DEPARTMENT OF HOMELAND SECURITY

DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE

FULL COMMITTEE MEETING

WEDNESDAY, JUNE 11, 2008

Hilton Arlington

Galleries I and II

950 N. Stafford Street

Arlington, Virginia 22203

MORNING SESSION

MR. HUNT: Welcome to the public meeting of the Data Privacy and Integrity Advisory Committee, a committee that advises the Secretary and Chief Privacy Officer of the Department of Homeland Security on matters related to privacy in programs of the Department.

My name is Ken Hunt and I am the Designated Federal Officer of this committee, under the Federal Advisory Committee Act. The Designated Federal Officer is required to be present during public meetings, and I am.

So, I'm going to turn the meeting over to Howard Beales, the Chairman of the Committee. Thank you, Howard, the meeting is yours.

CHAIRMAN BEALES: Thank you, Ken. And let me add my welcome to everyone who is here today.

A couple of housekeeping announcements, first, just please make sure your cell phone is turned off. We will have a ring tone competition at lunch, but in the meantime, you don't want to give away your secret weapons.

Second, if you're interested in signing up for public comments, we'd love to hear from you at the end of our day. Please sign up at the table outside the room.

As has been our custom, we will begin with an update from the DHS Privacy Office, and with us today is John Kropf, who is the Deputy Chief Privacy Officer at DHS. He also serves as the senior advisor for International Privacy Policy, and he's a key advisor to the Chief Privacy Officer and other DHS leadership about issues about privacy, and compliance with the privacy laws, as well as the Chief Operations Officer and policy strategist for the Privacy Office.

He oversees the offices international privacy work, and has represented the Department on U.S. delegations to OECD, APEC, and has served as the advisor to various international negotiations.

John earned his law degree and Master's of Public and International Affairs from the University of Pittsburgh. He's published numerous articles on global privacy issues.

And John, we're glad to have you with us to hear what's new and different in the Privacy Office.

MR. KROPF: Good morning, and thank you very much, Mr. Chairman, for that very kind introduction, and good morning to the other committee members, and thank you for joining us here in Washington.

Again, my name is John Kropf, and I am the Deputy Chief Privacy Officer for the Department of Homeland Security's Privacy Office. I am sitting in today for the Chief Privacy Officer, Mr. Hugo Teufel, who is unable to join us this morning.

But what I would like to do is, first of all, just start by thanking the committee for their hard work, and their continued support and advice to the Department, and especially to the Privacy Office, I know that we are the better for it, and that we are looking forward to your continued input, and looking forward to your committee reports later in the day. So, I'd just like to note that, that we're deeply appreciative of your hard work and dedication and traveling throughout the country to the various locations that we've selected.

With that, I'd like to just sort of run down our updates since we last met in El Paso, Texas, in March, to keep you current on the activities of the Privacy Office, and I'd like to start our update with just a review of the Office itself, and the personnel situation.

I think, as I noted last March, we are an expanding office, we are a dynamic office. We're about to post a new Director position -- this would be a Director of Privacy Incidents and Inquiries. This is to take on duties that have really been mandated by the 9/11 Recommendations Act, but it is to have a Director-level position handle those incidents and inquiries.

We are also currently interviewing a candidate for an Associate Director position of Privacy Policy and Education. That Associate Director will report directly to our Director of Policy and senior advisor, Ms. Toby Levin, and will be focused primarily on education and training. We have significant responsibilities in this area.

We also are very pleased to note that we have -- we're participating in the DHS Fellows program, we have signed on for two Fellows -- this is a DHS program that brings graduate students into the Department for a two-year assignment. They have selection of three 8-month rotations within the Department, and our first Fellow will be coming on next week, who has expressed a specific interest in the Privacy Office, and actually a very specific interest in the area of the cyber-imitative, and cyber-security. So, we're delighted to have some new blood coming into the office.

We have also two summer interns coming on, as well. We have a law student from Ohio State University coming on board very shortly, and a second student is slated to join us a bit later in the summer.

We've also been emphasizing training for the staff and staff development. I'm currently, myself, enrolled in a Senior Executive Development Program. The Deputy -- the other Deputy or the head of the FOIA Disclosure Unit -- has taken a number of executive development class, as well. Other members of the staff have been able to participate in training and conferences in their specialized areas. So, we continue to develop staff members' knowledge and levels of expertise.

We have also been involved in preparing for -- several exercises preparing us for the upcoming transition in DHS, with the coming change in leadership, so we're preparing our senior level career people for what may come with a new change in Administration, as well as, we have engaged in a significant Continuity of Operations Exercise. Essentially, what that means is -- it's an exercise where there was a simulated natural disaster, and also a terrorist event at the same time, and we were part of a larger DHS exercise, and the Privacy Office was involved in that, and that involved two days of intense participation by all of the senior-level members of the office, and provided us with an opportunity to put our expertise to use in a simulated emergency environment.

I'd like to turn from personnel now, and turn just briefly to one item to note on the Congressional oversight side of things. Next week, June 18, the Chief Privacy Officer will testify before the Senate Homeland Security and Governmental Affairs Committee. This is a hearing that is going to be held on a Congressional review on the scope of Federal privacy laws. And Mr. Teufel will be testifying, along with Linda Kuntz, who is from the Government Accountability Office. And they recently had concluded an engagement regarding a review of how the scope of Federal privacy laws might be improved. So, that is the most immediate Congressional activity that we have coming up.

I'd like to turn now to reports and guidance in the category of reports. We've now completed our third quarterly report on the activities of the Privacy Office, as required under the 9/11 Recommendations Act. This report is a compilation of the guidance, complaints, and training that we have done for the last quarter. That report is available on our website.

We are also beginning preparations on our 2008 Annual Report, which we expect to be -- to have a good final draft, perhaps, by the end of July. We also have a data call underway for an updated data mining report, so we're busy working with the Department on that.

As far as guidance goes, we have a very noteworthy issuance that we've done -- we've done System of Records Notice guidance, which was just issued last month. It is issued in a booklet form, much like the Privacy Impact Assessment booklet -- you should all have, hopefully, a copy in your materials.

We're extremely pleased that this has been issued, and we hope -- if it's anything like the PIA guidance -- that it will get a lot of use and -- a lot of use from the other Federal agencies who have looked at our PIA guidance, and we expect that they will be looking to the SORN guidance, as well. So this is really a significant accomplish for our compliance team.

We have also issued guidance on Privacy Act statements, that is, the statements that go at the bottom of the forms for collection of personal information by DHS. We've issued additional updated guidance on privacy threshold analyses templates that -- trying to make them more current with the OMB guidance on safeguarding of personal identifiable information.

And so we've been pretty busy in the last 3 months on the guidance front.

But I'd like to close out guidance, and turn, now, to our international activities, for a moment.

Significantly, Mr. Teufel recently went down to the Ibero-American Network Conference in Cartagena, Colombia just last month, and this is noteworthy, because it's the first time a DHS representative has gone down to this network, and he was asked to speak and present there on the U.S. privacy framework.

This is, essentially, for those not familiar with the group, it was established in 2003, by Spanish Data Protection Authority, and was a forum to advance EU-style privacy concepts across the Spanish-speaking countries in Latin America.

One other noteworthy mention on the international activities front is we -- we were able to send our Associate Director for International Privacy Policy to a European law conference, that was a fantastic opportunity for her to hear firsthand, an open discussion

of the implications of the Lisbon Treaty, which will affect data protection and data sharing within the European Union. It's something that is very important to the Department, and something that's very important to the Privacy Office, to know how that treaty will work, and affect on data sharing, with one of our most important allies and partners in the data-sharing arena.

Probably, of greatest significance to note from that conference is that, if the Lisbon Treaty does go into affect, all of the international information-sharing agreements with the EU will then have to be passed by the European Union Parliament and Council.

We have also continued to be an active participant in providing our expertise to the international policy discussions with the European Union on ongoing data sharing discussions. There's currently -- a set of discussions have been ongoing between the U.S. government and the European Union on data sharing, and the law enforcement and homeland security arena.

So, with the international -- I'd like to close that out there, and move right into compliance. And since our DPIAC meeting in El Paso, we have published 16 new Privacy Impact Assessments, and 5 new Systems of Records Notices.

I'd like to just touch on some of the more noteworthy programs that these compliance documents discuss.

The first two are U.S. Coast Guard systems -- the first being something called MAGNET, which is a database that allows the Coast Guard to look at and display different vessels, and that would include the passenger and crew manifests of those vessels. This is a very significant system for the Coast Guard, and we were able to work with them to issue a PIA, a SORN, and a Notice of Proposed Rulemaking.

The second Coast Guard system was something called LEIDB, or the Law Enforcement Information Database, and this was a system that involved archiving and storing text messages by the Coast Guard's Law Enforcement and Counter-terrorism sections. And in the case of LEIDB, we also issued a Privacy Impact Assessment, a SORN, and a Notice of Proposed Rulemaking.

Turning to a third system, the Customs and Border Protection very, very recently issued an interim final rule to create regulations governing the Electronic System for Travel Authorization, or ESTA. We issue a PIA, a SORN, and an NPRM there.

With ESTA -- ESTA is a system that will govern the collection and use of information on foreign travelers entering the United States from visa-waiver countries. It is, in short, essentially taking what is now a paper system, that is, the I-94Ws, which passengers would have to fill out on the planes, and converting it into an electronic system.

The information is to be collected electronically in advance of the passenger's departure. And that is a new technology that's being introduced. And once notable thing to mention is in doing the -- the System of Records Notice and the Privacy Impact Assessment, we have mentioned in both of those compliance documents, the mixed systems policy from the Privacy Office. That is significant, because what that policy says is that DHS will apply the Privacy Act protections to -- to all systems that, whether they cover U.S. persons, or not. If it's a system that has both U.S. person, and non-U.S. person information included in those.

So, ESTA is now the subject of Privacy Act protections.

The other two systems I'll mention would be the USVISIT exit system. And we did a Privacy Impact Assessment for that -- that is the first phase of what is to be the collection of the biographic information upon exist from the United States, it's the entry portion of USVISIT. This program has been implemented in phases, and this is the first phase of the exit system.

