue it with a sleeve. This sleeve is intended to block all

transmissions off the chip. So if it is out of the sleeve, you can read it. When it's in the sleeve, it is not readable.

The next item I wanted to cover is the e-passport. Also back in that travel context. Again as part of the intelligence reform and terrorism prevention act, I'm sorry, this was the enhanced f security act, there is a requirement that DHS be able to biometrically compare and authenticate different travel documents between the 27 different Visa waiver nations. The way we approached this in

the standards set by the international civil aviation administration is through the creation of what's called a proximity radio chip. Sometimes also called the 14443 chip for people who are real into it. The way it works is a couple fold.

Number one is that machine readable zone down at the bottom of the document must be read to unlock the chip. You can't just read the chip off the document. In the vast majority of countries have positioned how they are producing the document, that is how the U.S. is producing its document. In addition, the U.S. is doing something beyond that. They also put protective materials into the cover of the book. So that when the book is closed, the chip cannot be read. It has to be opened to be able to be read.

The last thing I wanted to show you is just some examples that you can see in use in the border community. So the first one up there on the top left is a standard reader reading those characters you can see how that works. The bottom two are the two biometric capture devices currently in use at our borders. For those for whom we take a photo and a fingerprint. The document in the middle that e-passport reader. So you can see you have to physically open the book, put it hard into the reader, so it can read it, and the chip. And the last one in there are the two pin print slap devices that we are currently looking at prototyping and piloting coming up in the relatively near future. The state department is already in the process of using them, as well.

I think I covered everything.

>> I have about five minutes to convey to you the real ID, which is an impossible task. So buckle your seat belts and drive warp speed. I hope you'll take time to look at these slides, which will be on the FTC website independently at your convenience. The Real ID was basically the recommendation of the 9/11 commission to affect drivers' licenses. All but one of the 9/11 hijackers had acquired some sense of U.S. identification, in some cases holding multiple drivers' licenses.

What does it do? It sets a minimum standard for a state-issued licenses. It increases the security and integrity of state-issued licenses. Makes the department stronger, safer and better protected against terrorism and identity theft. Respects authority and functions of the state which traditionally have done licensing and increases confidence that people are who they are who they say they are.

It creates a minimum Standard for licensing and ID cards for official purposes. And the act and implementing proposed regulations defines that as accessing federal facilities, boarding federally regulated commercial aircraft or power plants and then we have included comment on any additional purposes.

I should mention that the proposed regulation was published on March the 9th and the comment period closes on May the 8th.

At a minimum, each card must include this list of data elements. And applicants are required to provide a number of documents. This slide indicates those documents that are required to demonstrate citizenship.

And in addition to providing those documents, individuals applying for licenses will have to document name change, establish the date of birth, which can be through one of the prior documents, establish Social Security Number if they're eligible for Social Security; if not, evidence of why not? Establish their address of principal residence and establish a lawful status in the U.S. Very importantly, states, then, with this documentation must verify the data. And of course

with training, DMVs are very experienced in trying to assess whether a document is authentic or not authentic. And reader documents are obviously very difficult in terms of authentication. But through the Real ID, the statute and the implementing regulations, call for the data on these documents to be verified with the issuing agency. So I think the best way to demonstrate that is to look at this slide.

On the left-hand side, on your left-hand side, demonstrates the state's DMV processes in terms of authenticating individuals. And on the right hand side, the data verification as it will occur.

There are three key balloons there. I guess the top is the employee clearance. Certain DMV employees will be covered employees who are involved in manufacturing or issuance of these credentials will

have to undergo a criminal check. That will be done by the FBI. Then the states will check against four federal agencies the applicant data. And beginning with the department of home LAN securities-- home land security, I can't remember the acronyms. The student and exchange visitor information system, which applies to students, exchange students and visitors, academics. The systematic alien verification system. And then also check against the Evve system which was talked about earlier. And then the department consolidated counselor database. And then the pas information electronic system. And then the Social Security Administration's Sstalls system which is the Social Security online verification system.

Now, not all these systems are available to all the states. There are pilots with regard to the Evve system. The department of state systems are not available electronically to the states of the the Department of Homeland Security will be working very hard with the federal agencies to get these systems up and running and available to the DMVs. Many of them are available today through AMVA and we'll be hearing more from Seldon. States can check directly to single checks against DHS, for example, or SSA, the Sstall system. But

the department has proposed exploring a federated query to allow the states to do this checking in a much more streamlined fashion.

