DEPARTMENT OF HOMELAND SECURITY

DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE

FULL COMMITTEE MEETING

WEDNESDAY, May 7, 2007

Transportation Security Administration

Town Hall

601 South 12th Street

Arlington, VA 22202

MEETING MINUTES

MR. HUNT: All right, good morning. As we've just gotten a quorum of members, we're going to get started.

My name is Ken Hunt and I work for the DHS Privacy Office. I am the designated Federal officer for the Data Privacy Integrity Advisory Committee under FACA. The DFO needs to be at meetings, and call them to order, and I shall do so now.

We're here to hear a report, a white paper, developed by a subcommittee on the REAL ID Notice of Proposed Rulemaking, I will turn it over to our Chairman, Howard Beales, and we're meeting.

CHAIRMAN BEALES: Thank you, Ken. And welcome everybody on the phone, and those of us who are here in person. We have a somewhat daunting task today in trying to finalize a recommendation with a hard deadline of getting it on the rulemaking record for the REAL ID rulemaking of adopting this today. And with -- what I'm sure will be a variety of interest and comment and potential changes in language and the like -- and I think it's going to be a challenge, but I think we're up to it.

Those of you who are on the phone, we're obviously not going to be able to follow our tent procedure, you will just have to jump in. I would ask that you please identify yourself, because we do have a court reporter here and we are making a transcript, so the court reporter obviously will not know who is speaking unless you tell him.

We will begin, I guess, with Richard Purcell, presenting the Subcommittee report, and we'll go from there.

MR. PURCELL: Good morning, everyone, I appreciate everybody's attention to this task we have in front of us this morning. You've received copies of the draft of the comments regarding the Notice of Proposed Rulemaking for the REAL ID Act implementation. It's a 9- page document sent out late last week. If you have not received that, please signify to make sure that we do have copies all around.

We have received comments on this from Howard, from Joe Alhadeff, and from John Sabo so far. The Subcommittee thanks, particularly, Tom Boyd, Renard Francois, Jim Harper and Kirk Herath for their input into the paper. As it stands, since you have copies of the paper, I'm just going to give you the framework of the paper operating against, and the recommendations that were made in each section of the paper.

So, skipping the prologue, which concludes with the advice that, the issues presented pose serious risk to individual privacy, and comments that, without amelioration, those risks could undermine the stated goals of the REAL ID itself. We followed the specific tasking assignment provided by the Chief Privacy Officer of the Department of Homeland Security, restated that in the paper, and then immediately struck out on the voyage through the NPRM, starting with the comprehensive security plan, which we have in two parts.

First of all, the requirement for security safeguards to be detailed in that plan, within that, what we first recommend is that the Final Rules set forth an explicit standard for security policies and procedures for the States to follow. The idea there being that, today, the NPRM has yet to name a standard against which the States could frame their security plans, and within which the Department could actually read those plans and compare to a set of standards for evaluation of adequacy.

The second part of that also calls for security standards within the card itself. The recommendation is made that the Final Rule should recommend specific steps to prevent unauthorized access to personal information on the card, including that data that in included in the machine- readable zone.

The third part is more specific, about a uniform minimum security standards that are recommended in the first part. They go through the AAMVA security documentation that we have seen and recommend, finally, that the Final Rules should use. Those security standards included in the AAMVA plans, at least as a minimally acceptable

standard for the comprehensive security plan submitted by the States. The rationale being that the States need some kind of guidance to what standards, at a minimum, they are going to be required to meet, and the Department needs some framework against which to evaluate whether those standards do meet, or those plans do meet, a standard.

In Part B of this section, we take on the idea of privacy safeguards as well. The idea here being that despite the fact that there is no language in the Act to implement privacy safeguards, our job is to recommend to the Department how those safeguards take place, and we feel this is an appropriate moment, considering the Act doesn't require security safeguards as well, in explicit terms. Under Privacy Safeguards we simply list out, first of all, the kinds of policies and controls that are widely accepted, including accountability, where we recommend that States admit and sign up for accountability for the personal information they collect and store, and to assign an individual responsibility for carrying out that duty.

In terms of our next principle or control notice, we recommend that the rules specify that agencies implementing REAL ID provide privacy notices that explain information collection, storage and use practices. Those notices should be available to all individuals whose information is affected by those procedures.

We also address consent. In the REAL ID context, of course, consent is partly, can be withheld by simply not getting a driver's license. However, in the real world driver's licenses are very important to people for their livelihood, it is an economic necessity in many cases, and so we simply ask that the REAL ID follow.

Final Rule, we recommend the Final Rule include a requirement that those implementing REAL ID should support an opportunity for individuals to opt out of any secondary uses of personal information. This, of course, we accept from that law enforcement agencies who may have reasons for secondary uses, but keep in mind that some States continue to use driver's license information for a variety of purposes, including simple revenue for selling it to marketing companies. There -- we will have a discussion about the Driver's Privacy Protection Act in this regard.

So, accesses are -- the next privacy control we recommend. There we recommend the State support access for data subjects to correct errors in their information. Those data subjects who have access should be able to, not only challenge, or review and challenge inaccuracies held by State agencies, but they should be provided access to the reference databases, at least through some mechanism of referral.

Keep in mind, of course, that the Social Security database, and a number of other Federal databases, the State has not ability to create direct access to, but if there's a simple referral mechanism that allows people to know where to go for that access, it would be helpful.

We take up limited purpose. We are concerned there that States use the information in driver's license collection for licensing and authorizing drivers and identity, as opposed to other uses. And we suggest, or recommend, that restrictions be placed on unilateral authority to change the required uses for the REAL ID cards. That restrictions be placed on unauthorized uses, included commercial uses as a standard identifier, and that implementation of notice and consent options be put in place for secondary uses.

We, finally, in the privacy section, the privacy control section, take up the idea of redress and remedy. There is always an issue -- as we have all experienced in a number of programs we've already examined -- it's important for individuals to be able to inquire about, and even complain about uses of their information that have been, perhaps, violated or breeched. The Final Rule, then, we recommend, should require that State include procedures so that individuals are able to submit those kinds of inquiries, and/or complaints about compliance, with their program in their comprehensive security plans.

In the second section, we take up the question of storing information in the machine-readable zone. In this section, this has, of course, been the subject of much of our discussion and input to the subject, the machine- readable zone -- or allowing and enabling the ability to automatically pull information from a REAL ID driver's license. In this section, we conclude with a recommendation that there be a reduction in the amount and type of information stored in the machine-readable zone from that stated in the MRZ to include only the barest name and address, and a unique identifier, which is not the license number, but rather a reference to the license number on the subject's State system, and the license issue and expiration date.

In Section Three, we discuss the electronic access of any State to the other States driver's license databases. If -- you've hopefully read the discussion of that -- the recommendation concludes the Final Rule should require that State driver's license databases be coded in ways that specify the restrictions that are placed by that State on access on transfer and on secondary uses of that personal information.

Not all States, we understand, would have exactly the same rules, that would be very difficult. And, having a variety of different rules, for any one State to understand what the other State may have already promised the individual for the handling of their information. And we believe that by encoding through hermetic techniques, the ability within the data itself during that exchange, those restrictions and conditions are put in place, perhaps they can expect a higher level of compliance, while another State has any access or control over that information.

Finally, the fourth Section of the paper takes on the question of background checks for employees in the manufacturing and production facilities for REAL ID. The question there being, who should do this? And, the Final Rule, I mean, the recommendation is that

the Final Rule should specify that the Department of Homeland Security be the initial conductor of this background searches of the subject employees. It also asks that the Final Rule require the States to use direct data feeds from Federal agencies, and perhaps even consumer reporting agencies, which they do today to maintain the currency of an employees information. So, that if they can be the ones to detect changes in a current employee's status, that might raise alarms on their behalf.

Altogether, there are 12 recommendations in the paper, and we've received a number of different comments. I will return to you at this time, to take us through the editing process.

CHAIRMAN BEALES: Thanks, Richard. And I want to thank you, in particular, and the Subcommittee, in general, for an incredibly good products under very difficult timeframes to manage. Because, I think you all have done a great job.

My own concerns focus primarily on the privacy safeguards, the Section 1B. I don't have any problem with the accountability recommendation, and I think that could easily become a part of the recommendation regarding security safeguards.