And then, finally, I'll mention the Einstein-2, which is a Privacy Impact Assessment that we did for an update to USCERTS Einstein program. This is simply a -- meant to take into account technological improvements in the Einstein program, which includes now, the use of signatures to identify militia's computer code, inserted into computer networks.

And, as always, all of these PIAs and SORNs are up on our website, available for public access.

Finally, on compliance, we continue to look at our legacy SORN initiative to ensure that we have accounted for, and updated, all of the legacy SORNs that we inherited from the 22 different components that were consolidated to create DHS. And, to date, the Privacy Compliance Team has categorized and analyzed more than 215 legacy SORNs, and re-drafted more than 127 SORNs.

So, in the coming months, we hope to begin publishing further SORNs to clear out the backlog of the old legacy list.

And I'd like to mention on training -- training is increasingly becoming a bigger part of our activities, we're doing more and more external training. The DHS Privacy Office recently hosted a workshop on privacy compliance fundamentals. This continues to be a very popular event, the last event had 125 attendees from all over DHS and the Federal government.

We have also worked with components, to inspire them to do their own in-house training. The Coast Guard has conducted an all-hands Training and Privacy Awareness Week for its members and employees.

The Science and Technology Directorate recently held a Privacy Day, which included multiple one-hour sessions on protecting privacy, with our Director of Privacy technology, Mr. Peter Sand, and the Transportation Security Administration has begun a poster campaign, related to protecting personally identifiable information. I'm not sure if we can do something as formal as enter an exhibit into the record, but I will pass around for you a poster that TSA has done, featuring their Privacy Officer in the role of Privacy Man. So, I will pass that around for the committee's inspection and perusal.

CHAIRMAN BEALES: Is the flying pig in it?

MR. KROPF: There is no flying pig in it, but I think you'll see that it is -- it's an impressive poster. It has both a Privacy Officer and his assistant, suited up to do privacy work.

MR. HUNT: Peter Pietra actually addressed this committee in El Paso -- you might not recognize him -- this is his alter-ego.

MR. KROPF: Then, finally, I'd like to mention that we've been working very closely with civil rights and civil liberties. And we've been working on completing a training program for intelligence and analysis, analysts assigned to Fusion Centers.

And let me just pause there for a moment, and mention that we're very fortunate to have Mr. Dan Sullivan, who is the head of that Office here, today, who will be speaking to you shortly, as well as other members of his staff. And they have been extremely helpful and cooperative, and we've learned a lot from putting together training programs with his office.

We've also been working in cooperation with the Department of Justice, to develop training for State and local Fusion Center representatives.

And finally, just in the category of outreach, there was a -- recently this week we had a DHS-advertised speaking forum, where we had invited Professor Solove to come in and speak about privacy, and that was reported to be a very well-attended event. And based on that, we hope to hold future privacy speakers in the Department.

So, I think I've covered most of the waterfront in brief fashion, but I would like to just end my remarks there, and give you the opportunity to ask me any questions that you might have.

Thank you very much.

CHAIRMAN BEALES: Thank you very much, John.

John Sabo?

MR. SABO: John, thank you very much.

You mentioned Einstein on the PIA, and there's a classified initiative -- let's see if I get the name right -- Comprehensive National Cyber-security Initiative, CNCI, which is a classified program, but deals with protecting government networks, and from what we understand in the media, also, at some point, will migrate to private sector networks in some fashion.

And the question for you -- I realize you can't talk about the program, but a question is, is the Privacy Office involved in reviewing the privacy impact of the plans associated with CNCI.

MR. KROPF: If we're talking about a system that would come under a Privacy Impact Assessment, we would be doing that. It is our policy that is supported by the Department that we would do Privacy Impact Assessment even on national security systems that are exempt from that requirement. While these PIAs would not be publicly available, nevertheless, we go through the discipline of putting the component through issuing PIA.

So, does that --?

MR. SABO: So you -- but you're not disclosing whether or not you are examining the program, you're merely saying you would do that?

MR. KROPF: I'm merely saying, we have a policy where, where we would do this.

We're going to make this a team effort, if you don't mind, Toby Levin had --

MR. SABO: And I'm not asking you to disclose anything that's classified, I'm just --

MS. LEVIN: I suggest, if you take a look at the Einstein, the updated Einstein PIA, that is the assessment of the privacy impact of that aspect of that program, because it addresses how the networks -- the issue of the impact of the Agency's role in reviewing seeking to address militia's code, through the Federal network.

So, that's an important part of that initiative.

MR. SABO: Okay, thank you.

CHAIRMAN BEALES: Joe Alhadeff?

MR. ALHADEFF: Thank you. And I neglected to take down the actual name of the system, but it was where you were talking about the electronic I-94, and the pre-population of the information. And it -- just a couple of questions -- is that pre-populated by the person who's filling out the I-94? Or is that pre-populated by some other group?

I would assume it's the person who is -- ordinarily would fill it out by hand on the plane. And, if that's the case -- have you spoken with the Australians about their experience on the electronic visa, because they've had a long history of experience of exactly those kinds of electronic forms.

MS. LEVIN: I'll jump in again. In fact, it's my understanding that they did look at the Australian program, very closely. And in the PIA for ESTA, you'll see that mentioned. And it is the individual going online, putting in that information. But it does -- the PIA does reference the Australian experience.

MR. KROPF: This is truly a team effort. But, Toby answered the question, the name of the system is Electronic System for Travel Authorization, it's ESTA, it was -- it's mentioned in the legislation as simply Electronic Travel Authorization, but there had to be a modification. When it was simply ETA, that had some negative connotations in Western Europe, so they changed it for that reason.

Does that -- have I answered you question? Okay.

CHAIRMAN BEALES: If -- I was wondering if you could say a little bit more about the simulated exercise, and the Privacy Office's role in it, because we are working on -- one of the Subcommittees is working on information sharing in these situations, and it would be useful to know what we learned, and whether there was a privacy crisis.

MR. KROPF: What I can say about the exercise is it really focused a lot on -- for us, it focused a lot on logistics, and having people in place, ready and available. As far as privacy lessons learned, I think what we took away from it is, it would be very good for us to have some readily-available, short and concise privacy, and also disclosure guidance, for senior leadership that we could issue almost preemptively, so that people would have something in front of them to make them aware that privacy will be an issue that arises, rather than waiting passively for someone to call us.

So, we're preparing some guidance along those lines now, that would be issued for individuals to use in what we would call their COOP materials, their Continuity of Operations Materials. So, that would be standard reference material.

CHAIRMAN BEALES: Ramon?

MR. BARQUIN: I think we've read a lot about the attention up on Capitol Hill, vis-à-vis cyber-security, and I know that goes beyond DHS.

But I was just curious, because of the role of data integrity being so central and parallel to security, whether there's been any attention that has been given to that aspect of it, in at least the conversations within DHS. And I would assume the Privacy Office would potentially have a role in bringing that up, if it was relevant.

MS. LEVIN: I just wanted to -- this is Toby Levin -- I just wanted to mention that I had the -- a very wonderful experience, actually, a few weeks ago, DHS is a participant in the Global Information Project with DOJ, Global Information -- the acronym is escaping me right now.

But they have a FACA committee, much like this, that's been involved on a number of projects that are particularly focused on Fusion Centers, and sharing of criminal justice information. And they have a FACA group working on data integrity, specifically, and I had an excellent experience with that group, working on a product, I think that will be directly in response to the need for more guidance on data integrity issues, with regard to information, both at DOJ, and at DHS. And so, I was very excited to see that, their work.

And I know you, particularly, Ramon, have been very interested in data integrity issues. So, when I saw the -- the efforts they have underway, I was relieved to know that there's something coming down the pike that I think will directly address your concerns, and when it is available, we will make sure that this committee is informed about it.

MR. KROPF: And I was also going to add on to that, that we have been working with the CIO, and also the Chief Information Security Office, to update a lot of the safeguarding requirements for PII -- this is specifically in the certification and authentication areas. But, we're in close cooperation with those offices, so we have plugged into them and they recognize how important privacy and security of that information is, so --

CHAIRMAN BEALES: All right, well, thank you very much, John, we appreciate the update, and thank you for being with us today.

For the rest of the morning session, we're going to hear about another function in DHS that's closely related to what we do, and that is the Office of Civil Rights and Civil Liberties. Many of us think that privacy is a civil right or civil liberty, so it's appropriate that we should hear more about that part of DHS.

We begin this morning with Dan Sutherland, who's the Officer for Civil Rights and Civil Liberties at DHS. He was appointed by President Bush on April 16th, in 2003. He provides legal and policy advice on a full range of issues, at the intersection of Homeland Security and civil rights and civil liberties.

MR. SUTHERLAND has been a civil rights attorney throughout his legal career. He spent 14 years with the Civil Rights Division of the Justice Department, and 2 years with the Office of Civil Rights, at the U.S. Department of Education. He was the first Executive Director of the Brown v. Board of Education 50th Anniversary Commission.

He graduated from the University of Virginia School of Law, and the University of Louisville. Welcome, Dan, we look forward to hearing about your office.

MR. SUTHERLAND: Thank you.

I think I've achieved the hardest thing of the day, making sure I've got the little red light on.

I feel like we're a football field away. What I would like to do is have a discussion. I have a few remarks that I hope will kick us off, but I'd like to have a discussion with you about a couple of issues.

First of all, just to give you an overview of our office and what we do. And then, secondly, I wanted to talk about a really exciting new tool called a Civil Liberties Impact Assessment, and we're going to go into more depth with that as the morning goes along.

And then I'd like to talk to you, finally, about the new Privacy and Civil Liberties Oversight Board, which I've been nominated to chair, and that's really where I'd like to have some discussion with you. So, that's basically where I want to go over the next few minutes.

I wanted to thank Hugo, John, Ken for inviting me. Hugo, I know, wanted to be here. He was exchanging voicemail messages and email messages with me late last week about this, and what I should be saying, so I appreciate all of them.