And then finally the state to state data exchange and that is to the fact under the Real ID act that you can only have one real ID. So that states when you apply will want to make sure that you don't hold a real ID license in another jurisdiction.

And I should stop it for a moment and say that the concerns have been raised about whether or not people will be able to fly or enter federal buildings if they don't have a real ID after the effective

date of the regulation. The answer to that is yes, you will be able to enter buildings. You will be able to fly. What it means is that if you were going to present a driver's license for those official purposes, it will have to be a real ID license. But facilities and airplane carriers, when an agency that takes over all the functions in the future, will want to see a real ID driver's license. But they may also accept passport. Or you may have to go through additional screening in order to travel or enter a building.

Now, to the minimum security features that are to make the card itself more tamper-resistant, I'm unwilling to say tamper-proof because I think that sets the bar too high.

Some of these features are currently being used in a lot of states. Some states may currently have almost all of these features.

Now, to the issue near and dear to my heart and to the office of the department's privacy office, or the privacy considerations that are raised by the Real ID.

When the proposed regulations were released, we also issued a privacy impact assessment, which is posted on our website and the link is provided the end of the slide presentation. And it identified the following key privacy issues. Does the Real ID Act and regulations create a national identity card or database? Well I think the answer is it depends. It will depend on the use of the unique identifier and what the nature of it is. Will it be unique to a state or will it be unique across the-- across all jurisdictions? What will be the

nature of the query of the federal reference databases and the nature of the state to state data exchange?

Secondly, how will person information required by the act be protected in the state databases from unauthorized access or use?

Third, how will the personal information stored on the machine-readable zone, which is mandated by the act, be protected from unauthorized collection and use? The end carrier proposes a PDF bar code 417 which is currently being used in I think about 45 jurisdictions. It does not-- it's not currently encrypted or protected and may be read by 2 D bar code readers that are fairly common.

And some

of you may be aware that there are news reports of the 2 D bar codes being scanned at bars, convenience stores where they're appropriately doing age verification but possibly also downloading information from the 2 D bar code.

So the MPRM seeks comments on how to protect the information and notes the benefit of encryption but asks-- reasonably asks about the feasibility of such a system given the need for law enforcement quick access to the information on the bar code.

And then finally how do the requirements for photograph and address on the ID as well as a DMV employee background check, which includes criminal and financials had I impact on privacy?

Importantly the MPRM proposes a comprehensive security plan for DMV facilities. And this is significant because within the elements set out within the NRM is the information that there be information

protection and security safeguards. So we've invited comment on what those should consist of and demonstrate implementation of best practices to protect privacy based on fair information principles. Of significance is the architecture of the data system. We want to build on some of the current operations certainly because the significant cost involved in implementing real ID, they've been estimated at anywhere between 11 billion and 23 billion dollars. So there's a sensitivity with regard to the building of the architecture in a cost-effective way for the state. But we want to

that this architecture in such a way that it minimizes data collection and centralization to the extent possible and protecting the privacy of personal information that's collected and maintain We're concerned about how the data systems will be governed. And we want to make sure that there are privacy protections and security safeguards that reflect fair information principles. And this slide, since we identified some ways in which those principles can be implemented in an ID system such as the real ID, these were not identified in the MPRM, but these are ones that our office

applies in all the work that we do.

So the last two slides are the milestones. And I would just bring to your attention that the effective date is May 11, 2008. We don't expect all the states to be able to be in compliance by t date. So the MPRM proposes a five-year phase-in implementation. We hope some states will be up and running for the 2008 deadline. More to come by in full compliance by 2013.

So I look forward to your questions. And there is a link to the MPRM and the privacy impact assessment.

>> BETTY BRODER: Thank you, Toby. The next speaker is David from the general services administration. Thank you so much.

>> David: Thank you. I will very quickly go through what the requirements are as well as some of the background for the Federal Government identity program which was implemented under presidential directive HSPD-12.