But, with the rest of the privacy, the privacy safeguard recommendations, I would, frankly, delete them. I think that it is appropriate, and indeed necessary, that DHS should, in the rule, address the privacy problems that REAL ID creates, but not that it should try to fix all privacy issues that might be out there in the world, with respect to driver's licenses. I think the privacy recommendations go, are much closer to addressing other driver's license issues that exist with or without REAL ID, where DHS is not the right forum for address those issues, rather, it's Congress.

And, on the uses that States make of the data themselves, Congress has addressed that issue. I don't see what it is in the Driver's Privacy Protection Act, I don't see what it is about REAL ID that would justify that would justify changing that standard by rule, when Congress has specifically spoken to what is permissible, and what is not. So, that is my big issue.

My second issue, I guess is more of a question on the information in the machine-readable zone. I completely agree with the idea of narrowing the information that is there to what is necessary. I'm not sure what we really know about what is necessary for law enforcement purposes, and Richard, maybe there's something there that you could elaborate on.

And finally, on the financial history checks, I'm not sure why financial history checks are worthwhile at all. I think credit reporting data is particularly sensitive data, and absent some fairly clear evidence that it would help to detect a real risk and prevent a real risk, I would say that we should recommend not accessing financial information as part of the background check. I mean, what's important and useful is the criminal records

check, and the checks against other kinds of databases. I'm not sure what the financial check adds, in any meaningful sense.

So, Richard, I think if you have a comment, that would be useful.

MR. PURCELL: Sure. Well, I will take a shot. I believe that the Statement of Privacy Safeguards is valuable to States in that, because REAL ID becomes a standardized methodology for issuing licensing -- driver's licensing -- and thereby verifying identity, I believe that it bears directly on the job that, the task that we have been assigned as a Committee to advise the Department and the Chief Privacy Officer of the Department how best to promulgate privacy in the programs within which the Department of Homeland Security is providing advice or direction. Not only within the Department, in this case, actually out to the States.

The reason that I believe that notice is important, is I don't believe that individuals -- when they get a driver's license -- are fully cognizant of the very many ways, and the very many people that are -- have access to the information that they are providing in the long term, including commercial enterprises that are yet, in some States, able to purchase this information from States.

And, additionally, there are new requirements in the REAL ID that are not the same requirements we have seen in the past. Which include, not only the verification of source documentation, but imaging and storing of that source documentation, which is an entirely new task for the States. And, to the degree that individuals' birth records, and other records, are going to be maintained by the Department of Motor Vehicles across 56 jurisdictions, I believe it would be important that those people understand that that circumstance is now occurring -- or will occur -- under a REAL ID implementation.

The others, which you've mentioned, including the distinction between primary and secondary use -- there are certainly a number of secondary purposes for which driver’s license information is currently made, and the question that I pose here is simply making it clear what uses those secondary uses are, by the States, and who has access to information for secondary purposes, and allow people to make choice around that. Whether they agree to that, or do not, or if they can withhold if they so chose.

In terms of access, it seems to me that today, people take it for granted that they know what's on the face of their driver's license, but to the degree that source material is being maintained by the State, I believe that it may be a good idea to provide subject access to that material for correction. Particularly in the case of the individual having been the victim of identity theft, and perhaps somebody else has made that claim, that they have -- it seems to me that that is an accepted practice in the commercial world. It's been an accepted practice today in law enforcement, I see no reason to be redundant, and simply make it a clear statement up front.

The fourth issue in the privacy that you mentioned, Howard, is the one about limited purpose recommendation. The idea between consent for secondary purposes, and limited purpose -- share information, but the recommendation is that controls be put in place so that purposes for which the information is gathered is actually enforced in some way, with monitored compliance.

You state, also on the machine-readable zone, do we know -- or do we have a basis of knowing what law enforcement really needs? I think that you're right that that is an area where we haven't gotten a lot of input, we certainly have anecdotal -- each individual probably has anecdotal evidence of that -- but the most important being the safety of the law enforcement officer himself. The quick retrieval to know, is this a forged document or not? Yes/no. Very important. Secondly, is this individual the individual who is represented on this? Very important. And thirdly, is the individual represented on the card wanted for any purpose that law enforcement has an interest in.

Those three things have to be the foremost concern for law enforcement. To the degree that there are other concerns, then perhaps the immediacy of knowledge may be less apparent, or have less of a need. For those reasons, I simply recommend we minimize the amount information to allow the law enforcement office to know, as quickly as possible, if it's a forgery, if the person is the person who is carrying the document is the person recommended by the document, and finally have a quick lookup to the document itself, to see if the person represented on the document is wanted for any purposes outside, that would present any danger or need to further attention.

As far as background checks, I've found perhaps this is, again, anecdotal. I've found that most background checks that include financial history checks, help reveal whether individuals have dealt, or have a need for financial gain. That may indicate further analysis, in order to make sure their financial gain isn't gained through some fraudulent activity, or some inclination toward fraudulent activity.

That's my run-through. Any others?

CHAIRMAN BEALES: Comments from other people? And this is Ramon, right? If you could all please identify yourselves for the recorder.

MR. BARQUIN: I thought I did. The only thing I wanted is to mention here is, and this is something that John Sabo had drew up, and it's in relation to the need to do a substantial job much, much better. And I want to say much better -- orders of magnitude better -- than anything we have done, to date, in the area of redress. I mean, I think that's a REAL ID, is a large change, in terms of the ability of an individual to have something that is going to be used. If it's not a National ID, it's pretty close to it. And, hence, I think it becomes very important to be able to have a quick system, not just send in a complaint.

But, I think you have something along the lines of how you do it. If cracking a shipment from FedEx or something, you can do it yourself, that doesn't mean you're going to have access to make changes in any database of your personal records directly, but the ability to, maybe actually see your information, and have someone who serves as ombudsman, either at the State level, or I would say, maybe at the federal level who could interact with States to get redress actually effected, quickly and effectively.

MR. PURCELL: Ramon, I appreciate the comment, I share the sentiment, as well. I went down that path, somewhat, in preparing the recommendation, and backed off when I couldn't resolve for my -- to my satisfaction -- the need for strong authentication for an individual's access. I am very, very troubled by -- not necessarily the issuance of the license, but the subsequent verification of the individual in an electronic format, to allow them access to their information online.

I worry very much that just entered -- certainly entering a driver's license number, having some lack of authentication, like using a password or a PIN, troubles me quite a bit, because it simply provides access to that information by a variety of different people.

So, I thought about dual factor authentication, and using the machine-readable zone. And then I thought, anybody who had access to the card might be able to do that, so I had, I went to a PIN and a password and I said, people aren't going to remember passwords for very long. We have a sufficient number of passwords, and so the problem becomes people using the same password over and over again for a variety of different purposes, which of course, means it's like having one key to your car and your house and your bank deposit box, and everything else. If it's breached, then everything's breached.

So, for a number of reasons, Ramon, I thought about that, and I would love to define that better, but I found it very difficult to do so.

MR. BARQUIN: You know, I understand where you're coming from, and you and I have talked about this. And, I will share that, and I would be willing to back down, as you did, but only on the condition that we come up with some other approach that guarantees an effective redress.

MR. PURCELL: I completely share the need for quick and effective redress, absolutely.

MR. HOFFMAN: This is Lance Hoffman, the issue of quick and effective redress is just one of several where I think the Subcommittee's report is actually very good, because it calls for more specificity. That is where I disagree with Howard. I think, I think right now, there are too many generalizations, which I'm very concerned that we're going to go down the same path we did when confronted with a similar situation about 7 years ago, when all of a sudden a flawed Government system came to light. There was a big rush to

fix it, and it was done wrong. And, of course, I am talking about voting machines after the 2000 election.

So, the Help America Vote Act was passed, there was early adoption of unproven systems, little or no accountability built in. And, what has happened is, this has produced a lack of trust. So that, for example, where I vote, the Governor urged everybody to vote absentee last year and not trust the system. Just last week, Florida -- the early adopter, went back and said, We're going to get rid of those new systems, and put in another new system at how many millions of dollars of expense.

In other words, there's a rush going on to do this, which I think is going to come back and produce such a lack of trust, that it will have an effect counter to what is desired.

I heard, Howard, about Congress being the right forum, and not DHS. I think that is true, but I think we have to be very careful in whatever we do, not to provide to the States, yet another unfunded mandate. Especially one that isn't tested once or twice a year, but that is tested many times a day. I think there are profound implications for doing it wrong, and I think we ought to reconsider that.