Thanks to Howard, and really all of you for your service. I've known about the DPIAC since the first days when the Department first started -- Nuala and I shared an office -- the two of us shared an office, and a single employee -- that was it. That was the whole group, right there. So, we shared in a lot of different projects, and I've known about the DPIAC all along, but I believe this is the first meeting I've ever actually been to.

So, it's a big oversight, and I'm glad to finally be here.

We do work very closely with our colleagues at the Privacy Office and I wanted to acknowledge that and let you know the really good work and relationship that we have – John has already referenced that to some extent.

But we've, for example, we hosted -- co-hosted -- a seminar of CCTV -- a workshop on CCTV, it was in this room, wasn't it? It was in this very room, a few months ago, and I think we're going to look at some things we can do, ongoing.

We've worked very closely on -- you've talked about the cyber issues, again, it's a classified program, but we're working closely together on that, on the National Applications Office, which has been in the news quite a bit, and a number of other projects like that.

One other thing that I'd mention is that, as we have developed this new tool, a Civil Liberties Impact Assessment, we have really benefited from discussions with our colleagues at the Privacy Office, with their experiences with the Privacy Impact Assessment -- lessons learned, how did you do your template? All of those different things. And I actually sat in on a training, 2- hour or 3-hour long training session that Rebecca Richards ran just a few weeks ago on how they do that.

So, my point is, basically, that we've had a very good working relationship, we're approaching almost all of the issues the same, but from different perspectives, so we're working on a course of issues.

Let me just tell you basically what our office does, and as I said, we'll get into a couple of specific issues.

We handle issues, as I said, almost all of the same issues that you hear the Privacy Office talking about, and then some additional ones, like, we do a lot of work in immigration law. That, you know, the Washington Post just ran a series on detention facilities and medical care, very critical, the medical care that's provided to immigration detainees -- we work on those issues very substantially, over the last several years.

We work on a lot of emergency preparedness and response issue -- I have a whole team of people who help FEMA figure out how do you deal with people with disabilities, or what they call special needs populations in emergency preparedness and response -- it's a very substantial area of the emergency preparedness field, and we have experts in the area that are able to assist them.

We work in equal employment opportunity law and a number of different areas. We have -- and I think this is probably the same as the Privacy Office, but we have a project ongoing -- or have had, at some point -- with every box on the DHS organization chart except one. And I always kid the guy who runs that one organization, that we haven't found a project with you, yet. We're going to find one.

But it's interesting to be in the place where we are, to be cross-cutting, working with, essentially, everybody in the Department, on a substantive project. We also work quite a bit with the National Security Council, the Homeland Security Council, and a lot of Federal agencies.

We do, essentially, four things. One is, we give a lot of proactive advice, trying to help shape policy, so that as policy is developed, it's mindful of our Federal civil rights statutes, and more generally, our civil liberties in the constitution. That's a lot of what we've talked about, so far, today.

The second thing that we do is, we investigate complaints that people in the public file with us, regarding actions taken by the Department, or actions by a Department person, like racial-religious profiling at the border or something like that, watch list issues -- we have a lot of disability-based discrimination complaints.

We have over -- I don't, I am not completely sure how the Privacy Office handles the complaints that they receive, but we have a team of investigators -- essentially if you're -- one of your law firms, you'd have like an internal audit group. And that's basically what we have, we have a team of people who handle these, we've over 400 of

them over the past few years, and we investigate those, that's under our team of investigators, and write reports.

We also -- the third thing we do is we do -- we provide leadership to the EEO program, in the Department, and then the last thing is we do a lot of work with NGOs, or just people in communities, trying to tell them -- trying to be an information channel, trying to bring some transparency to the work that we have in the Department, but also to bring their thoughts and ideas into the Department.

So we do roundtables around the country, particularly with American-Arab, Muslim, Sikh, South Asian communities -- we do that in six or seven cities, and a number of other efforts like that.

So, that's just generally what we tackle.

John talked about training, and we have seen training as a really essential element of what we do. When I first started, all we had was myself, and the seven or eight lines in a statute. And what do we do?

And I sat down with Secretary Ridge, and I gave him a list of ideas that I had for things we should tackle, and one of the bullets I had, there was training. And he had circled that one. And he said, "You're going to have a very small staff, and you've got 200,000 colleagues. The only way you're going to bring your expertise to all of them, is through training programs."

So, we developed something that we call Civil Liberties Institute, which is a package of training programs on a wide variety of topics.

For example, we have one on how to screen people who wear religious head coverings -- either coming in and out of Federal buildings, or particularly, at airports.

We have some training on how detention -- and people in the immigration system, but particularly in the detention facility -- should response to people who are asylum-seekers, the special considerations to that, that people who are asylum-seekers would have.

We have training on basics of Arab and Muslim cultures and traditions and values. And then we're working on something that I think both Toby and John referenced, which is a training program that deals with State and local Fusion Centers, just the basics of privacy and civil liberties protection.

So, that's this whole bundle of projects we call Civil Liberties Institute.

We also work quite a bit on redress issues, I was the co-chair of the Department's effort -- the Department's Governance Board -- effort to create what has become DHS

TRIP, which I believe you're familiar with, if not, we can talk about it, to some extent, but it's the redress process that travelers can have.

We also created what we call the Incident Community Coordination Team, which allows us to be in direct contact, quickly, with leaders of the American-Arab Muslim and South Asian communities, in the event of a terrorist attack, or some significant incident.

We've used it, we've actually activated the team four, five, six times. It's primarily been, for example, like after the August 2006 London bombing arrests, we activated the team, and it was able to -- it's a way for us to get the FBI, our intelligence people, our operations people, TSA, and others in touch with leaders of the American-Arab and Muslim communities to talk through issues.

And that's something I could -- and would like to -- talk about for an hour, but I don't have that, particularly. But I'll just -- this is just a highlight of some of the things that we have handled.

Okay, let me dive into two things, specific issues, that we were asked to talk to you about, and the first is this new tool called a Civil Liberties Impact Assessment. Of course, you're familiar with a Privacy Impact Assessment, these have been very important, I think, across the government, but I have seen it within our Department, in making people aware, as they're developing a project, how do we answer these questions that have been given to us? It expands their perspective, and I think it’s been really significant there.

Now, Congress has required us to expand that into a related, but complimentary subject area called Civil Liberties Impact Assessments. In the 9/11 Recommendations Act, there were Civil Liberties Impact Assessment required on three programs -- I can tell you about each one particularly if you'd like, but they relate to a variety of different, primarily, intelligence programs.

And then the Congress started to think about applying it in some other areas, so in the Appropriations Act, the 2008 Omnibus Appropriations Act, it said that no funds should be expended on the National Applications Office for another program called the National Immigration Information Sharing Operation, until -- it says -- the Secretary certifies that these programs comply with all existing laws, including all applicable privacy and civil liberties standards. And so, we have decided, let's use this tool -- the Civil Liberties Impact Assessment tool -- in those specific programs, as well.

We've also had components say to us, We're not required by statute, we're not required by OMB or anybody else to have a certification of this, but we would like to get a certification, we'd like to get your thoughts, and can you go through this formal process with us?

So, what is a Civil Liberties Impact Assessment? It's really, basically, a comprehensive template of questions that you would ask, how would this program -- or

does this program, if it's an existing program -- impact upon people's civil rights and civil liberties? And it's been a fascinating intellectual exercise to figure out the answer to that question.

It's really, I think you could teach an entire law school seminar for a semester on the questions there. We have bundled the questions -- and I'm not going to go into great depth, because you've got a panel that's going to talk about this is some -- in a lot of depth a little bit later on -- but basically we've bundled up questions in several different groupings.

For example, we have a whole set of questions that relate, say, what is the impact of this program on particular individuals, or particular groups? Like, racial or religious ethnic minorities? People with disabilities? People with limited English proficiency, and others?

So, looking at how would your program impact on specific individuals or specific minority groups is one whole set of questions.

A whole nother set of questions deal with the influence of government -- how does this program -- does it increase the authority, the control, the influence of the Federal government, vis-à-vis State and locals? Or the Federal government vis-à-vis the individual? Or the Federal government vis-à-vis the private sector? So, again, that's a complicated set of questions, but that's the whole, the analysis that we want people to go through.

We have a whole nother set of questions that deal with notice and redress. A whole nother set of questions that deal with alternatives. As you look at your program, is this the least restrictive alternative? Is there any way you could minimize the impact on civil rights and civil liberties and still achieve your objectives? So, we go through that analysis. We also have a section on safeguards, and that includes some things like -- do you have embedded legal counsel? There are Congressional reports that are required -- things like that, some sort of oversight, that sort of thing.

So, we're excited about this tool, we think that -- I've been here for five years -- we think that this development, which is just over the last six or nine months -- could be one of the four or five most significant things we will ever do. It will be a tool that will hopefully be long-lasting, and will change the way people look at their programs.

So that's the Civil Liberties Impact Assessments, and again we'll -- we can go into that in as much depth as you want to.

I would like to dive into the Privacy and Civil Liberties Oversight Board just for a couple of minutes, and then ask for your thoughts on it.

You are real experts in the field, and so I really appreciate your thoughts on how this new Board should develop, what it should do, and how it should go about its business, what issues it should tackle.

I have been nominated to be the Chairman of this new Privacy and Civil Liberties Oversight Board -- it's an honor, and I'm excited about it. I'm excited about it for two reasons: one, it's a fascinating opportunity to start an agency from zero, there is nothing, and to build it up from there. And so it's a really neat entrepreneurial opportunity within the government sector, which you don't typically get.

And the second reason I'm excited about it, is because I think that this new Board, as it's been restructured, can be a really significant asset to the Executive Branch, and also the Congress, as they are tackling some of these really complex issues over the upcoming years -- there are a full slate of security issues on everyone's plates and will be for a number of years, and almost every one has a civil liberties, privacy, impact or perspective to it. And so, these are very important issues that I think the Board can play a role in.

So, let me just describe to you the structure of the Board, in case you're not familiar with it.

This -- the previous Board -- there was a Privacy and Civil Liberties Oversight Board that existed, and it was disbanded by the 9/11 Recommendations Act, which passed, as you know, last fall. So the Board actually went, closed shop last fall, and I think it was actually done in January. So, this is a totally new entity.