Okay. HSPD-13 signed by the president in August 2004. Now, there are four key control objectives within the presidential directive that identity and the vetting of identity information is based o sound criteria. Those are specified in a standard published by the national institute of standards and technology called BIPS 201. That standard, the program called personal information verificati program or PIV and HSPD-12 really can be used synonymously.

The second key point is that the cards are

strongly resistant to tampering and counterfeiting. There are extremely secure counterfeiting measures deployed on the cards. These are smart cards with coshed credentials. I'll go into what that is. It is required that these are not used as flash pass but are used to validate and authenticate identity electronically. There are multiple use cases for that electronic authentication. And you heard a lot about centralized and decentralized systems but the cards are required to be issued by issuers whose reliability is accredited through a process. I'll talk about how that is being done across government.

Key milestones. President signed the presidential directive in August 2004. This was given six months to establish the standard for the Federal Government. They met that time frame.

The next key milestone we had was the identity vetting portion of the standard to be implemented in October 2005. The identity vetting standard requires both controls in the enrollment process as well as background checks of all individuals.

Background checks and background investigations. It applies the presidential directive applies to all federal employees and contractors outside of the intelligence community.

In October 2006 was the next key milestone, which was the initiation of issuing the badges, the cards for all agencies and departments to replace whatever badges are currently being used.

Next key milestone on this chart is October 2008 where we will have converted all of the current employees to that PID program, the PIV program. We're not done. But these are just key milestones to get

the credentials into the hands of verified individuals. What this chart is intended to show is that we don't see authentication of identity as just one flavor; but, in fact, depending upon the level of access control that's required. And the assurance authentication that we support multiple levels of authentication. We see the HSPD-12 PIV card at the very highest level supporting multi-factor authentication if it's needed. There are other levels of authentication capable within the PIV card.

The card itself supports visual credentials. Well there's badge, there's picture, there's printed information on the card. The card supports the contract of a chew it. A number associated with e individual that's enrolled into the program that can be shared. Consider it like a credit card number where there's different fields within that number that have different meaning to the account holder.

The card supports PIN-based authentication in order to access information on the chip. It's mandatory that the card and the system support fingerprint template biometric on the card as well encryption-based asit mem Rick key credentials which are managed through authentication certificates. There are additional credentials and technologies that may be optionally supported on the card.

For across government, this is really about trust, supporting identity federation where identity management and vetting is supported by multiple agencies in order to trust this card has been prop issued and has been issued to, in fact, a vetted individual. That trust is mandated through the presidential directive. It's mandatory. It's mandated through the standard. As well as interoperable

technologies which allow information to be exchange One of the things that we talk about in centralized or decentralized systems may not be the key point. If you've got separate issuers with separate databases and you expect to exchange information,

you need to be able to do that in a meaningful, interoperable way. One of the things we did was identify 22 different categories of products required for HSPD-12 implementation to test against conformance to the standard, the FIPS 201 standard. We do that in laboratories today in published an approved products list. We require all agencies to use those products in order to insure that

data across systems can in fact be interoperably and meaningfully shared.

So where are we today? There's more than a dozen agencies that are implementing, consider them

stand alone or separate HSPD-12 systems. There are over 100 agencies that have said they don't have the technology expertise. They don't see the reason to implement a separate HSPD-12 system within their agency. They're looking to share infrastructure, to have an issuer, an agency, provide that service for them.

There are four designated shared service providers across government: Department of Defense uses defenseman power data center. Department of state services eight international agencies that are typically housed by them. Department of interior provides personnel services for 25 plus agencies.

This is a direct corollary to that. My agency, GSA, provides services available to any other agency in government, who plus agencies have signed up to us-- with us. We are testing all of the cards that are being issued by the 16 plus different HSPD-12 systems to make sure that the data the cards and in the systems, the back end systems, can in fact be shared in a meaningful and interoperable way across government.

Again, trust and interoperability is what HSPD-12 is all about. So that we can have common, trusted access to federal facilities and federal systems for all government entities.

And so the conclusion. In implementing-- in issuing the cards that comply with the standard, in converting all of our current employees to that program until October 2006, this is still just the start of how we manage electronic access and physical access for all personnel to systems on an ongoing basis-- on going basis. So this is the start of where we're going in Federal Government. It is

certainly not the end.