CHAIRMAN BEALES: This is Howard again. I wouldn't have any problem with retaining the redress and remedy recommendation, either. I mean, I think the heart of my concerns about imposing a general privacy regime on the States are the notice of choice and access, and purpose limitations. And, that set of recommendations, as I said, I think accountability recommendation is fine and should stay, and I think we could keep the redress and remedy recommendation as well.

MR. SABO: It's John Sabo. I sent my comments in last night.

MR. PURCELL: Yes, John. This is Richard. Thank you for those comments, I appreciate it.

MR. SABO: I just hope that people would read them, but in a couple of -- just to kind of hit some key points, relative to the current discussion.

Overall the thrust of the opening statements are remarkable in that they really point out and extend the implication in the PIA that the Privacy Office developed, and the language, where in some of it, I think, using the word privacy in the actual NPRM, and extending it and pointing out that building a colossally new and integrated identity system which met a certain documentation, mandates a life cycle for maintenance of that, mandates data elements, and mandates the use of technology to integrate this through network database management systems, is something that is remarkably different. And I think the implications that were addressed in the opening statements of the comments are very much on the mark.

In other words, we're talking about a significant public policy change, implemented through significant new network systems.

So, having said that, the use of the word privacy is a throwaway line, to some extent, in the actual proposed rule, it's generally meaning security. And we -- this is the Data Privacy and Integrity Advisory Committee -- we're concerned about privacy, and privacy includes fundamentals of accountability, purpose, et cetera. We don't need to go through that.

We're all experts, though I disagree with Howard's perspective -- very respectfully -- that we shouldn't really address privacy in our comments. I think that just goes against the whole point of our comments. The reason I say that is, even though we may not be able -- or the DHS rule -- may not be able to impose privacy restrictions, data elements, et cetera, in addition to those mandated by REAL ID, the fact that DHS can go on record, addressing the notice and the other provisions that we associate with privacy as a part of the rule, would set a National baseline, and understanding about the importance of privacy and the State issuance of these documents, and at least provide privacy protections for those elements that are mandated by the Act.

So, I don't think it's a stepping on the State's responsibility, I think, in effect, we're creating a national system, there should, at least, be a national system of privacy, even if it's a policy framework.

The other thing is security. A lot of references to security, and I think that the notion of High Level 17799, or the other ISO standards, impacting security controls are fine, but they do not move to any level of specificity, so should there be an expectation that, for example, states security measures, and the network interconnection, the interchange of data includes some baseline security components or controls. That should be addressed. It should not just be the fact that we have an ISO standard than each State and Federal Government, and contractors, perhaps, who are supporting these systems may choose to enforce what level they think is adequate. It would seem to me, we would need to have some reasonable baseline, and that baseline is really not articulated in these High Level standards.

They're very useful guides, but, in the end, just like the U.S. Government has done with the NIST standards, you need more specificity if you're going to have a common standard. I'm not arguing, and I don't argue in my comments at all that it should be an absolute mandate of particular controls for each State. I think you have to allow flexibility. And, I think Joe has made the point in his comments, and my comments, that States are dealing with legacy systems, and a whole range of other factors that cannot accept a mandate of particular controls or software or hardware.

On the other hand, I think the comments that we make should go to requesting a more clear and uniform baseline. Either development of such a standard by AAMVA, or an association of States that they deem appropriate, and the publication of those, and a lot more attention to audit. I think those were some of the key points.

I would say one other thing, and I allude to it in my document, and that is that there's this huge reluctance to use the benefits of technology -- and I specifically reference PKI and there are others -- in data encryption standards. It's one thing to create a huge, integrated network system, and forget about the importance of identity authentication, and access management controls in this new system. And that goes to the discussion that, with Howard just now, and Richard, in terms of an individual authenticating themselves for purpose of redress, or access to data, and amendment of records, which is part of our privacy heritage in this country, to the Privacy Act. And, I think that technology is going to used to collect data, store digital images, store data, transmit data, interconnection of systems and databases for purposes of law enforcement and identification. And yet, we seem reluctant in the NPRM and reluctant in the PIA, and reluctant in our document to suggest we should also use technology to help provide security and privacy controls.

PKI is a way to do that, because it's not the only method, but it's a very strong method, allowing the system itself to authenticate the current validity, the validity of the card, the issuance of the card, and to determine if the card has been revoked because of fraud. You don't have that in a purely paper system. It's the example of the old credit card scheme where you would go info a merchant, and they would pull out a four-inch thick book, and begin looking up tiny numbers to see if it's been revoked.

We're doing all of this electronically to gain the benefits of security, that is the intention of the law. We should also be using technology to protect the data in a machine-readable zone to allow access and amendment to records to authenticate the current validity and reliability of the card, and to support the privacy components of the expected in the law for this new system.

So, those are my general comments, and I really, strongly encourage the Committee to incorporate privacy specifically in your remarks, and to support stronger references to security controls.

CHAIRMAN BEALES: Tom Boyd?

MR. BOYD: Thank you, Howard. I have -- however we may feel about REAL ID, I think some of us have some strong views with respect to the underlying law, much less the rule which we are now debating. I'm not sure that it is our charge to get into creating a privacy framework, in the context of a rule which is not addressed in the underlying legislation.

Congress is now engaged -- and has been for some period of time -- in trying to debate what is, and is not, the appropriate policy, with respect to issues like consent and access. And, I had reservations, and expressed them to Richard, about some of the language in that part of the Recommendations, and he was kind enough to consider them in the development and promulgation of this final draft.

But, I think that the more I listen to the Chairman, and the concern I have about incorporating our own views about how a privacy regime should be structured into what is, really, a rulemaking procedure, that we're not members of Congress. And, I have reservations about doing that. However, I might agree with some of the individual comments. I'm not sure it is our charge.

MR. PURCELL: Tom, this is Richard, if I may -- and certainly, I struggled with this myself. However, I just have to ask the question -- is not the rule establishing a security regime, without, absent any mention of doing so in the law? And why -- if it is establishing a security regime without any particular charter directly from the Act -- why is it difficult to establish a privacy regime without any direct charter in the act?

MR. BOYD: Well, I think, a security regime -- when you're dealing with information -- and I think a rule has the flexibility to address how that information is protected. Insofar as security is concerned, I don't think that the elements of the privacy regime, such as we have articulated them is necessarily, follows, and I don't agree that privacy and security are one in the same.

MR. PURCELL: Absolutely agree, but at the same time, I would, though, argue that information security is a very current hot button with all of the -- with the obvious lack of security that has been applied to a variety of different databases in the Federal and the public institution, and the commercial sphere. And, for whatever reason, it's kind of an issue de jour. And, rightfully so.

For that reason, I would argue that the NPRM and the Department and our Committee will consistently, and rightfully, argue that we don't need an act of Congress in order to encourage better security practices.

MR. BOYD: I agree with that, Richard, I agree with that. There is a common law obligation on the part of custodians of information to provide security, we don't even need Congress to act on that. So, I think that that is certainly true.

MR. PURCELL: What I wonder about is if, why -- if we're in agreement on that -- why there's a lack of agreement that the custodial relationship with the use of that information doesn't meet that same standard? It seems to me, it does. It seems to me that securing the information is a part of a privacy program. But, certainly, we all know you can have security without privacy, and we're simply advancing the stewardship and the accountability for the use of that information, as well as for the security of it.

CHAIRMAN BEALES: Richard, this is Howard. To me, there's two differences. One is that REAL ID, and the requirements that are inherent in verification and sharing information across States, creates new security risks. And those risks have got to be addressed in the Rule. And I don't think that the uses of the information that is on the driver's license creates new privacy risks in that same way.

And second, there is no security scheme in Federal law, I mean, other than common law sorts of standards that would apply to this information, and a rule is, therefore needed. There is a Federal statute that governs how DMVs can and cannot use the information that they obtain in this process. In one case, we're creating a scheme where none exists, in another, we're replacing Congress's considered judgment about how to regulate DMV use of this information.

MR. PURCELL: I take it as my task as a member of this Committee to do that. That's why we have an Advisory Committee, otherwise we wouldn't need the advice of outsiders, if it was a done deal.

MS. SOTTO: This is Lisa Sotto. In thinking about the common law security requirements, they are paltry and scattered. There's really, sort of, very little in the way of a fixed framework for anybody to follow, whether you're in private industry, as to data security. I think you're suggestions -- which is really all we're doing -- we're not trying to impose ourselves on Congress, we're making suggestions here -- is appropriate, and they will be selected or not, for ultimate implementation as others deem appropriate. So, I think I would argue in favor putting all of these Recommendations in, and then letting others make the determination as to whether they are appropriate, ultimately, for the Final Rule.