It will be an independent agency, not part of -- as the old Board was -- part of the Executive Office of the President -- this is an independent agency. It will have its own staff, and it will have its own budget. These are not advantages the previous Board had.

And I think because of these three things: independence, staff, and budget, the Board has a chance to be a significant asset, and a significant player on these issues.

Its statutory responsibilities are three, really: to give advice to the Executive Branch, to try to help shape policies before you get too far down the road, it helps to shape policies and give advice on how to shape policies.

The second is, it will be very interactive with the Congress. And the statute actually says it should be helping Congress review proposed legislation, regulations and policies, related to efforts to protect the nation from terrorism. And I think this is a really important piece -- that members of Congress, the Congressional staff -- really would like to have a group of staff experts who they can call on, brainstorm with, talk to, about these issues.

And then the third -- well, I guess related to that, I'm sorry -- it's supposed to provide oversight of actions taken by the Executive Branch.

So, then the third general area is, it's supposed to coordinate the activities of the various privacy and civil liberties officials around the Executive Branch. So, it's supposed to bring together all of the privacy officers, the civil liberties officers around the Executive Branch and work with them on training, cross-fertilization of issues, maybe attempting to enhance their stature and their influence within agencies and all of that.

The Board will consist of a Chair, the Chair will be a full-time employee, and then 4 other Board members, 2 from each political Party, who are part-time Board members.

The statute -- the authorizing statute -- gives the Board the opportunity to be funded at $10 million annually. Now, you have to go through Appropriations, that's just the authorizing statute, but eventually it will be up to about $10 million, annually, under the authorizing statute. Which, it seems to me, would be able to hire 30 or so expert staff, which would make it a really substantial group of people looking at these issues.

I have been nominated along with General Frank Taylor, who is the Chief of Security at GE, and Professor Ron Rotunda, who is one of the nationally renowned constitutional law professors in the country.

The two nominees that represent the input of the Democratic leadership have not been announced. So there are the three nominees, but not the others, at this point.

It seems to me that one of the untold stories of the past several years has been the development of a privacy and civil liberties infrastructure within the Executive Branch. We now have embedded privacy and civil liberties officials, obviously, in DHS. We were the first with a -- and Officer for Civil Rights and Civil Liberties and a Chief Privacy Officer, by statute. But now they're in DNI, DOJ, the Terrorist Screening Center, and other places. More are being added at this time -- one of our great friends, the, Lyn Rahilly, who had been at the Terrorist Screening Center, is not the Chief Privacy Officer at Immigration and Customs Enforcement. And this is happening in a number of agencies, I just was contacted by a new colleague from the Treasury Department, who is supposed to set up a privacy and civil liberties entity within the Treasury Department.

And, of course, there are Boards like the DPIAC, which have not existed before. So, I think there's an infrastructure that is beginning to take shape, and so far what we have had is embedded privacy and civil liberties officers, and officials.

Being embedded is really important, because you're able to sit at the table with your colleagues, you talk with them, you go to lunch with them, you do things together with them, then they get to know you, they invite you to look at policies with them. So you're embedded, you're part of the team. They trust you with their thoughts, they brainstorm with you, because you're as part of the team, you're embedded there with them.

This is how the Privacy Office and our office have worked over the past 5 years, and we're really getting some momentum. I can tell you, we spend a good bit of our time in our office talking about, how do we deal with all of the opportunities that have been placed in front of us? And I think the Privacy Office is in the same place.

So there is momentum that has been built over some years, as we've developed trust among our colleagues, by being embedded.

What is missing in the infrastructure, though, is an independent agency, that is also expert on these issues. And the Board fits that piece of the puzzle -- the Board is separate from Homeland Security, FBI, DIA, CIA -- anywhere -- it will be independent, and because of its independence, it will be a perfect compliment to the people who are embedded, and hopefully will enhance their work, and their stature, and their influence, and sometimes be the voice that is necessary -- the bad cop, maybe, that is necessary – or to play the good cop in other circumstances.

It will be a -- by being independent, by having Board members who have sat terms in office, by having its own budget, it can play another unique, important role in the whole picture.

It also has the ability to subpoena private entities to get information that it needs.

So, I think that maybe I will stop there and ask for your thoughts on how this new Board might go about its work, in terms of mechanics, operation? But also, what issues do you think the Board should be tackling? I'll be taking some notes, and I can share with you some ideas that I have already heard, and things that I think will be significant areas for the Board to be looking at, but I would be very interested in hearing your ideas.

And with that, I'll just say thank you, and see if I can turn it over to you, Howard, and see if we can just generate some discussion?

CHAIRMAN BEALES: All right. Thank you very much, Dan. I'm sure we'll have a lot to say.

Renard Francois?

MR. FRANCOIS: Thank you for your time.

And I just wanted to go back -- I have two questions -- I wanted to go back to something that you said about one of the roles of your office being to, a public policy role? Giving advice on certain policies? And one of the subcommittees of this committee is looking at information sharing, between Federal agencies and non- Federal agencies, at a time -- basically after a natural disaster or time of emergency.

And I was wondering if you all had tackled an issue like that, or had thoughts on issue such as that?

MR. SUTHERLAND: We are on the same work groups as the Privacy Office would be on, in the information- sharing environment. There's a lot of work that we do, and the Privacy Office do in that area, in a variety of different work groups. So, the answer to your question is yes, we do have a lot of thoughts on it. And for your subcommittee that's tackling those issues, we would be very happy to have someone come and sit and give you some of our thoughts, and then maybe be a resource to you, as well, so that you have a name, a phone number where you can bounce some ideas off of somebody.

MR. FRANCOIS: And my second question is probably a little bit more random, it's the lawyer in me, and I notice that in terms of the Privacy and Civil Liberties Oversight Board you talked about, you have the power to subpoena privacy entities, and I just had wondered how was that enforced? Is the structure of the Board going to be similar to Federal Trade Commission where you have attorneys that can issue subpoenas or investigative demands with some sort of enforcement authority behind it, or what is the, kind of teeth that enforces the subpoena, or do you have to go through the Department of Justice?

MR. SUTHERLAND: Yeah, I wish I had -- I need -- I don't have the statute in front of me I left it in my briefcase here, but you need to go through the Department of Justice.

I, you know, this is new territory for us, so we're not sure how it will play out. My initial reading on that is that that is a good development, because you have some check and balance in the sense that you wouldn't have a rogue agency out issuing subpoenas to anybody, at any time. You'd have some checks and balance to it, and the Department of Justice attorneys helping to enforce that, and bring some rigor to it.

So, that is how it works, it's not the agency itself issuing the subpoenas and enforcing the subpoenas and going through Administrative Law Courts to get them enforced. But, it's new, it's a virgin area, so we'll have to see how it develops.

CHAIRMAN BEALES: Jim Harper?

Mr. Harper: I, too, have passed a major test by getting the little red light on, on my microphone.

The TSA announced a policy about a week ago on ID requirements at the airport checkpoints. And I wonder if you had an opportunity to review that policy change before it went into affect, and whether or not you did -- if you have an opinion on the sort of new state of mind requirement that someone who travels without ID must not be willful, or else they'll be prevented from traveling.

Do you have some observations on that, and what involvement did you have in the policy?

MR. SUTHERLAND: TSA has its own Privacy Officer, Peter, it has an Office for Civil Rights and Liberties, and so they give advice directly to TSA and then call in those of us at headquarters at particular times.

The new package of policies that TSA has put in place -- the Checkpoint of the Future -- which they are modeling at BWI, they did ask us to come in and look at some of those, and some of those are very significant in terms of redress.

They've developed some systems with the airlines where they can clear up a lot of the errors -- the misidentifications that happen. We're very hopeful, crossing our fingers, that what they hope will happen, will actually play out. The early reports are that the number of misidentifications are going down a good bit.

Specifically to the identification issue, I personally was not involved, and so I'm going to defer on that. I'm going to find out what advice we gave, and I will let you know. I will call you and let you know what we worked on in that area, if you don't mind.

CHAIRMAN BEALES: Joe Alhadeff?

MR. ALHADEFF: Thank you. Apparently, all of us are studiously ignoring the request you made for advice.

CHAIRMAN BEALES: You raised your tent before he asked for advice.

MR. ALHADEFF: I know, but still it's -- I'll phrase the question in a way that might also be advice, so that I -- I try to respond to the question that you asked, as well as ask the question that I wanted to.

The -- and this related back to your comment on Fusion Centers, and also to John's testimony related to that -- but it's a larger issue which I think your organization is perhaps well, or even uniquely suited, to deal with.

And that is, as we get into this information- sharing environment, which is essential for the security of the country. We have a situation where people who are used to dealing with a varied form of information, are sharing information with people who are used to dealing with a very specific form of information.

And many of the first responders at the State level, are used to dealing with criminal information from a criminal justice system. And that information has boundaries and rules, but it doesn't have a lot of the grey area and permutation that a lot of the more robust information that would come from, let's say, accessing a database who has information on people who are merely visitors to the country, but has no context related to them beyond that.

And so the question becomes, the initial access, or the process, or the screening related to a legitimate question that entails that information is obviously straightforward in its sense, and makes sense.

But a fact that a vestige of that information may somehow stay in a system that wasn't designed to control that type of information, creates very substantial concern. And the question is, how can your office help to address what is an unintentional downstream consequence of a legitimate first access which leaves a footprint of some kind in another system that was not designed to deal with that information, and therefore there are privacy issues, especially since a number of those systems don't come under the same PIA rigor that some of the Federal systems do.

MR. SUTHERLAND: I think you have stated very eloquently, a substantial issue. And I'm taking it as your advice, or recommendation that, if I'm confirmed to lead this new Board, that this is something this new Board needs to keep its eye on.

The answer with regard to our office is, we are developing a training tool with the Privacy Office, that will hopefully inform State and local Fusion Center employees, hundreds of them out there, about issues just like you advised.

Now, the training product itself would be sufficient. So, we're also developing contacts, or relationships in these State and local Fusion Centers, where they would hopefully, then, begin asking you questions, picking up the phone, saying, What do you think we should do in this situation? We have had that experience already in these early days, where people in the State and local Fusion Centers have expressed to our folks, concerns about a particular scenario, or a broad policy issue like that, and have asked for our help in figuring out the way forward.