And one of the points on this chart is: Can other entities use the standards, the policies, the systems, the approved products that we have? We say it's a standard for the Federal Government, but can be adopted by other entities, as well. And we'll point to the approved products. We'll even test systems to insure that interoperability.

>> What I'd like to talk about is kind of the

practical implications of all these issues on something like the financial services industry and give you some sense how we are very dependent on obviously what government and private sector are doing regarding data. I'm going to focus entirely on our requirements at account opening, what we look at in terms of our requirements under something that we all know as the U.S. Patriot act.

Let me say there has been confusion for years that what we're talking about is know your customer. Know your customer is a different concept within financial services. Know your concept is what happens once you've been engaged with an institution and we look at transactional activity and make decisions about what sort of due diligence we have to do regarding your activity with us. Customer

identification programs are the regulatory obligations that our industry faces under the USA Patriot act. Briefly what we're required to do at our institution, we open up millions of accounts a year.

You can open up accounts in two ways. Online obviously or walking into a banking center.

Typically when you walk into a banking center, you're going to be giving us a document. When you do this

online, it will be nondocument verification. I want to focus more of my brief time on document verification because that's what we're talking about today.

The requirements under the Patriot act are basic. Basic but moving to the bank from a trade association, very difficult from a systems perspective to implement.

We're required to obtain four pieces of information. So when you open up an account with a financial institution, you have to tell us your name, your address, your date of birth and if you have one your Social Security Number. We have to obtain that information.

But under the regulations, we have to attempt to verify that information. We don't have to do a 1 for 1 match. So as you heard today, a lot of what we do in terms of "authentication" is really

dependent upon the information that's given to us after it's been processed from the states or the Federal Government. So that information is required to be obtained. We have to do a risk-based analysis on what we verify.

So, for example, we may decide that if an address doesn't match, that's not as important as the date of birth and whether the Social was validly issued. So banks go through their own decisionmaking regarding risk assessment. So that's something that's relevant because it's not a 1 for 1 match.

These requirements have been in place only since October 2003. Certainly prior to that you were giving information to financial institutions but it wasn't under a particular mandate. Key elements I've already mentioned is that we collect the data and we attempt to verify. I've been asked to talk about this because we believe it has a side benefit. We can arguably say that some authentication is done throughout this process because we've collected the information and tried to authenticate it through the documents you've given us.

If you're doing this online, we are going to use an outside private sector source, nondocumentary verification. If you're going into a banking center, you're going to give us some document. We accept what's required under the patriot act and that's a government-issued identification document with photograph or similar safeguard. That's what the regulations state. That could be a passport.

That could be a driver's license. It could certainly be a foreign-issued identification document. It can be, as we've seen in the press, a metricular card if it has a photograph. And obviously it's

consistent with the regulations. So the bottom line is we collect these records, we attempt to verify the information, and we have a process at our bank as do many other banks to repair deficiencies. If there's not a match, if there's a problem with the document, we go back and try to repair those problems. If we can't repair those problems within a reasonable period of time, most institutions will close the accounts. So that's sort of the check on authenticating identity. It's not one

for one, but obviously it's a help.

In addition, it's a recordkeeping and verification, we're examined. So we're examined by the federal regulators to show what our programs are. Typically they will go in and assess what our policies

say regarding what information we can collect at account opening, what's our verification process and go through and test the processes. We are also being tested by our internal audit function a some of us have our own self-assessment program.

So there's a way to see if the financial institutions are following the letter of the regulation and whether that process exists. The regulators

again are a test of our program to see if in fact they are following those requirements.

Jumping up here, one of the positive aspects that we believe here does assist in fraud prevention through both the use of the document verification and the use of external sources. So whether it's Dunn and Bradstreet, whether it's nexus, it is one of the processes that we will look through that the information we have is valid and can be tested through those processes. We think that helps in fraud prevention although most of what we are doing is to prevent money laundering and terrorist financing in terms of customer identification program. Challenges going in the future? Bottom it's risk-based. There's not a 1 for 1. So to depend totally on the bank if you're working with us from a third-party perspective, there are going to be some gaps because again we're required to obtain but we're not required to verify every piece of information.