MR. ALHADEFF: This is Joe Alhadeff. I don't actually see that we have any issue here concerning State guidance, or Congressional or legislative interpretation. Whether we have is specific instructions that were given to the Committee requesting information, that information was in the form of a request for guidance related for a specific topics that are laid out on page two of the document. We're not creating binding rules for States, we're creating advice to the office of the CPO at DHS, to concepts that we think they should proceed on relating to this.

That being -- and I think that within two and three, we can talk about the privacy requirements that Richard is talking about, that are things that inform the security policies. And, I think when we look at those things, they are legitimately within the ambit of the questions we were asked to answer.

And so, I think we have overstepped the question to say, are we binding States? Because we're not binding States, we have no power to bind States, we have no power to bind Congress. We have merely the power to provide advice, which we are doing.

So, I don't necessarily think it's outside the ambit of the questions. Whether or not that is consistent with what the rulemaking authority is or isn't is, I think, a different question, which we're not being asked to answer. So, I don't really have a problem with the Recommendations.

But I did make a comment, and I will apologize to the Committee, because I sent the comment really, really late last night, which is why you can also disregard the last comment, because obviously I didn't read the topic header close enough. So, on the financial background checks, ignore my comment there.

But, essentially, we have -- I don't really have a major problem with the Recommendations, except I don't think they're provided in a fashion that, I think, is as usable as possible. And, that is because, I think, we have a very imperfect knowledge of the needs and uses of information, and the context within which it is being used, and therefore there's a significant chance of unintended consequences if you don't understand the context well enough.

As John said, we have existing legacy systems that have to be accounted for, so I think we have to make sure there's flexibility to deal with real-world implementations, not just what's the best case implementation. I think we have to look at a policy, technology, and practice approach, because where you may have deficiency in one, you can beef up the other. And that goes, also, to John's concepts of audit. I think we need a flexible approach that has a learning curve, and an evaluation process built in, because it's going to be a concept of iterations here, we're not necessarily getting it right the first time, this is very important, and we want to do everything possible to get it right. But there is some need to debrief the system, and understand where things are working, and where they aren't, and continue to have improvements.

I think we need to identify what the process is, related to how you get to the decisions, and how you make those policy decisions, and I think we've had some previous framework documents that go into that. But, if we could reference the process of how you make the decisions, then, to the extent that people take on board some of the Recommendations, they have a framework to evaluate the process of how those recommendations were made, and how you evaluate, take compelling public policy need against a privacy risk.

Lastly, I think we have some issues related to technical specificity. I can't remember, I think it's Recommendation 11 where you talk, Richard, about using data elements, and I think when you look at legacy systems, it’s very hard to code data elements in legacy systems that already exist, so that's the kind of situation where we may be able to use role-based access controls and other things to accomplish the same ends.

So, I'm a little leery about getting too specifying in that level of detail on the methodology.

And, lastly, I completely agree with John, we should consider technologies as possible benefits, and we should evaluate them related to usability, practicability, and feasibility, as a part of the ways forward, and see where they can provide a benefit, where they might be a detriment, where it's too complex for a user to use, where a number of factors have to be evaluated.

So, essentially, very comfortable with most of the document, but I think it needs to be framed in a slightly more flexible and adaptive manner. And, with learning processes, perhaps a little more highlighted. Thank you.

MR. PURCELL: Thanks, Joe.

CHAIRMAN BEALES: Are there any other comments? John?

MR. SABO: Just a question, Howard. Maybe you'll be moving into this -- what is a reasonable process to propose specific changes or edits to the document, given the fact that we are really, I guess, required to do this, and vote?

CHAIRMAN BEALES: I think that's exactly right, we don't have much choice, although I think at the end of the day, we could delegate some discretion to Richard to produce a final version. But, I think, we obviously need to talk about the substance of any changes, and have some pretty clear idea of what the language needs to be.

MR. PURCELL: Pardon my interruption, we're getting some interruption from some background noise.

MR. HOFFMAN: It sounds like breathing.

CHAIRMAN BEALES: Much better. Well, I suppose the way to proceed is to, is that I would entertain a motion to adopt the report, and then amendments to the report would be in order. And we can vote on the amendments, and then on the report itself.

MR. HOFFMAN: Mr. Chairman, this is Lance Hoffman. I'm wondering if we could have a little tweak to Recommendations. I don't know if you want to go recommendation by recommendation or not, but if you do, it could be that some, even many, of the recommendations are not controversial -- at least some of them aren't -- and they could be adopted, and then we could pick off the other ones one by one. You may not want to do that, it's just a suggestion.

MR. BARQUIN: Let me just ask a question, again, once we adopt this report, does that mean that it becomes public? I'd be concerned with the report becoming public as it is without some of the amendments, and having to deal with everybody else and their brother complaining about it.

CHAIRMAN BEALES: The report is public now, in its current form, and whatever we do today will be public, and whatever we adopt today will be public, and conveyed to the Privacy Office today. Joe?

MR. ALHADEFF: Perhaps the suggestion is this –

MR. BARQUIN: Why is the report public now?

MR. PURCELL: Because we're meeting as a Committee.

MR. BARQUIN: I see what you mean. Okay.

CHAIRMAN BEALES: Right now it's a report, it's a Subcommittee Report to the Committee, that the Committee is considering.

MR. BARQUIN: I know, I'm just trying to avoid the whole RFID mess when the thing was out for the world to see long before, even members of the Committee, had seen it, other members of the Committee had seen it.

CHAIRMAN BEALES: Well, this time, Ramon, we'll be able to fix it the same day they see it.

MR. PALMER: This is Charles, here. I would also support what Charles is saying.

MR. ALHADEFF: I guess, for me, the concept is there seems to be some, I mean, what we have here is a public draft of a Committee work in progress, and I think the concern by some is adopting it as a final, is different than having continued work on a work in progress. And so, there are perhaps four or five people who've indicated strong or distinct opinions about some aspects. And, it could be that those four or five could consult with Richard in tweaking another draft, which is kind of the one that gets, perhaps, suggested for adoption, or a final round of comments. I know that that doesn't fix the document in as short a time period as we were hoping, but that could be a process step forward as well.

CHAIRMAN BEALES: That would certainly be a possibility, okay, but what would happen in that context is, it would not end up as a part of the rulemaking record, its status, as not being part of the rulemaking record in the REAL ID proceeding leaves it a little bit up in the air as to the extent to which it will be or can be considered. We can offer advice to the Privacy Office at any point, and do that sort of directly. And we can offer subsequent advice, that is, further elaboration.

But, the more we can do today, and have on the record of the rulemaking proceeding, the stronger grounds there are for actually considering our recommendation. So, unfortunately, I think that means we need to try to do this as a Committee of the whole, and figure out the necessary changes to get sufficient consensus to adopt it, or to adopt something.

John?

MR. SABO: On that line, I would suggest that we might do what you're proposing, is proceed with a motion to adopt this, have the discussion period, and accept amendments. But, do it in a sense that the comments we will be agreeing on today, hopefully -- because there's a lot of good stuff in this draft -- would represent initial comments for the rulemaking process for DHS. But, we would make clear that we are continuing to develop more detailed comments that may supersede these with respect to our advice to the Privacy Office, so we at least get something on the record, and I would say maybe approach it like, is there anything in here so difficult that we would want to raise it as an issue that we would want to propose a specific language change or deletion and go through the document in that way, and just treat it as our initial comments, given the short time span available to the full Committee?

CHAIRMAN BEALES: I like that idea, and I think probably the easiest way to implement the -- sort of the flexibility part of the notion -- is to do it, for me to do it in the transmittal letter that says, These are our preliminary comments, in the time that was available. And, we look forward, as the Department does, to looking at the comments and the rulemaking record, and offering further advice as, that would be useful or as would be appropriate. And, subject to whatever revisions we make in the document now. Joe?

MR. ALHADEFF: I've got no problem with that process. I was thinking that we might actually start the process, and one question I had, which was really kind of geared to the comments you had made earlier on some of the concerns were, to the extent that we spoke about the fact that we were providing guidance related to the questions asked us by the Secretary that may be beyond the scope of the rulemaking that is currently before Congress, but maybe a useful context and implementation, would that help address some of your concerns? That we're overstepping the rulemaking as a part of that process? Because we, realistically, this was actually answering a slightly different, and broader, question than just the rulemaking was considering, so would a qualification, to some extent, of that nature help address some of your concerns?