So, we are encouraged by the appetite within State and local Fusion Centers to get the answers right, but the issues are substantial, and I think will grow, and are complex.

So, we're hoping that the training will address it, but then we -- we just are going to have to have an open line of communication with them.

CHAIRMAN BEALES: Ramon?

MR. BARQUIN: I've got two questions and they're interlinked, and depending on your response, I may have some advice, but --

[Laughter.]

MR. BARQUIN: -- this is specifically tied to, first of all, the DHS situation -- if you could give us a bit of an idea -- of how we're doing, vis-à-vis Executive Order -- I always get it wrong, but I think it's 13766 -- the one that has to do with limited English proficiency citizens. So much of what DHS does, in some way, is addressing, you know, individuals who are, almost by definition, of limited English proficiency.

So, I would like to just understand how we're doing in that area, which I know is one of specific relevance to civil rights.

But, tied to that, I also want to bring up as a question, the privacy implications of both the language and the cultural usage, specifically in terms of redress. And I mean, something as simple as, for example, the issue of a name, as you know, in Spanish, you know, heritage, you use your father's last name followed by your mother's last name. But then when you come to the U.S., you know, that often gets changed. It takes awhile before it sinks into the individual that, you know, that your name is not really Ramon Barquin Cantero, but Ramon Barquin, or whatever.

And when you are trying to find appropriate ways of redress, then you have the need to be able to map, you know, across all of the different databases. So, it's a bit of a double-edged sword, because it has privacy implications if you get it wrong, with false positives. On the other hand, you need to get it right to be able to redress when there is a need for individuals, such as this.

MR. SUTHERLAND: Excellent questions. The second one is a core issue that we deal with all the time. Every day, every week, we're dealing with that specific question.

We deal with it quite a bit in, among people with Arabic names, or who come from the Muslim world, generally. You know, the name Mohammed or some derivative, you know, covers 500 million people -- Mohammed, Achmed, something -- and that creates a lot of misidentifications in our systems, we know that.

And there are tensions between the, maybe the privacy interests and the civil rights interests there. We find that the civil rights groups who represent -- whose constituents tend to be from a particular minority community, are much more willing than, perhaps, the privacy community would be, to give information to TSA, or whoever, in order to clear up those watch list issues. They believe that their constituents would be very glad to give date of birth and a number of other identifying information, so that you wouldn't have these issues. That -- in other words, they're willing to respond to it in ways that the privacy community is uncomfortable with. There has got to be some sort of balance as we approach that.

The limited English proficiency, you're asking how the Department is doing on it -- very well in pockets, and it's an issue that we need to remind people in other pockets. We know, like, the USVISIT program translates everything in 30 different languages, and USCIS has things translated in every language you can imagine.

Other times, like after Hurricane Katrina, we were called by someone who was in a small town in Alabama, on the coast, that had quite a number of Vietnamese and Cambodia fisherman in a community of several hundred -- perhaps even a thousand --

people who were refugees from Vietnam and Cambodia, who didn't speak much English at all, and no one walking through that town had materials in their language to give them.

And we tried to -- and finally we just went to a translation service, paid for it ourselves, and took it down there and somebody handed it out to them, particularly. To try to respond to that, we are working on internal policies and regulations on the LEP issue.

So, I think, on the whole -- and it's also part of the Civil Liberties Impact Assessment -- on the whole, it's an issue that people within our Department are aware of, just purely on operational grounds. They don't know Title VI of the Civil Rights Act exists, necessarily, but they know they need to get some information to people in airports, or whatever, in different languages.

But, we need to make sure that Title VI of the Civil Rights Act is also in people's minds, so that they get the full sense of the requirements there for dealing with people with limited English proficiency.

CHAIRMAN BEALES: Lance Hoffman?

MR. HOFFMAN: Thank you.

This is a question that really relates to when you get involved -- this actually relates both to your current position in DHS, but also the potential new position -- but in particular, let's focus on DHS, for a moment.

You mentioned, for example, going out and giving advice to people in the Fusion Centers, and trying to get some program worked up there. One thing we've noticed, DPIAC, is a lot of programs get started, and then sooner or later, they get some momentum, and then somebody thinks about privacy somewhere along the way.

What are you doing right now, and what can you see doing in the future, to build it in, rather than try to bolt it on?

MR. SUTHERLAND: That's a daily issue with both us and the Privacy Office. The Privacy Office had the advantage of having a Privacy Impact Assessment and it's -- there's certain points at which, in the system, at which you cannot move forward without having that box checked. That's one of the advantages of, perhaps, institutionalizing the Civil Liberties Impact Assessment, you would get these questions asked early on.

We are constantly trying to let our colleagues in the Department know about the expertise that we offer. And sometimes the lesson is best grasped when there's been a failure. For example, there was one component that instituted a new policy, it created a huge firestorm, and then they asked for our help. And for months, we have been spent trying to help them get their way out of a problem that would have been fixed early on, and the head of that component in one of our senior leadership meetings, put his arm

around me -- I was sitting beside him -- put his arm around me, and said to all of this colleagues, he said, "As the current chief center, I highly recommend you talk to him. He can help you with your problems early."

And so, that's one where we try to jump on that, and say, "Look, we can help you with this problem." And we are having a lot of success.

I had -- I was just walking down the street the other day, and the head of one of the component agencies called me on my cell phone and said, "I've got a situation, what do you think?" And it's somebody we had never had any contact with before, but he had been exposed to the kind of expertise that we, hopefully, can offer, and he called me on my cell phone, and asked me, "What do you think about this situation? What can you do for us?"

So, there's -- that's the informal, sort of, networking part of it, and the institutionalizing is by having something like a Civil Liberties Impact Assessment. We also have a very, very supportive Secretary and his staff, and we are very much -- the past couple of years, getting phone calls from components saying, The Secretary's Office tells us we've got to get your approval before we move forward, what do you think?

So, that sort of leadership-driven aspect of it is really important, as well.

So, I'm not sure that I'm totally answering your question, but that gives you a flavor, I think, maybe, for how we're approaching the issues.

CHAIRMAN BEALES: Okay.

If I could just follow up on that a little, and this goes more to your new role. I mean, you know that -- some of your ability to do that comes because you're embedded –

MR. SUTHERLAND: Exactly.

CHAIRMAN BEALES: -- that you're part of the team and helpful. Being the one pointing the finger, as the independent Board, arguably makes people less willing to come to you early, to figure out, you know, to build it in rather than bolt it on. And I'm wondering what you think about addressing that tension, because as you move to the independent rather than embedded role, it's important -- I mean, the embedded role, I think, is important and valuable for all of the reasons you talked about, but --

MR. SUTHERLAND: Well, I'm, you know, I have different thoughts on -- I think one is that the independent can point the finger, can raise the red flag that then enhances the stature and the influence of the embedded. So, if there's a Department of Homeland Security program or policy that the five members of this Board are concerned about, and they raise the red flag, that means somebody's going to call John or Toby or somebody and say, "What are we going to do?" We've got these people who are -- we've got to respond to. So there's, I think there's that element of it.

I imagine that this Board will develop good relationships with certain agencies, you know, the DIA, for example, you might have friends there, and they might start to draw you in, and say, "Look at these programs with us," and then that will build some momentum to it. That's the way it has worked within our Department, success has bred more success, word-of-mouth business.

This Board, however, is independent, and its responsibility is to be independent, and to be very interactive with the Congress, and transparent with the Congress, and helping the Congress, as well. So, I do think there will be points at which Executive Branch agencies will say, "Thank you for raising the red flag, we have our own people, and we want to work through these issues with our people here, internally."

The Board will have really served its purpose by elbowing people in the ribs, raising the question they didn't want to have raised, and then requiring that there be answers raised.

CHAIRMAN BEALES: John Sabo?

MR. SABO: Thanks for your openness to advice. I have three pieces of advice, this is great. Although the advice may not be good, I have three pieces of it.

One is, you talked about bringing together Privacy Officers, and then you talked about relationships with a Board, such as this particular Advisory Committee. I think that's a great -- in your new role, I think that's a great thing to think about. We've got the DPIAC, and we focus on DHS-specific issues, data integrity, and privacy, although we did the framework for evaluating programs which I think is very useful, and included civil liberties.

But we exist, and we focus on DHS programs, and those seem to cause a lot of -- seem to have embedded a lot of the issues you've talked about.

There's also the Information Security Advisory Board run by NIST. And that was specifically mandated to look at both data security and privacy. And NIST deals with operational privacy standards and guidance.

So, my first suggestion is that you leverage the other existing committees and boards in an ongoing way, not just occasionally speak, but figure out how to either leverage, or provide cross-pollination or input, and see if initiatives that are underway in these other boards, actually fit into this wider scale.

I think you'd find that there are issues or is, were, by collaborating or at least thinking up agendas, there can be much greater values. That's one piece of suggestion.

The second one is, looking at the collections of systems and programs, and one of the problems that I see is that program managers or specific agencies are focusing on their issues. Nobody's looking at the whole elephant, everybody's looking at, you know, the

tail or the toe or the trunk, and dealing with privacy or civil liberties here, and dealing with it here.

But cross-government -- if you look at the programs we just talked about this morning: USVISIT, ESTA, Einstein, REAL ID, there's probably scores of programs out of all of these implications that share data with one another, and nobody looks at that. And I think that was raised earlier.

So, I think there's a very strong role for looking across programs, across agencies, and looking for common issues, and then helping develop policy recommendations as you talk about, et cetera, or recommending action to Congress.

The third area, I'd say, somebody needs to look at, which is very hard to do, is the world of operational policy, because I see a lot of attention given to the policy statements, but when those statements and positions, and policies get translated into operational guidance, whether it's guidance at the State and local Fusion Centers, you talked about training -- what's happening on the ground? Very little attention paid to what is actually running our systems, which is either code, or operational policy. And things like, I don't want to talk about data integrity -- issues like the efficacy of data, used for particular programs -- what's the data source? And what -- what cleansing is associated with it? And what common data dictionary components are there, and what standards around longevity of data or current accuracy of data, as they impact the system?