We've also heard today the varying level of strength in all the documents, in the databases. So we're very much dependent on the drivers, the motor vehicle groups are doing, what the passport issuance processes are doing, what homeland security are doing, we're depending upon the government in those situations to do the hard work. So again it is what it is. It is only as good as the

documents we are relying upon. Social Security Numbers, for example, is not a 1 for 1 match. You

can see whether the number was validly issued, whether it's on a death master list. We certainly some due diligence there. So there's not a 1 for 1. So we're really dent den on the outside sorts. Foreign documents, when we started the debate several years ago, some drivers' licenses issued b states were pretty faulty. We've seen from a policy standpoint that's been improved dramatically. But foreign documents versus domestic documents, we can accept both. We obviously have to look to groups like AMVA and others to work very hard with their organizations to strengthen that documentation, but we have no control over that. Finally, the general impact on the economy. There has been some debate in corner and I was asked just briefly to touch on this. Throughout the process of trying to finalize these regulations, t was some debate whether or not financial institutions should be able to accept foreign documents like the Mexican me trickular card. Obviously that was a heated debate. It touched on immigration and other issues not related to identity. Although we have seen the public comment several times when they were asked should that be accepted, and overwhelming the public has said that should be an acceptable document. It's currently allowed. We do it accept it.

If that were to change, however, then obviously our requirements would change. Bottom line is: We believe that we do a lot of other things to help authenticate information. But from the stand of these regulations, we do think it has a benefit of helping the customer know that we have these pro Seth and programs to attempt to verify the data that they've given us.

>> BETTY BRODER: I think we could probably spend the rest of the day just kind of teasing out from each of these applications some of the challenges and problems, but I want to circle back to our first presentations, the famous Simon and Gus road show. I wrote down lots of things that we're not gentlemen was the first thing I have. And something like dogs to the dinner bowl. But the real point I want to circle back to is

Simon mentioned being at the sharp, jagged and bloody edge of identity policy. And whether we find ourselves here, kind of teetering on that edge, being

given a mandate, trying to implement it, but perhaps not being able to step back because of legislative mandate or being too close to it to understand what these other issues are.

I'm also thinking a lot about the concept of usability and putting consumers first, having a consumer-centric model so that it can be applied in a way that works well across-the-board.

And so with those things in mind, I thought I would like to ask Ari: Well my first question was what is wrong with this picture? But I think I will rephrase it a little bit. Simon and Gus also talked about consumer acceptance having to do with a trust. And who has the information and how it's going to be used. It's one thing to have an identity policy that is housed or owned, if you will, by a government entity that is associated with consumer well-being. People have a different reaction, at least they did in the UK, when the identity policy was going to be housed in the home department, which people associated with law enforcement, the government. And suddenly the comfort level was much lower. So with these things in mind, I wonder what your feedback is on the various

models that we've heard proximate this morning?

>> ARI: I'm reminded what Jim Harper said when he first started. He didn't have anything to criticize yet because there hasn't been anything put out there. There was so much that I wish Jim here to help me out a bit.

Let me point out that CDT has done the privacy principles that are out on the back table. They are in draft form. We want people to comment on them. That's sort of the basis how we evaluate the systems today. I think that there are a lot of positives that we heard from here and a lot of negatives on the privacy side.

Garland started off and went through let me start with some of the positives. Garland started off, he talked about birth/death matching and securing the documents, the breeder documents, et cetera.

To my those seem like very strong beginning points. Obviously the devil's in details, to some degree, but those are the types of things that may actually end up helping and privacy issues, cutting down on identity theft and other concerns while having very little impact on privacy while helping the entire system to work better, if we can get them done.

The next one I wanted to comment was on David. We worked pretty closely with David on some of these issues. He's gone along. And I wanted to point to people and see if they saw the risk assurance levels and made comments on. Really the best thing that we've seen out there in terms of breaking down different kinds of uses for a document like an employee card. A lot of thought went into that

and it's something that shows that the stronger the authentication is doesn't mean you want to use it for everything, for all purposes. You need different kinds of authentication for different purposes and you need different kinds of-- identity doesn't even come into play until you come into some of the higher levels of the risk level. Places where we have more concern, I'll start with the one that I think is probably the most concerning, at least in terms of implementation, and that's the pass card. Patty went through some of the

issues in a positive light there. I think the implementation of it, I mean as far as something that people may use out there, it's a useful-- potential useful tool for people out there, but the current implementation on it borders on reckless.