CHAIRMAN BEALES: Well, I think it is hard to separate that way. I think the difficulty is that the heart of the recommendation here is that DHS should adopt a rule that would require States to adopt this approach to privacy. And, for DMVs, and that would be -- I mean, that would be a new scheme different from the existing Congressional scheme. I don't see it as beyond the question we were asked to answer, that is not the argument. The argument I am trying to make: there is a scheme, we haven't really explored in any detail the adequacies or inadequacies of that scheme. And, yet, we're saying it should be replaces. And that is where I'm not willing to go.

MR. HOFFMAN: I understand. This is Lance Hoffman. I understand Howard's comment there. But, without re-hashing things too much, if we're going to move forward, and arrive at -- it sounds to me like -- arrive at something with a suitable transmittal letter by noon, or something like that, we have to move forward and decide whether the majority, I guess, agrees with that point of view just stated, or it doesn't? And, in that regard, I would restate what, I think, Joe asked -- is anything in this draft report so unpalatable that we can't accept it, along with suitable things that along later? If that is not the case, I would say -- I would second the motion that, I think, I heard made, to accept it as is, and then that will be the default, and then we can retract things, if people don't like that.

CHAIRMAN BEALES: That's exactly what I was proposing. Okay, and so I will -- there is a motion on the table that we adopt the report as is. And, there's a second for that motion. And, discussion and amendments are in order. And I agree that -- I guess the part of it that is unpalatable to me is, I would propose an amendment to delete Recommendations five, six, seven, and eight, which is the privacy safeguards we have been discussing, but keeps accountability and keeps the redress and remedy requirements.

MR. PURCELL: Howard?

CHAIRMAN BEALES: Yes.

MR. PURCELL: This is Richard Purcell. I've already argued against the amendment you have just proposed. I would like to suggest another amendment, if I may, just as an insertion. I would like to replace four words in the document, words that you point out probably are inappropriate and I recognize that and apologize. The words are financial history, they're repeated twice in the document on pages two and on page eight. My amendment would be to replace those with background.

MR. HERATH: Richard, this is Kirk. I would agree with that. I can't accept taking out the whole Recommendations. It seems to me the centerpiece of the whole program or, actually what should be the program –

MR. PURCELL: Howard, with apologies, we may be breaching protocol, but I thought that was an easy one we could get at least on record and at least change that to background.

CHAIRMAN BEALES: Unless there's any objection, I think we can treat that -- we can treat your amendment as adopted.

MR. PURCELL: Thank you. Again, Howard, I've already argued that I believe that the wording on five, six, seven, and eight provide guidance in a fragmented sectorially-guided world where we're trying to apply both uniform security standards. We're making an effort in this paper to also apply some uniformity to broadly accepted privacy

practices, some of which are a matter of law today and of decision making today. Spot recommendations are worded in such a way that providing privacy notices about collection, storage, and use practices.

Is five providing a chance to opt out from secondary uses, which are not specifically defined? Is six providing subject access to sources of their information and references or referrals to sources that are beyond the States control? Is seven, and limiting the purpose of the use of the collected information, limiting unilateral authority, unauthorized uses, and implementing consent for secondary uses? Is eight just to remind everybody -- I still believe those are simple guidance that don't change legislative history -- but rather just help guide States. Again, this is the recommendation, is these be included in the comprehensive security plan.

CHAIRMAN BEALES: Right. Okay. Is there a second for my amendment?

MR. BOYD: I second.

CHAIRMAN BEALES: Is there further discussion of the amendment to strike Recommendations five, six, seven, and eight? [No response.]

CHAIRMAN BEALES: Then I guess we should vote. Joe?

MR. ALHADEFF: I think, I still think there's a way to have -- I think the point you make that the systems in question haven't been specifically reviewed for adequacy and applicability is a legitimate point, but a recommendation that these might be the standard practices that one should adopt is also a valid point. So, I think there might be a way to suggest that in the rulemaking, that there be a charge that the systems be reviewed for adequacy and this be considered one of the, kind of, hallmark or benchmarks against which they could be judged. Because to the extent the system is already compliant, you might not have to make dramatic changes.

But these aren't non-standard practices. These are fairly standard across a number of organizations, including some governmental ones. And I think how you apply and how you look at them is an issue, but I take your point that it's a little difficult to say that axiomatically these should be adopted without going through a process of evaluation and review.

So, I think there is a process that might say a recommendation is that these are the types of things one would ordinarily see specified in security policies or at least be the inputs to security policies. And therefore, States should develop a policy by which they can review their policies across these parameters and that is where I think we can make also a comment for later to balancing on how you, then, make the public policy decisions necessary.

CHAIRMAN BEALES: Okay, do you have –

MR. HOFFMAN: Howard, this is Lance Hoffman, again. There's a good reason why you don't have language. It's hard to write language on the fly and I think the Subcommittees has obviously worked hard and produced a pretty good product -- a very good product -- given the time available. I'm very struck by Lisa's argument that we give advice, we make suggestions that, sort of, ameliorating language can be developed -- even by the Department -- it doesn't have to be developed by us. So, I think that if we don't have language, we ought to just leave it the way it is for now.

CHAIRMAN BEALES: Well, and the difficulty is that the language that we have now says very clearly, require the States as opposed to these, our criteria for evaluating the plan. And, that's the heart of my problem. There might be ways to make it into criteria.

MR. PURCELL: Howard, this is Richard. Would you be satisfied if we, on the Recommendations five, six, seven, and eight, that the statement was that the Final Rule, that the Department of Homeland Security, in evaluating the comprehensive security plan, should evaluate the way in which -- dot, dot, dot.

CHAIRMAN BEALES: Yeah. MR. HOFFMAN: What is this dot, dot, dot?

MR. PURCELL: Evaluate the way States provide privacy notices, and six, it's the way they support the opportunity to opt out. And seven it's the way they support data subject access. In eight, it's the way they support restrictions on unilateral authority, unauthorized use, and notice of choice for secondary use.

CHAIRMAN BEALES: And, could you repeat what you had before the dot, dot, dot?

MR. PURCELL: The DHS, in, I'm sorry, in evaluating the comprehensive security plans, Homeland Security should evaluate the way by which States dot, dot, dot.

MR. BOYD: And Richard, this is Tom Boyd. And this would go in the initial paragraph under B?

CHAIRMAN BEALES: No, this would go in each of the Recommendations that I propose to delete. Is that right, Richard?

MR. PURCELL: Correct. Recommendation five, as an example, would read something like, it would read something like, In evaluating the comprehensive State, comprehensive security plans, DHS should evaluate the way the State specified the need, no, the way the State provides privacy notices detailing.

CHAIRMAN BEALES: I could live with that.

MR. SABO: It's John Sabo. Is it just evaluate? Or evaluate the effectiveness or efficacy?

MR. PURCELL: I would accept that.

CHAIRMAN BEALES: The effectiveness or efficacy, I think, doesn't end up working as well. As one phrase that works everywhere, it would work in the notice.

MR. BOYD: This is associated with the security plan, right, Richard?

CHAIRMAN BEALES: Yes, this would be the privacy evaluation criteria for the security plan, correct? I mean, I think evaluating the effectiveness is implicit in evaluating the ways that they do it, if they do it in an ineffective way.

MR. PURCELL: With respect, I worry about implied -- implications are configurable, depending upon context, so I worry about that, but in some manner we should say that. My concern here, my basic concern here, is that the States in their privacy security plans, privacy policies and controls specific to these issues, and that DHS should evaluate whether they're in there. And then, should we include whether they're any good, but we don't have goodness defined. I would love to have another six months to do this.

MR. HOFFMAN: I would like to separate. I propose we separate what is now the amendment, if you will, the amendment to the amendment, I guess, that Richard is talking about. Because I think they're two different things. I think this is just an example in the last 10 minutes of how flawed this coding at the key punch, if you will, this doing it on the fly is going to be. I think it’s going to open us up to the kind of criticisms that some people made in earlier times on other issues and, therefore, I'm against this changing.

CHAIRMAN BEALES: So Richard, your language is, in evaluating the State comprehensive security plan, DHS should evaluate the ways in which the States provide privacy notices, support, and opportunity to opt out, support provision of data subjects with access, implement controls that are consistent?