So, those are three areas, I think, no one is focusing on, in any ongoing, strategic way, and could be a good place, if you get staffed up, to look at.

MR. SUTHERLAND: Excellent, thank you.

CHAIRMAN BEALES: Neville?

MR. PATTINSON: Quick question on the scope and tasking of this Board that will be set up, an independent Board, obviously, with yourself as a -- potentially the Chairman of that Board -- how do you pick the subjects that you're going to work on how do you set priorities in that Board, and on that basis of asking that question, I'd certainly like to suggest a mechanism for the Board to receive input from the public, from agencies, from Congress, whatever it is, but here is an open period for requesting topics for the Board to address.

Obviously, the Board will make its own mind up, I presume, as to what it will take on, but I think there needs to be a mechanism of request. There's a whole, you know, rainbow of possible topics that you could pick up, what are the priorities, how will they be determined, and what will be the mechanism of having the Board work on these things?

MR. SUTHERLAND: Fantastic question. The statute – I failed to mention – the statue says that there must be public hearings, so there must be that, exactly what you're talking about -- where the Board is interacting with the public, and getting their feedback on what the issues are that they see.

I think that the issues that -- let's say that there's 30 people working there, obviously you're going to have to pick and choose which issues you dive into. I think that the issues the Board chooses will be based, is part on what the members of Congress who are most interested want the Board to be looking at.

And so, as I've gone through the process so far, I'm going up and talking to the staff on the Homeland Security committees, for example, and saying, what are the issues that you see? You know, so it'll be, I think, driven, in part, by what the Congress would like to be looking at.

I think that there will also be times that Executive Branch agencies will call and say, We've got this program we're going to roll out in 6 months, we need you to take a look at it now. So, it will be driven, in part, by that, as well, too.

So, it's all three parts -- well, public, requests from Congress and from Executive Branch agencies, and then it will also be shaped, in part, by the interests and background experiences of the Board members, themselves.

I would picture that if we are privileged to be confirmed and start this Board by the time the Congress recess this summer, that we would spend the fall in a series of public hearings around the country, asking people for their input -- what are the issues that you see? And then the Board issuing some sort of report toward the end of the year, that would say, here are the top six, eight, ten, twelve issues in the privacy and civil liberties bucket. Which, essentially, would then be setting for the new Administration and the new Congress, an agenda -- here are the issues in our world that need to be addressed, and try to break them down.

I also see that it would be difficult for any group of 5 people who are experts in this area to agree on them. And so, what I'm picturing in my mind is, we might very well say, "Here are the 8 that we all agree on," and then each one of us are going to list three that are of particularly of interest of ours.

But in any case, my point would be that, if the Board is created, it would spend the next several months trying to lay out an agenda for -- that would be prepared for the new Congress and the new Administration to tackle when they came into work in January and February of next year.

It requires a huge amount of work, because at this point, the Board does not exist -- there's no office space, there are staplers, there are no pens, you have no idea who's going to issue the checks, or if you travel somewhere, who's going to reimburse you -- all of

those infrastructure things don't exist, and it will take months to develop that, while also making a substantive mark.

And that's why I am enthusiastic about the opportunity to get going as soon as possible, so that we are really ready to be of service to the new Administration and new Congress, come the January/February timeframe. If there's not action taken, that Board will not be in that position. So, we're enthusiastic about getting going, because there are so many important issues in this area that, I think, we need to tackle.

So, I hope that's partly an answer to your question.

MR. PATTINSON: Indeed.

So, in the vein of seeking input, I think this committee has looked to many of the programs within DHS over the last few years that involved PII, obviously, and how that material is managed and dealt with as far as policy and privacy concerns.

The common theme that tends to come through in many of these programs, is that PII involves identity, and identity is part of all of these programs that we deal with, in one capacity or another.

So, one of the tasks, perhaps, for your Board to consider, would be a national policy on identity -- where and how should identity be managed, and how should it be looked at, as it covers both privacy and civil liberties. And not to take the thunder out of Jim Harper, and his passion on this area, by the identity mechanisms within, off to the side today, are not clear, I think.

We see many of the agencies and boards looking at identity, one way or another, from identity theft, through to identity management, et cetera, and there's a -- if your Board is an oversight Board, you're advising Congress, you're picking up an area which is, I think, something that we need for our information society, as we move forward, that identity is a common aspect that we need to manage and have good policy around privacy and civil liberties and how that's managed in our national society.

So, that's my soap box request for your gathering of information tasks.

MR. SUTHERLAND: Thank you.

CHAIRMAN BEALES: If I could just inject a follow-up to that, and then follow-up to something you said earlier about Arab-Americans and their representatives would prefer to provide more information in order to avoid misidentification -- to some extent, the issue is, I mean, people have different preferences about what they want to part with is anonymity, or whether what they want to part with is, you know, the intrusion of secondary screening, or a physical search, or whatever.

There are some mechanisms like frequent traveler kinds of programs that sort of let people make that choice, to some extent, you give more information to sign up for the frequent traveler, and you get less hassle in actually going through the airport. But, it's not very well adapted to the occasional traveler, or that sort of circumstance.

It may be worth giving some thought to other mechanisms that let people make that choice for themselves, rather than imposing a uniform, everybody's got to do it this way kind of approach, it's not completely clear what those mechanisms might be. And if you -- if your office now has done any -- has given any thought to that, I think we'd be very interested, and maybe we could follow-up. But either in your office, or in your new capacity, it's an issue that may be worth some thought.

Richard?

MR. PURCELL: Thanks, Howard.

Hey, Dan, thanks for joining us today.

Just a piece of advice that might be helpful -- this committee's been constituted for several years now, and we've looked at a number of different programs that are technology systems, that are developed in order to carry out some sort of specific function, and generally mandated. There's been -- Secure Flight is an example, REAL ID is an example, E-Verify, as an example -- different committee members have taken different levels of exception to the veracity of these programs, the efficacy of these programs -- but as a committee, we're not able to actually say they shouldn't exist -- that's something perhaps that your Board could help to elevate as a question. Because technology systems that are mandated in the heat of an emotional moment, may not actually be as well constituted as we'd like.

What we can do, and what we have done, is look at two major components of how those systems operate in their implementation. And these two areas, I think, are ones that we can focus on, and with your help, can actually make systems that are mandated, and are going to be real. Actually, help minimize, even, a sub-optimal system, in terms of its effect on people, on our citizens' information privacy and civil liberties.

The two areas are, first of all, its vulnerability. We find that a number of these systems are being thrown together and as questions and advice have been mentioned today, they're often thrown together in ways that make them vulnerable to either mischief or mistakes. People could game the system, because it's thrown together so fast that it may not have the proper security mechanisms for authentication, for the proper person to use it, to use it in a proper way, or it could just be through simple mistakes, gaps, errors in programming, code-writing, or implementation rules; operational rules that could make it vulnerable, so that it doesn't accomplish its mission.

The other part of it is the harms that some systems do, inadvertently. The funny thing about systems is, because they're coded, that when they do create harm, it's rarely inadvertent, because machines do what they're told to do. So, it becomes a question of, how do you remedy those harms? When someone is mistakenly identified and pulled aside, and treated in a way that is based on mistaken identity, how do you remedy that? So, what is -- what are the redress procedures?

And secondly, it's not sufficient to create a work-around for redress, and just say, Oh, dude, sorry, we've inconvenienced you, you can go on now, you have to actually correct the information that caused that, so you don't have to keep redressing the same situation. And the problem with harms is that redress is only one component, and that correction is another.

And that's very difficult, because a lot of these systems are not necessarily controlled by the operator -- they inherit the data from somebody else. And how do you go backwards through a system, through three or four levels, to where you finally get at source data, and then correct that source data, and then get it to ripple back forward, so that the individual is therefore not -- no longer a delayed harm, discriminated against, or whatever, by that system.

So, my encouragement would be, when you have your staff assembled, that you give a certain priority to looking at three levels: one, should we be advising the current -- the ongoing existence of the system, in other words, is this really the system we want? And, two, if it is a system that we want, or that we have to accept, how do we, then, minimize its vulnerability, and how do we remedy the inevitable harms that will occur, just in any system?

MR. SUTHERLAND: Outstanding. I'll get the transcript, that was just great. I do believe that this Board, one of its functions or purposes should be to give voice to all range of commentary on a program or a policy that are constructive.

I mean, we see, sitting in the Department, we see at times, a group will issue a report on something, and it's not actually very well-informed, just because they're on the outside, not the inside. Our responsibility would be to have really well-informed, but a wide variety of opinions. I would think that this Board we want to foster the idea of -- if he's going to write a report, for example, on a particular project, that there's not a five to nothing Board vote that, yes, we're going to issue this report -- somebody on that Board should be writing the alternative view. Because they're on -- these are complex issues, and one value of the Board would be to lay out, in a thoughtful way, the alternative views.

And it could be on, for example, REAL ID, you could have somebody write the paper that says, “Why are we going down that path?” But, let's look at that core issue, is

this the right path we should be going down to? So, this Board needs to give voice to -- to those core issues, so that you can really address, I think, the first question that you raised, "Is this where we should be, at all?"

I think the other thing, you talk about redress, correction, the other part, though, is compensation. And if somebody loses a benefit that is a meaningful benefit -- I don't mean their flight was delayed two hours and they had to catch the next flight or something, but they lose a job -- there's compensation for that. That's got to be a central element of this.

CHAIRMAN BEALES: Dan, thank you very much for being with us today. This has been most helpful and most informative. And whether in your new role or your current role, I hope we can build a better relationship between your institution and ours, because I think we have a lot of common issues.

MR. SUTHERLAND: Absolutely. We'll make sure if you don't have our contact information, that you get it -- that they send it all to you, because I would like to -- I think that we have a lot of issues in common, a lot of areas where we could help you, and we could certainly benefit from your thoughts, so thank you.

CHAIRMAN BEALES: Thank you very much. Our next panel is going to examine the Office for Civil Rights and Civil Liberties and its use of the Civil Liberties Impact Assessment.