And think about this. It has nothing to do with security. The pass card has nothing to do with security. If it had to do with security, they would have people using the e-passport. It has to do with convenience and cost. Those are two legitimate concerns to get down to, but we shouldn't sacrifice security and we shouldn't sacrifice privacy for

that particular privacy. Because Congress did not give it to us. It assumes that security and privacy are separated in this space which a lot of times we spend time trying to separate out privacy

and security. But in this space, you're talking about identity to go hand-in-hand a lot. We think DHS can do more to protect privacy in the name of protecting security. If you have identity theft, it's both a privacy and security threat and one for the entire system in this case.

But we also think that there are other ways that you can build in privacy protections. There was a discussion Tommorer wits asked a good question about creating decentralized systems from governme and how you go about doing that. This seems like a natural fit. Here we have amber sitting right next to me. You have 56 jurisdictions that are collecting all this information, that are storing this information in a decentralized way, why not create as decentralized a model for accessing that as possible rather than creating a centralized where you have both the central of a centralized and decentralized model because the information is stored in the states as well. Wee think there are ways to go about doing that and we would hope that DHS will be createtive in those ways and if it takes-- if that means upgrating the states and needing more money to upgrade the states, the smaller states and the systems that they have, we may want to roll this out in a slower time frame t trying to Russian do all of this at the same time. There is benefit from some of the other pieces of real ID such as strengthening the card itself, strengthening the issuance process. Someone said earlier the CDTs did a report on weaknesses at DMVs. We found that we think the weakest link in the chain is the ability to bribe the DMVs themselves, the people that work at the DMVs. And background checks only get you so far as that goes. The people that are going to be working at DMVs probably haven't had the history of being in a position to being bribed, to create licenses or create some kind of identity in the past, so it's a new kind of threat for them.

The physical security of the DMVs as well is only slightly addressed in the NPRM. We think that those areas are probably the place to start and let's work at getting down the road the bigger iss as we build the states up to the level rather than going to the lowest common denominator at the

states and providing the Feds an opportunity to access it.

They had the drawing of the privacy protection across-the-board. There is a question if you do have a Valogized, any centralized set of information, where that's held and what pro techs come under

it. If it's at DHS, what protections stop it from being shared within other people from DHS. If it's held in AMVA as some people discussed where are the privacy pro techs? There is no protection for the information being held by a third-party. You don't even get the state BMV protections at that point.

Drivers license protections at that point. So there's a number of potential threats in ow this architecture actually shapes up and how we end up implementing it.

>> BETTY BRODER: Thank you. Seldon, if the Social Security Number has always been thought of as de facto identifier, and we're only now realizing what a mistake that was, maybe the drivers's licen has been considered the de facto identification card. And here you have all of the support of the Federal Government behind the states to insure its greater authenticity. What's the problem, if any with real ID from your perspective.

>> SELDEN: So many notes and so much time.

>> BETTY BRODER: Besides money.

>> SELDEN. I rest my case. I need to make a couple clarifications. And I sit here listening to the same kinds of discussions we've heard since 9/11. First of all, let's think about the origina role of the driver's license. The driver's license was created to prove you had the ability to drive. AMVA represents 56 jurisdictions throughout the United States plus several in Canada. Think

about the implications of that to the governor.

The motor vehicle association, the DMV, is the number one customer base for any governor in this country. And the reason that I felt like I should wear a flak vest up here when I sat through this two-day conference is because it all comes down to internal fraud or long lines or inefficiencies that are perceived. And yet there are other threa

to the data that we hear about that I don't see represented. So I'm not trying to be defensive. I am trying to paint the perspective to get to Betsy's question. We've seen in recent weeks identity that's been stolen from retailers. We know of identity that's been threatened from government agencies. We know of identity that's been threatened as a result of stolen or mislaid data from universities.