MR. PURCELL: Correct. That would be my counter- proposal or counter-amendment to your new cut.

CHAIRMAN BEALES: Okay, and that, I could accept that and support that.

MR. PURCELL: Excellent, now we're dealing here and Lance is saying -- Lance, this is Richard -- I appreciate what you're saying that merely talking about, they should evaluate the ways in which -- but we do lay out, throughout the section, statements that help flavor the evaluation, as well -- the efficacy and effectiveness issues. Perhaps you could accept the amendment based on that?

MR. HOFFMAN: Richard, I hear what you're saying, and I know there's goodwill on all sides here to get this done, but this is the only place, it seems to me, that suddenly we're saying, Okay, we have general principles for the Final Rule. Then all of a sudden, in four of the twelve Recommendations, suddenly there is this wording that says, DHS will

evaluate, and only DHS, will evaluate and decide, and that will be it. And, that may or not be a good thing. Maybe I'm the only one here. I'm not comfortable just hearing that and saying, Okay, let's do that. Especially since I think there was adequate language proposed by, I think, Howard in the transmittal letter.

I think that is a much better place to deal with it. It is only temporary, here's our advice now, rather than trying to look at this rocket as best we can in limited time. It might be right, but I'm unwilling to accept it at that point. Now, maybe I'm the only one on that.

CHAIRMAN BEALES: And Lance, I guess I think in terms of the structure of this whole rule, the way this is going to work is, DHS approving comprehensive plans. So I don't think the look of these criteria is out of place. That's the nature of what the task is going to be. And, you know, I guess, I guess maybe I'm the only one, but I can't go with the language in its present form. And I think what Richard is trying to do is to find something that we could all agree on. And, I appreciate that effort.

And, I guess, probably, the way to resolve this is, Richard, I would take your language as an amendment to my amendment and then call for a vote on an amendment that says to replace that introductory phrase in each of those Recommendations, with the, in evaluating the comprehensive plan.

MS. SOTTO: Is there some way that you could suggest to get to a compromise position that you could live with?

CHAIRMAN BEALES: I'm sorry, who are you asking?

MS. SOTTO: I'm sorry, Lisa Sotto.

CHAIRMAN BEALES: No, that is the compromise position I could live with.

MS. SOTTO: I know, I know, but even more of a compromise, so that we take the language that Richard suggested and tinker with it a little bit more so that Lance can be satisfied with it.

MR. HOFFMAN: Lisa, that is not my problem. I guess I have a procedural problem. I can do lots of things at the last minute, but on something that is racing as fast as this, I'm perfectly willing to be outvoted. I don't think we need complete unanimity here. But I'm just saying, for me at least, if I had to pick, I would rather pick the initial language than Richard's amendment, if you will. But I wouldn't go away feeling that I hadn't been heard.

MR. PURCELL: This is Richard. My effort here is respecting the Chairman's views and very, very strongly wanting these four Recommendations to survive in the document. My amendment is to amend the language, specifically to lower the value of the language from requiring to evaluating.

CHAIRMAN BEALES: And I appreciate it. John?

MR. SABO: I would just say I would support the amendment and I fully agree with Lance's point, but I think the overarching issue for us a full Committee -- and ultimately there will be a final vote -- is whether or not recognizing there will be a lot of imperfections because we haven't had a chance to do this in a methodical way. Recognizing right up front, we will be, whatever we Recommendation might be subject to some criticism, but the value will be at least we'll get something into the rule making process as long as it's properly caveated, we'll have a chance to do more work directly to provide advice to the CPO and to the Secretary.

MR. PURCELL: This is Richard. If I had the floor, I would call an adjournment and try to lobby for votes and count noses and try to figure out if my amendment could be defeated and it could stand as is, but I don't know that, so I'll let my amendment stand.

MS. SOTTO: Howard, could you lay out specifically what the positions are now?

CHAIRMAN BEALES: I am accepting Richard's amendment and so my amendment would be to replace the introductory clause in Recommendations four through, I'm sorry, five through eight, with the language about, in evaluating the State comprehensive security plans. And I guess what I would do, is to say, let's vote on that amendment.

MR. ALHADEFF: Actually Howard, I have a proposal for an amendment to the amendment, because I actually think it might be better to group the concepts together as opposed to try to do that as breakouts. So, my suggestion would be, if we took accountability and redress and put them together so they are Recommendations.

Because otherwise, we're splitting Recommendations with evaluation criteria, number one, which doesn't make sense. We're leaving the other two as Recommendations. Then I also think we can group the four other remaining things with this language. A number of other factors related to privacy also need to be considered when developing security guidance.

DHS should evaluate the ways in which States give effect to the concept of notice choice, access, and limited purpose. The Committee has set forth a criteria against which DHS should evaluate State practices, procedures, and implementation for their effectiveness and practicability. The evaluation process should also take into account the analysis framework previously developed by this Committee.

MS. SOTTO: One more time, Joe, a little slower.

MR. ALHADEFF: At dictation speed, as they used to say at OECD. A number of factors related to privacy also should be considered when developing security guidance. DHS should evaluate the ways in which States give effect to the concepts of notice, choice,

access, and limited purpose. The Committee has set forth criteria against which DHS should evaluate State practices, procedures, and implementations for their effectiveness and practicability. The evaluation process should also take account of the analysis framework previously developed by this Committee.

MS. SOTTO: You didn't like the original framework?

MR. ALHADEFF: I don't remember what we called the document. That's the best I can do without it in front of me.

CHAIRMAN BEALES: Okay Joe, and we would drop all of these specific Recommendations, five through eight?

MR. ALHADEFF: No, the Recommendations are dropped and they become the evaluation criteria, yes.

MS. SOTTO: So, we're not actually imposing on the States the need to provide notice, we're just going to evaluate, in evaluating the whole, whether notice is part of the plan and, therefore, whether it's sufficient?

MR. ALHADEFF: So, I would say under each of those, then, the criteria listed or the criteria Richard has set forth, but they're not the Recommendation for adoption, they're evaluation criteria at that point.

CHAIRMAN BEALES: Okay, and then, okay, and then the paragraph you proposed?

MR. ALHADEFF: It's the chapeaux to the others without the recommendation language, but still with the detail.

MS. SOTTO: I completely agree with the comment to break it out, if we're going to do this, break it out as a separate category, so it repeats in the preamble of each of these with the same language.

CHAIRMAN BEALES: The things that are now recommendations would just disappear, right? I'm just trying to understand.

MR. ALHADEFF: The only place this appears is in the bold-faced type of the Recommendation, the discussion topic under reach remains, and I guess to be consistent with Richard, I guess choices should be consent because I think he called it consent instead of choice.

CHAIRMAN BEALES: I like that. Richard?

MR. PURCELL: I'll go with that.

MR. ALHADEFF: Lance, have we moved the ball forward for you any?

MR. HOFFMAN: It's inching forward. I wish I could see it. I'd rather have two votes and that's going to help. I need to see the whole thing, I'm sorry, in context, but I would like to have two votes. One on this amendment, this new revised amendment that everybody except me can apparently accept and then that will either pass or fail and if that passes, a vote on the final thing.

Is that workable?

CHAIRMAN BEALES: That's exactly what we will do. There may be additional amendments, absolutely, and so I guess what I would do is call for a vote on Joe's amendment to Richard's amendment to my amendment. And, the package that we agree on, of that set of changes and I don't know of a way to do this other than call the role because of the phone situation. So, Joe Alhadeff?

MR. ALHADEFF: Yes.

CHAIRMAN BEALES: Ana Anton? [No response.]

CHAIRMAN BEALES: Ramon Barquin? [No response.]

CHAIRMAN BEALES: I vote yes.

MR. BARQUIN: Howard, I'm here, Ramon.

CHAIRMAN BEALES: How do you vote?

MR. BARQUIN: Yes.

CHAIRMAN BEALES: I vote yes. Tom Boyd?

MR. BOYD: Yes.

CHAIRMAN BEALES: Renard Francois? Renard, are you with us? [No response.]

CHAIRMAN BEALES: Reed Freeman? [No response.]

CHAIRMAN BEALES: Jim Harper? [No response.]

CHAIRMAN BEALES: Kirk Herath?

MR. HERATH: Yes.

CHAIRMAN BEALES: David Hoffman? [No response.]

CHAIRMAN BEALES: Lance Hoffman?