Our first speaker will be David Gersten, who's the Director of the Civil Rights and Civil Liberties Programs. He manages several units in the Office, including ones dedicated to conducting Civil Liberties Impact Assessments, engagement with American, Arab and Muslim communities, emergency preparedness, civil rights and civil liberties.

He's familiar with challenges, he's the proud parent of 5 children, including 5-year old triplets. So, Mr. Gersten, welcome.

And if I could ask you to keep your remarks brief, we've run over, I'm perfectly willing to eat into our lunch, but I understand that our last panelist has to leave, so I want to make sure that we have time for her, and for questions, if we can.

MR. GERSTEN: I'm perfectly happy to eat into lunch, as well.

Thank you very much for have us here today to talk about the Civil Liberties Impact Assessments.

Quick background, I know that Dan covered some of the territory, but I thought I'd get a little bit more in- depth, and talk about what we've done, so far.

What we're really talking about with Civil Liberties Impact Assessment, is institutionalizing something that the office has been doing, ad hoc, for many years. We

have been reviewing programs, reviewing clearance for testimony, policy, regs, SOPs, Con Ops, directives, instructions, et cetera, and providing our own impressions of the impact on various statutes, regarding rights and liberties. So, we've been doing this for years.

We've also, of course, responded to complaints, our Review and Compliance Division handles casework, and issues recommendations to the component of DHS that is charged, in some manner, with a violation. And so we are - have been in the business of reviewing and providing recommendations for many years.

Now, Congress has given us a path and a push to formalize these ad hoc assessments. In the 9/11 Act, they specifically charged our Office with conducting Civil Liberties Impact Assessments, the first time this term had been used in statute -- for three specific programs: the Information Sharing Fellowship Program, the State, Local, Regional Fusion Centers Program, run by the intelligence and analysis component of DHS, and the Interagency Threat Assessment Coordination Group.

In addition, two other programs, as Dan mentioned, were noted in the Appropriations bill, in the, I guess you would call it a comment section, as requiring a review, or a certification by the Secretary, which we interpreted to mean a review, Civil Liberties Impact Assessment was in order. And we have been working to create the program ever since these mentions in statute have occurred.

We've developed templates, we've developed questions like the ones that I've passed around, to ask Program Officers. We've developed the matrix for assessing the qualitative analysis, looking at the discrete facets of legal authority, structural, constitutional issues, Bill of Rights issues, statutory rights issues, unenumerated rights, as well.

We've also reached out to others, to seek input. Primarily, of course, right off the bat, we sought some input from OMB, and received their assurances that they were enthusiastic about this. And we also talked with our partners in government, other Civil Liberties Officers, and the Privacy Officers throughout government.

We began very quickly to meet with the Civil Liberties Protection Office at ODNI, and with the Privacy Office at DOJ to seek their input. We've also gone out into the public sector and met with key advocacy organizations. I met with the Privacy Coalition in a small meeting, and then made a presentation in which I described some of the questions that we'll be asking in our assessments.

We've also met with key racial and ethnic groups, we’ve brought the questions that I've passed out to you today to the Department of Justice Engagement Roundtable, with American-Arab, Sikh, and South-Asian Muslim community leaders, to seek their input.

We also brought Sharon, who graciously, actually met with us, and was enthusiastic about providing us with input for our process. And we've conducted some briefings for Hill staffers, in particular, those who had their part in placing this into statute.

Now what is the Directive, actually -- what does the Impact Assessment actually do? It looks at how a program or a policy might impair a particular right or liberty, it looks for feasible -- to implement countermeasures to the impairments that we may find, and it identifies risks, and lays the groundwork for the program to improve its practices, to mitigate or eliminate the risks.

And, of course, it also provides the groundwork for CRCL, our office, to be better able to enforce the statutes it's responsible for, and to offer training, and to improve the public awareness of the programs that we're reviewing.

We have, thus far, conducted and finalized only a handful of the Impact Assessments. We have finalized the Impact Assessment for the Information Sharing Fellowship Program, and delivered that to the intelligence and analysis component who, in turn, vetted it and delivered it to Congress. And we have developed our -- we have finalized our Impact Assessment for the National Applications Office, again, a program run by INA, and they have, in turn, delivered with a package, including the Privacy Impact Assessment, as part of the certification called for in the Appropriations bill, delivered our Impact Assessment to Congress.

We received very favorable feedback from the component that we work with, with the Program Officers that we work with, all the way up to the head of NIA, Charlie Allen, who issued a memo back to our office, accepting the recommendations of our Impact Assessment for the National Applications Office.

And, I think that that is how we envision this working -- we expect that there will be, of course, some give in, during the drafting of the Impact Assessments themselves, where we are working with the Program Office, to try and figure out how to improve the program, even before it launches, but then as we make our final recommendations, we're expecting that the Program Officer will issue their own response to our Impact Assessment.

We're also working to institutionalize this in other ways -- we're drafting a directive, as part of the DHS Directive System -- that will call on the Program Managers throughout the Department to inform our office of a policy or procedures that may need some sort of threshold assessment to determine whether or not a full Civil Liberties Impact Assessment is required.

That's about all I wanted to mention to get us started into a conversation. I'm hoping that Sharon and Tim can add to the discussion.

CHAIRMAN BEALES: All right, thank you very much, David.

Our next speaker is Timothy Edgar, who is the Deputy Civil Rights and Civil Liberties Protection Officer in the Office of the Director of National Intelligence.

Welcome, and we look forward to hearing from you.

MR. EDGAR: Thank you very much, it's my pleasure to be here to talk to your committee.

My name is Tim Edgar, I am actually the Deputy Civil Liberties Protection Officer for civil liberties at the Office of the Director of National Intelligence. Our office was created in the same legislation that created the DNI in 2004, the Intelligence Reform and Terrorism Prevention Act, and my history is somewhat unique, because I came to that office shortly, really, within a year of when it stood up, and was the first hire by my boss, Alex Joel, who is the Civil Liberties Protection Officer from the ACLU, from the privacy and civil liberties advocacy community.

So, I have a different perspective than some of my colleagues who have a government or intelligence community background, but it's been a fascinating journey, as you can imagine.

So, we're here today to talk about Civil Liberties Impact Assessments, and the role we might consider using that tool within the intelligence community, in the Office of the Director of National Intelligence and I guess I'd start out by saying, echoing something that David said, which is we -- in our office -- have been, have a series of listed statutory duties, under the Intelligence Reform and Terrorism Prevention Act.

And probably one of the most important -- the first listed duty, and certainly one of the most important duties -- is to ensure that there are policies and procedures in the intelligence community's programs that ensure protection of privacy and civil liberties. And so, that is a broad mandate that extends throughout the intelligence community -- some of out other statutory duties apply only to the Office of the Director of National Intelligence, and so we really see that as our principal function, that one of the main reasons that our office was stood up.

We were kind of modeled on the DHS office in some ways, but there was also some differences in our office, and one of the reasons, I think, that we were made a principal office of DODNI that reports directly to the Director of National Intelligence, is the understanding that empowering a new head of the intelligence community, that would have greater powers over all 16 agencies of the intelligence community.

And particularly was going to focus -- although we're still focused on foreign intelligence and foreign powers as the main function of the intelligence community, versus law enforcement and homeland security, functions which are the functions of other

departments and other communities -- we still knew that having this Office was going to create concerns that traditional protections that the intelligence community has.

The wall that was erected between foreign and domestic activities of the intelligence community -- that taking that down and creating more information sharing was going to create additional privacy and civil liberties issues, and that having a full-time Office dedicated to that was an important part of intelligence reform.

I'd say one of the important differences of our office from the DHS, is that we actually have combined the two offices -- we didn't, Congress did -- Congress and the statute that set up our office, assigned us both civil liberties and privacy responsibilities. So, in DHS, there are two officers, and two offices with the attendant problems of figuring out which office has which jurisdiction, though they work together very well, and with us, very well.

We have that, I think, the advantage of having those in one office, and because the issues are different, but related, we are able to look at programs both from privacy, and from a civil liberties standpoint.

Another key difference is not so much a difference in law, but it's a difference in how the offices tend, I think, to operate in practice, and that is that we rely less heavily on the Privacy Impact Assessment, and the reason we do is because so much of what we are reviewing are national security systems. And because of that, the EGOV Act exempts national security systems from the Privacy Impact Assessment.

We can still use that tool, but it's not one that we see in the same way that other government offices may see on a very regular basis, because so many of those systems are, in fact, exempt.

As a result of that and because we do need a tool to implement our statutory obligations, you know, it's our intent to formalize and regularize what we have been doing on a more ad hoc basis, in a more formal assessment tool, that would examine both privacy and civil liberties issues. And so, the advantage of that being that we would perform one assessment of the program, and look at both sets of issues.

It's our intent that this tool would not be simply a “check the box,” or compliance-type of an exercise. In some cases, I think that -- you know, obviously those are important mechanisms, but we think it's important that the resources of our office, and the issues that we're examining, really be those issues that are going to be of most interest to the American people. And so, we think that it's important that in the course of that assessment, we identify those privacy and civil liberties issues that are going to really present the greatest challenges to the intelligence community in ensuring the protection of privacy and civil liberties, and then formulate substantive regulations that will address those issues.

The final thing I'd say about this tool -- which we are, I think, not as far along as DHS is in developing, but are doing some very intense thinking about -- is, it wouldn't be appropriate, in our opinion, for this to be seen as mainly a legal opinion, or an assessment of the legality of programs. The way I would put it is, just fairly straightforward.

You know, if there's a program that's illegal, it should be shut down. If there's a violation of the law, it needs to be reported and addressed.

So, we sort of -- if we come across something that might be of questionable legality, it would be our job, and our responsibility, to work through the Office of General Counsel, to ensure that that program has been reviewed and, if necessary, of course, as we would traditionally do in the intelligence community, we would, perhaps, go to the Department of Justice for a legal opinion on certain aspects of it.

I think that the purpose of having the Privacy and Civil Liberties Office, and the purpose of having this sort of assessment tool, is not to duplicate that review, or in some way to, sort of counterbalance somebody who might think that the review that was done by the Attorney General was wrong, because that's really -- you know, I think that that's really not the role of the Civil Liberties Protection Office and the DNI.