So let's keep all of this in perspective. There isn't always a potential for internal fraud. No matter what happens if you have access to private Secondly, AMVA is all for-- in fact our primary concern with all this is protecting the privacy of the individual. Some of that is mandated by the privacy protection act that's been there for years AMVA is all for most of the issues that we all as citizens have concerns about as a result of the statement that said all but one of the people who have gone on airplanes had fake DLs. Well in fact they weren't fake. They were real. And some of those people had multiple driver's licenses in their pocket. We recognize this long, long, long before 9/11. But it didn't grab legs until 9/11. part of what our issue is trying to do is come up with a mandate by the Federal Government-- and I will finish this without going on because like I say, I have pages of notes-- in saying when we're told we have support from the Federal Government, somebody else, not me, made the statement 11 to 23 billion dollars to implement the Real ID that will fulfill all the requirements of what's on all these different slides.

And when you talk about centralization versus decentralization, there are 56 or 57 U.S. jurisdictions, and they're all doing it differently. And they're all mandated by their governor. And you've been reading the same quotes in the newspaper that I have. A number of states that are just defying the Federal Government and saying we're not going to do Real ID. The Real ID Act doesn't require that every state has one. Just you need a real ID compliant document to get one. Some states it's cheaper to give everybody a passport than to reconvert all of our internal systems. I will say

this. Let's think about the process. I didn't come for the first 20 minutes this morning but I did hear the second panel. And this is the picture that is in my mind.

You want a secure document. In my own mind-- and I work for an association that represents the people who issue the driver's license-- in my own mind, I think of the most secure document as the passport. The problem with that is: What's it take to get a passport? A birth certificate and a driver's license.

Now, when you go get a driver's license, you have to go through the similar kinds of identification processes. So when you go to get a driver's license, what are they asking for? A birth cert and a passport. I mean, as my son said, we got us a sear you say-- serious situation here.

The point with the birth certificates when you're asking employees to verify all of these breeder documents, by the way, we don't talk to each other, all the federal systems that are there, there are

14,000 different birth certificates out there, forget the 6500 people who are issuing it. My only, if I had one flag to that point, and I go around with the federal trat commission and other agencies

that train local law enforcement on this, I have a picture, a slide show of five different birth certificates in my family. Five different legitimate legal birth certificates. There's only three

people in my family. And I don't mean to be trite. I'm just saying let's deal with the issue.

Centralization versus decentralization. There's goods and bads for all of that. But 11 to 23 bill dollars is a huge issue. And 57 jurisdictions trying to do what's right in protecting your data and then going right to the heart of what the DMV is there for, which is highway safety. We were invented for highway safety. We were not invented for identification verification or establishment.

So if somebody else wants to create whatever card that Betsy is calling this, that's fine. The DMVs will take that card and verify your identity with it.

But let's go back to my last question. When was the last time you pulled out your driver's license for the purpose for which it was intended?

>> BETTY BRODER: Let me ask the panel, everybody on the panel, following up on an earlier thought, very few of us have really talked about Social Security Numbers and the role that they'll play in any of your current systems. So if you could give a sense, maybe John, Social Security Number, is it important in the process that the bank follows in under 326? Where does it come into play? And should we abandon completely reliance on Social Security Numbers as part of the identity process?

>> Well as I said, you can't do a 1 to 1 with socials. All you can do is see if they're validly issued or if they're on a birth/death list. We have internal verifiers. He we rely on other documents. I personally believe that social have outlived. They were not created for Social Security benefits as you know. We need information to authenticate. There's gaps. There's clear gaps.

You can't use the social as your primary.

>> BETTY BRODER: Patty?

>> PATTY COGSWELL: For purposes of what I talked about in the travel context, there is extremely limited to no use of Social Security Numbers. However one place that DHS does interact extensive with Social Security Numbers frankly is the requirement to verify noncitizen's eligibility to work in the United States. And actually that would be the purpose for why Social Security Numbers were created. So I think we're actually in pretty good shape there.

>> BETTY BRODER: Is anyone going to stand up for the Social Security number?

>> If I could just talk about, it may not be well known about how Social Security Numbers are generated now. When a child is born, the mother has the right to indicate if she wants to have a Social Security Number issued for her child. If she does, then that's marked in the creation of the birth certificate and an electronic exchange is then submitted from the health department that receives the birth certificate to the Social

Security Administration who then issues the Social Security card back to the child. So there's an electronic transmission system. It's voluntary. does not have to request the Social Security card. But that's the way probably 98 percent of Social Security cards are issued today.