MR. HOFFMAN: No.

CHAIRMAN BEALES: Joanne McNabb is not participating. Charles Palmer?

MR. PALMER: Yes, sir.

CHAIRMAN BEALES: Neville Pattinson?

MR. PATTINSON: Yes.

CHAIRMAN BEALES: Larry Ponemon? [No response.]

CHAIRMAN BEALES: Richard Purcell?

MR. PURCELL: Yes.

CHAIRMAN BEALES: John Sabo?

MR. SABO: Yes.

CHAIRMAN BEALES: Lisa Sotto?

MS. SOTTO: Yes.

CHAIRMAN BEALES: All right. The amendment passes. Are there other amendments? Joe?

MR. ALHADEFF: I have a very low-hanging fruit amendment. It goes to my concern about, where we talk about providing in the Recommendation, the restrictions on access. I have no problems with specifying the restrictions on access, but where we talk in the second paragraph about data coding procedures, it's on page eight. I would either be desiring to either strike the data coding procedures paragraph, or just quantify it as one way in which this can be accomplished, is by using.

MR. PURCELL: I would prefer the latter.

MR. ALHADEFF: I have no problem with keeping it in, but it's not, it's just one way, it's not the only way.

CHAIRMAN BEALES: Okay. So, everybody's okay with that amendment?

MR. PURCELL: The preliminary language then, to the second paragraph on page eight under part three, states electronic access currently reads, stated coding procedures come already widely deployed. Joe, would it be sufficient to say, one possible solution, data coding procedures already widely deployed create constraints against?

MR. ALHADEFF: Fine by me.

MR. PURCELL: One possible solution.

CHAIRMAN BEALES: Okay. Are there other amendments?

MR. PATTINSON: This is Neville Pattinson. I would like to look at Recommendation 10.

MR. PURCELL: One moment before you get to that. We have to change the language on Recommendation 11. I changed the paragraph, the second paragraph, but the Recommendation 11 would then read differently.

MR. ALHADEFF: All you have to take out is be coded.

MR. PURCELL: Right, so the Recommendation 11 would read, The Final Rule should require that all State drivers' license databases specify the specific restrictions on access, dot, dot, dot.

CHAIRMAN BEALES: Okay.

MR. PURCELL: So we're adding one possible solution as the introductory phrase to the second paragraph and deleting, be coded to from the Recommendation. Am I correct, Joe?

MR. ALHADEFF: Yep.

CHAIRMAN BEALES: Okay. Neville?

MR. PATTINSON: Okay, Neville Pattinson, speaking on Recommendation 10. It's basically on section 2, pages 7 and 8. I think, from looking at the MPRM and looking at the comments here, I disagree with this Recommendation. I think because of the weakness of the technology selected, be it a printed barcode that DHS proposes, that we end up with a Recommendation that is a result of a weak technology choice.

I would propose that Recommendation 10 is changed to redirect DHS to go back and select the technology that supports the appropriate security features and would enhance, in such a way, that law enforcement officials could obtain access to information in a secure and private manner.

MR. PURCELL: This is Richard. Bless your heart, I struggled with this one for a long time. If a REAL ID scheme -- which will establish a uniform standard nationally for identity verification -- is deployed, I agree that the deployment methodology is inherently, not only weak, but overcomes the advantages of doing, of creating the REAL ID process in the first place.

And, I struggled for a long time, Neville, with whether or not I would recommend in this section that we revisit the issue entirely from a technology point of view. As profound a system as this will be, it must be protected and made accessible in equally profound ways. And, the PDF-14 doesn't make it. I agree with that. I did not recommend it.

MR. PATTINSON: I think we need to go back and my recommendation here is that we instruct DHS to go back and revisit their recommendation. Because it is quite clear to me that in their selection they fundamentally do not offer a sufficient way of addressing data privacy, integrity, counterfeiting, by using printed technology. And so on that basis, I disagree with this Recommendation as we have it and would recommend we replace it, as I said, with some instructions to go back and find the technology choice that addresses the need, which this doesn't do.

CHAIRMAN BEALES: Neville, this is Howard. I guess it seems to me, this one is a bit outside the scope of what we have been asked to do. And, I guess I see -- it seems to me that the recommendation that Richard has here, and your recommendation, are not inconsistent, in that whatever information is going to be, whatever the technology is going to be, there is going to be a machine- readable zone.

MR. PATTINSON: Then it should be protected in such a way that clearly law enforcement officials should be able to access, and other commercial entities should not be able to obtain access, under the privacy issues we're looking at. I mean, it's a part of the -- under section 2, our guidance of how it should be stored, possibly in the machine-readable zone. I think we should go back and tell them that they selected, or proposed to select, technology, which is insufficient for the purposes of the task. And, the Department has something that is used on driver's licenses to date, under a weak ANSA standard. I think it is inappropriate. And we should be looking at the importance of how this should be implemented for the future of our identity system, that we're looking at there. And, that we owe the U.S. public a review of how this information should be stored and protected.

MR. PURCELL: Howard, this is Richard. Number 2 in our task matters, specifies we should be looking at how it should be stored, what is stored and how it should be stored on the machine-readable zone, so it is in our wheelhouse.

MR. HERATH: Can't we accommodate both, can't we start out with a suggestion that the technology be, be revisited? Alternatively, if that isn't where, isn't that where they go, then we go with what we've got right now?

MR. PURCELL: I think Recommendation 10, from my point of view, is a minimum.

MR. HERATH: So we go with the amendment and then a fallback?

MR. PURCELL: I can accept that.

CHAIRMAN BEALES: John?

MR. SABO: I guess I agree. We're supposed to address this, and we have some scope in how to address it. I agree with Neville. And I think the reason I agree is the prior discussion. Under Roman II on page seven, we talk about the many threats associated with being able to read data from the machine-readable zone et cetera, et cetera.

And as someone said, it's into the context of our concerns about threats to privacy and then we say there are two additional threats, and we set up a straw man of technical approaches to mitigate a threat as being threats, which is the issues around key

management for encryption and failings there. And, even if you had such technology for the MRZ, you would bring an OCR in and scan.

Those arguments, I think, show a strong bias against what I was arguing for earlier, which if you're going to implement a technologically-based system with an MRZ, then you should not be immune to examining technological solutions to protect the data on the MRZ and to simply say, our technological solutions is to store less data on the MRZ, is kind of a throwaway. So, I would agree.

I'm a little troubled by that language that sets up two mitigation -- one mitigation technique as a straw man and destroys it and the other saying, Well, you don't need to worry about the MRZ because you've got OCR at the front of the document. I would support Neville's approach, but I would also urge us to change the language. There are two additional threats to the information stored in the MRZ. You might say, there are other factors associated with MRZ data storage and talk about that. And, then I would support their amendment from Neville.

MR. PALMER: I also would agree that, given their charge, the specific instructions we've received -- number two, Please provide comments on what data should be stored and how it should be stored in a machine-readable zone so it can be protected. I think this is perfectly fair game for us to push back and make comments and especially, given our history with RFID, I think it is still perfectly reasonable to push back and say, Perhaps the technology you chose is inappropriate or is not quite as good as you might think. That's all I have.

MR. HOFFMAN: I think there's a balancing act here. This is Lance. I think we need both. I think we need a built-in suspenders approach. I like what Charles and Neville and everybody seem to agree on saying, but I think we have to say it in such a way, that if you're still going to, basically, ignore what we say and go with what you have, then at least use what is in, what Richard proposed or what the document has originally.

MR. PURCELL: That's exactly what we did in the RFID. I agree with you, Lance.

MR. ALHADEFF: I think, you know, part of how you chose a technology is a balancing of a number of factors, including usability, including cost of deployment, including technical complexity, including I lost my password, and the kind of support facilities you have to go to replace those kinds of issues. And, there's a whole ecosystem you look at when you choose technologies, and I think they should be advised to go back and revisit the technology choices.

But I also think Richard's suggestion is a very useful one, which is that the information stored on the card should be tailored to the level of protection afforded by the technology chosen. And, this is a recommendation related to, if this technology is chosen, we would recommend a limitation based on that choice. However, other choices may be

made with other technologies and then the revisit concept Neville was looking for, I think, is appropriate.

But, I also think we have to, when you look at what AAMVA started out doing, is they started out attempting to protect the driver's license, not a national ID card. And, I think part of the things we always come to terms with, is we have a card that is being made to do much more than it was ever intended to do and therefore, the protection's made need to be higher, based upon those kinds of concepts.