>> BETTY BRODER: I have a question for Ari and Toby. And it's reflecting back on the 5 D's, the principles that Simon articulated in developing an identity policy. And I think I have four of those so maybe that's good enough. An adequate discourse. That there is a decision process. That there is a design process that links back both to the decisionmaking and the discourse. And then there's

the issue of delivery. Does it work? I guess that's the fifth. Delivery. Does it work? Is it acceptable? And throughout this whole process, we're re-examining those issues to make certain th this is a system that works both practically and it has buy-in from consumers. So let's look at this from the concept of-- and Selden, also, of real ID and measuring the development of Real ID against these principles. I'm not going to ask you to grade it, but where you think the process has been very strong and where there might still be some learning to do.

>> TOBY LEVIN: Let me start by saying that DHS did not choose to that Congress pass the Real ID Act. I wish we had had this workshop for the Congress prior to their issuing Real ID. So we're dealing with just the harsh reality of legislative requirements.

I do think that we have engaged in a great deal of dialogue with the states, with state representatives and with AMVA, who is absolutely central to the implementation of the Real ID.

Whether we've done the other ones, I'd say the report card is incomplete to a great degree. But I think we were dealt the cards and we're dealing with them.

>> It's actually a great question in terms of Real ID. Toby said that Real ID, that the 9/11 commission called for Real ID. In reality. They called for driver's license reform. The intelligence reform bill actually addressed driver's license

reform in a way that we were supportive of. First of all, it was directly introduced in both bodies, the House and the Senate. It had to be. It had in it a negotiated rule making that had all the parties, deliberations and all that. We thought that was headed in the right direction. In its wisdom, Congress and our understanding is it was pushed by the White House as well. I'm not letting the White House off Scott free as Toby seemed to there. But I would say that that bill that Real ID bill was never introduced in the Senate as a stand alone measure because its supporters knew that it was going to lose as a stand alone measure. It was attached to the Iraq war spending bill. So senators had to decide if they were going to vote for the soldiers or they were going to vote to rerepeal the driver's license reform that existed before that had the deliberative process in it. Instead the whole thing was shipped over. Every time the word privacy was used was taken out of the document, out of the statute and it was shipped to DHS rather than Department of Transportation. So this deliberative process that we had in place that thought was going in the right path was usurped by a non-deliberative process that we think is headed in the wrong direction right now. And I think if you look through Simon's-- if you checked off Simon's list you would see exactly why it is. It shouldn't be a surprise that states are rejecting it the way Selden said.

>> BETTY BRODER: But I think the privacy--
>> Even though it does not appear in the act itself. There are requirements in the NPRM which can be augmented in the final rule. And I think there is a sensitivity to the privacy issue. Notwithstanding the fact that the privacy was not at all addressed in the Act itself.

>> BETTY BRODER: I have one very short question. And whoever wants to weigh in on this. We've been talking about the value of interoperability in terms of identity and authentication and actually don't know what word to use anymore. All these comfortable words. Now something else. But there is also an issue of identity creep or

use creep, perhaps. And I want to know if any of you have thoughts about credentials being used for purposes that go beyond the original purpose of their program. Again, another issue that was raised this morning about "I give my consent for you to use this for a certain purpose" but then it's just so very tempting to expand that to some purpose. Any thoughts?

>> Well, I think I mean Selden addressed it best in his conclusion about the driver's license. But the one thing that we are concerned about in the real ID proposal is the lack of limitations for federal uses of the data that's then held by either centrally and by the states, both sets of data. And potential transactional data for the use, with the use of that information. We think that it should be limited, because of the mission creep concerns and because of further use concerns, it should be limited to access, that it should be limited to access by the the DMVs and DMV employee the purposes of that person's-- for administration of that person's license and by law enforcement for those same reasons.

Beyond that, we think that you're putting the data itself at risk by giving more people access to it.

>> BETTY BRODER: Okay. I'd like you all to join me-- I'd like you all to thank me-- I'd like you to join me in thanking the panel.

(Applause.)

It's been a really fabulous morning. I think each panel is building on the other one. I'm going to ask you all now to be back at 2:15 when we resume. Some of you have asked if you will be able to get a copy of the identity taskforce report when you get back. Yes, we'll have copies for everyone. Thank you all. And see you at 2:15.