But, I think we can come to an agreement as long as we understand their balancings that will take place as part of the ecosystem and there are choices for which we don't know all the factors. And, as those choices are made, there needs to be an appropriate consideration of the possible technologies and then a limitation based on the choices of technology made.

MR. PALMER: Sorry to be a stick in the mud here, but unfortunately we don't know what these things are going to be used for, and so we don't know to what extent these things will be at risk.

MR. PURCELL: No matter what the regulations or guidelines say, they may be required for all sorts of situations. So, while I'll never convince everyone we should do this as best we can, that is this whole technology choice should be the best possible.

I don't know how we can express better that what was said a moment ago, which is, it should be the right technology for what we expect the use to be. I don't know that I can really predict what it will be subjected to, but it does scare me a bit that if we say it should be a task- appropriate or use-appropriate, that we don't actually know what the use is.

CHAIRMAN BEALES: So, I guess I'm not clear on exactly what language we're talking about here and what it would end up looking like. I'm completely comfortable with the notion of saying, We think you ought to reexamine the technology choice, but given this technology choice, we recommend you do this. Does that work for you, Neville?

MR. PATTINSON: I'm not sure the second part works for me. I fundamentally disagree with the technology choice because it's completely inappropriate in being able to do the task that it has been assigned to, which is to provide law enforcement access, and not other people access. And, I don't believe it's appropriate technology, so, I guess, let me think about that for a minute. I can't really support anything to do the MRZ in a printed bar code form. To me, it doesn't have sufficient security or privacy protections for the information.

CHAIRMAN BEALES: Are there any other thoughts on how we might bridge this?

MR. SABO: One way to bridge it might be to accept Neville's approach about reexamining technology. This is John Sabo -- reexamining technology, and instead of saying, where's the language? I lost my language. The Final Rule should require reduction in the amount of, type of required MRZ. However, with the technology identified in the NPRM, at a minimum, a reduction in the amount and type of any data stored in the MRZ would be of value. This is not an amendment, however, the Committee has not fully evaluated -- has not had an opportunity to fully evaluate these issues -- something like that, just to show this isn't a definitive Recommendation.

MR. HOFFMAN: I think there's enough language going to be in the letter from Howard that says, We're transmitting this, and more may come later, I think it weakens it too much, John, to say that kind of thing. And, it sounds to me like it's pretty clear what people are saying, and why don't we just -- Howard, I think, Howard laid it out very well, it may be that everybody but Neville can go along with that. And, I don't know, in which case, Neville, you might just have to say, Okay, I'm against it, just like I was the one outsider on the other one.

MR. PATTINSON: I can go along with that.

CHAIRMAN BEALES: So, I guess what the language would be is that Recommendation 10 would start by saying, DHS should reevaluate the technology, the appropriateness of the MRZ technology for this task. Assuming this technology, however, the Final Rule -- dot, dot, dot -- the Final Rule should require --.

MR. HERATH: This is Kirk Herath, I have to drop off for another meeting, but I would -- what you just stated is what I support. I think we can assimilate the two ideas effectively, and assume that -- in the best possible world -- please reevaluate it, however, if you're not going to reevaluate, then here's some other considerations. I think you have to have a fallback. I have to drop off.

CHAIRMAN BEALES: Okay, thank you, Richard.

MR. ALHADEFF: Just a word suggestion, instead of saying assuming, say if.

CHAIRMAN BEALES: Okay, DHS should reevaluate the appropriateness of the MRZ technology --

MR. PURCELL: Of the proposed --

CHAIRMAN BEALES: -- of the proposed technology for what?

MR. PURCELL: For the machine-readable text.

CHAIRMAN BEALES: -- for the machine-readable text. If it maintains the current approach, the Final Rule should require, dot, dot, dot.

MR. HOFFMAN: Excuse me, Richard and Howard, do you want to really say text in the machine-readable rule? It may not be text.

MR. PATTINSON: The MRT is machine-readable technology.

CHAIRMAN BEALES: So, shall we vote on this? Joe?

MR. ALHADEFF: Yes.

CHAIRMAN BEALES: Ana? [No response.]

CHAIRMAN BEALES: Ramon? [No response.]

MR. BARQUIN: Yes.

CHAIRMAN BEALES: I vote yes. Tom?

MR. BOYD: Yes.

CHAIRMAN BEALES: Renard? [No response.]

CHAIRMAN BEALES: Reed Freeman? [No response.]

CHAIRMAN BEALES: Jim Harper? [No response.]

CHAIRMAN BEALES: Kirk voted yes before he dropped off.

David Hoffman? [No response.]

CHAIRMAN BEALES: Lance Hoffman?

MR. HOFFMAN: Yes.

CHAIRMAN BEALES: Joanne McNabb is not participating. Charles Palmer?

MR. PALMER: Yes.

CHAIRMAN BEALES: Neville?

MR. PATTINSON: No.

CHAIRMAN BEALES: Larry Ponemon? [No response.]

CHAIRMAN BEALES: Richard Purcell?

MR. PURCELL: Yes.

CHAIRMAN BEALES: John Sabo?

MR. SABO: Yes.

CHAIRMAN BEALES: Lisa Sotto?

MS. SOTTO: Yes.

CHAIRMAN BEALES: All right, that amendment passes. Are there any further amendments?

MR. SABO: Yes.

CHAIRMAN BEALES: John?

MR. SABO: I have a proposed light amendment to Recommendation number 3. I had proposed language in my email. My concern is that the AAMVA standard is, in fact, not at such a high level set of standards as it's not really useful to establish a baseline. So, if I can pull it up, where is my recommendation? Here it is. I would propose, for Recommendation number 3, the following substitution, if I can find three.

MR. PURCELL: I'm sorry, John, I lost you.

MR. SABO: I'm proposing language that says, The Final Rule shall reference the AAMVA situation security standards for a comprehensive security standard that will be developed and defined by AAMVA, working with the States and DHS, and that will be published and applicable, specifically to REAL ID.

In other words, if you look at the language in my email I sent yesterday, under Roman V, I said I would be much more comfortable saying something like, and then, that is the recommendation I have. So, it would be the AAMVA information, security program and standards should be the foundation for a comprehensive security standard that will be developed and defined by AAMVA, working with the States and DHS, and that will be published and applicable specifically to REAL ID.

CHAIRMAN BEALES: Is there comment on this amendment? [No response.]

CHAIRMAN BEALES: Is there objection to this amendment? [No response.]

CHAIRMAN BEALES: We'll consider it amended. Any further amendments? [No response.]

CHAIRMAN BEALES: Then I call for a vote for the amended final recommendations to be accompanied by a transmittal letter saying, We're not done yet. Joe Alhadeff?

MR. ALHADEFF: Yes.

CHAIRMAN BEALES: Ana? [No response.]

CHAIRMAN BEALES: Ramon?

MR. BARQUIN: Yes.

CHAIRMAN BEALES: I vote yes. Tom?

MR. BOYD: Yes.

CHAIRMAN BEALES: Renard? [No response.]

CHAIRMAN BEALES: Reed? [No response.]

CHAIRMAN BEALES: Jim Harper? [No response.]

CHAIRMAN BEALES: Kirk? [No response.]

CHAIRMAN BEALES: David Hoffman? [No response.]

CHAIRMAN BEALES: Lance Hoffman?

MR. HOFFMAN: Yes.

CHAIRMAN BEALES: Joanne is not participating. Charles Palmer?

MR. PALMER: Yes.

CHAIRMAN BEALES: Neville Pattinson? Neville?

MR. PATTINSON: Yes.

CHAIRMAN BEALES: Larry Ponemon? [No response.]

CHAIRMAN BEALES: Richard Purcell?

MR. PURCELL: Yes.

CHAIRMAN BEALES: John Sabo?

MR. SABO: Yes.

CHAIRMAN BEALES: Lisa Sotto?

MS. SOTTO: Yes.

CHAIRMAN BEALES: All right. Thank you, Richard, in particular, for your yeoman's work, both in producing the draft, and today, in producing a final product. If you will email to Ken and me, a final version, we will get this out the door later today.

MR. PURCELL: I'm on it.

CHAIRMAN BEALES: Thank you all very much, for accomplishing what, on the way in, I was thinking was an impossible task, and I'm glad I was wrong, and I guess this meeting is adjourned. [Meeting adjourned at 12:05 p.m.]