But instead to say, "Okay, if we're assuming that we've come across this program, and that it is within the intelligence community's legal authorities, and that we have complied with Executive Orders and legal requirements, what are the risks to civil liberties and privacy, of going forward with this program? And what are the safeguards that we might consider employing to minimize those risks?" That's a -- that's really, I think, the job and function of our office, and it sort of presumes that if there's something that we're doing that's illegal, that we wouldn't -- simply wouldn't do it.

So, I said a little bit about what we're thinking about, in terms of developing a more formal assessment, I did want to describe, very briefly, the kinds of things that we're already doing on a more ad hoc basis to fulfill our statutory obligations.

We've looked at a whole range of issues across both ODNI and the intelligence community. Just ticking off a couple of them -- information sharing has been a big source of work for our office, because ODNI has within it, the Program Manager for the information-sharing environment. Also an element of the Intelligence Reform Act, and we are working together with DHS and DOJ, to implement guidelines for the information-sharing environment.

Our office has been involved, together with Department of Justice, on reviewing compliance under the new surveillance authority granted by Congress last summer in the Protect America Act, which extended the Foreign Intelligence Surveillance Act to foreign targets, where the acquisitions occurred within the United States. And so our office has

reviewed those -- has participated in those compliance reviews, and has looked at that whole set of issues.

We've also, together with DHS, looked at the National Applications Office, and particularly from the intelligence community perspective, the National Applications Office being essentially another mechanism to do something that the intelligence community has traditionally done, which is to provide assistance to civil authorities under proper safeguards. And that office will be basically using intelligence community assets -- both overhead, and perhaps other assets, as well, to assist civil authorities. And so we've looked at that, and compared some of the things that they would like to do with the National Applications Office with the traditional way in which the intelligence community has gone about providing that assistance.

And then, of course, we reviewed a number of other sensitive programs that we can't discuss in an open forum. And that's another, I think, example of the difference between what our office does, and what DHS does, which is that -- although DHS, you know, itself, may have to deal with certain classified areas, such as with the National Applications Office, our office is much more frequently dealing in the classified realm.

And so, a lot of the time when we do our assessments, you know, the assessment itself will be a classified document, or even the fact of the assessment might be classified, if the program about which we are assessing is a secret program.

So, those are things that, I think, are challenges for us, that we, you know, welcome suggestions from you and from everyone else, about how to consider addressing those challenges.

I would just tick off two more things before turning it over to Sharon. The first thing is, this is something that we have really addressed, or thought about, from the very beginning of our office, even before I was hired, and the office was really an office of one, Alex Joel talked about what he calls the SAFET cycle, which is just a way of thinking about how one might go about assessing, as well as implementing, protections for privacy and civil liberties.

And SAFET is an acronym for stands for Spot, Assess, Formulate, Execute and Test. So, spot and assess would be the process of going through and looking at a program, and going through and looking at a program, and spotting and assessing those privacy and civil liberties issues that that program presents.

Obviously, in some cases that's fairly obvious, in some cases it's not so obvious. We think that that's an important part of it, but sometimes one of the problems with being a lawyer is that you're very good at that, and then you're not very good at doing the next parts of the cycle, which are really, in our view, where the value gets added.

So, you've spotted, and you've assessed the program, and you've understood where the risks are and where the problems might come up.

The next set of steps is formulate and execute. So, formulate means you are looking at the kinds of protections that might be needed to fill whatever gap might exist in the program. And this involves, oftentimes, working with the program personnel and getting them to better articulate and document what it is that they actually want to do, what their processes are going to be, what data they're going to acquire, why they're acquiring it, who's going to get to see it, what training, if any, are we going to be looking at?

And then execute being, essentially, working with those program personnel to say, "Okay, you've agreed to these protections, we may have to go back and forth on these protections, to make sure that they don't interfere with your program objectives, now how are we going to get this actually rolled out?"

And then, of course, test is the compliance review, the -- you've agreed to do it, now are you actually doing it, how are we going to figure out how to do it. And then the one thing that I think is a -- is a way in which we differ from DHS and from other Privacy Offices, is that we are working through a infrastructure of intelligence oversight, which really stems from the Church Committee reforms of the late seventies, and which is embodied -- for the intelligence community -- in its United States person rules, under Executive Order 12333. And those rules -- which have to be approved by the Attorney General for each element of the intelligence community, so that's 16 agencies, 16 sets of procedures for handling United States person information. And that would be -- a U.S. person would be a citizen, lawful permanent resident, company or organization.

And essentially, what those rules say is that in order to collect any personally identifiable U.S. person information to begin with, you have to have a valid mission to collect that information, and you have to fit it into one of the categories of permissible U.S. person information. And those categories are things like, publicly available U.S. person information, information that constitutes foreign intelligence or counter- intelligence -- other such information.

And so, essentially what those rules do -- and they apply to both the collection of the information, the retention of the information and dissemination of the information -- and what those rules do is really provide a substantive standard for how the intelligence community goes about its work of collecting, retaining, and disseminating information and then formulating intelligence from that information.

And that's an infrastructure, a set of rules and guidelines that long pre-dates the existence of our office, as well as that of the DNI. And so one of the things that we do, when we go through these assessments, is that we see how those programs are --

specifically how they're going to not only comply with their U.S. person rules, but also how they're going to address any novel issues that might come up, because in some cases these rules may be relatively old.

So that's, I think, how we, you know, are doing it at the ODNI now, and how we plan to continue to do it in the future. Some good news is that -- although our office is quite small at the present, we are looking -- we have been given some additional funds to hire additional people, and so we expect that we will -- you know, in addition to being able to develop this more formal process, we may actually have some additional personnel that will be able to assist us in executing those responsibilities under the statute.

CHAIRMAN BEALES: All right, thank you very much for being with us today.

Our third speaker is Sharon Bradford Franklin, who's the Senior Counsel for The Constitution Project. She works primarily with The Project's bipartisan Liberty and Security Committee. She previously served as a trial attorney in the civil rights division at the Justice Department as a Special Counsel in the Office of the General Counsel at the Federal Communications Commission, and is the Executive Director of the Washington Council of Lawyers.

She graduated from Harvard College and Yale Law School -- and I actually didn't know either institution permitted that practice -- welcome, Ms. Franklin.

MS. FRANKLIN: Thank you.

I want to thank the committee for inviting me to participate in this hearing here today, and I also want to apologize in advance -- when I was invited late last week to participate, I was happy to have this opportunity, and I told them that I would try to squeeze this in between two prior commitments, but that will require that I leave here -- I had said 11:00, but I think I can probably stretch it to about 11:20. So, I apologize in advance for that.

But I thought it was very important for me to be here today, and particularly, I wanted to commend the Department of Homeland Security for taking these steps to institute these Civil Liberties Impact Assessments.

The Constitution Project is a non-profit organization here in Washington, D.C. that promotes and defends constitutional safeguards, by bringing together people from across the political spectrum who share a common concern about preserving civil liberties.

Our Liberty and Security Committee was launched in the aftermath of September 11th, and it comprises a variety of members from law enforcement community, legal academics, former government officials and advocates, and they all work together to try and promote policies that will preserve both our national security and our civil liberties.

And our Committee has specifically recommended that Civil Liberties Impact Assessments be conducted, in the context of any community considering the development of a public video surveillance system. And our Committee's analysis and recommendations may be applied more broadly to the development of DHS programs.

In my remarks here today, I will focus on three categories of recommendations for the use of this assessment process.

First, the Civil Liberties Impact Assessments should be mandatory, should be conducted for every DHS policy and program, and should require that any negative impact on civil liberties be minimized.

Second, the Civil Liberties Impact Assessment process should be as transparent as possible, and DHS should release public versions of the assessments.

Third, there are a series of specific modifications to the draft guideline questions that would strengthen the assessment process, and ensure it is as complete a review as possible.

On my first point -- you already know, and there's been some discussion today -- about the E- Government Act, and the requirement for Privacy Impact Assessments under that Act. And in addition, there's some further authority under the Homeland Security Act, requiring that DHS conduct these types of reviews.

The DHS Privacy Office issued guidance last year on conducting PIAs, which makes clear that the goal of the PIA is not only to assess the impact on privacy, but also to ensure that Department managers, "have consciously incorporated privacy protections throughout the development life cycle of a system or a program."

The questions contained in that report make clear that Department managers must identify risks to individual privacy, and demonstrate how they were mitigated.

Although the new Civil Liberties Impact Assessments have not specifically been required by Congress, other than for the three specific programs that David mentioned, DHS itself should make these assessments mandatory, and as with the PAAs, make clear that the goal is not only to assess, but also to minimize any adverse impact on civil liberties. And David discussed the authority requiring those assessments, I won't go into that as I had in my prepared remarks.

DHS should specifically endorse this process, and issue regulations to codify a requirement that such assessments be conducted for all DHS policies and programs. Further, DHS should issue detailed official guidance on the creation of the Civil Liberties Impact Assessments, as it did with the official guidance on the PIAs that was issued by the Privacy Office in May of 2007. That report provided a detailed description of what PIAs must cover, and how they should be conducted. Similar guidance for the CLIAs

would help ensure that the Department conducts meaningful reviews of each program's impact on civil liberties.

Second, the CLIA process should be as transparent as possible, with publicly released reports. To ensure that these assessments have their intended effect, DHS should publicize this new requirement, and provide transparency regarding the assessment process. The evaluation questions to be considered in the analysis should also be publicized.

In addition, DHS should release the completed CLIA reports to the public. If a given assessment includes a review of classified information, then a separate, public version of the CLIA report should be created, and released.

Finally, I want to offer a few specific recommendations to improve these assessments. I was -- had the opportunity to be provided with the draft set of questions, but I understand you also have been provided with -- that was prepared by the Civil Rights and Civil Liberties Office.

And that list is divided into 6 categories, covering impact on particular groups or individuals, influence of government, notice and redress, alternatives, safeguards, and other rights.

Each of these categories includes important questions that should rightfully be part of a Civil Liberties Impact Assessment. Beyond this list, however, I have several recommendations to strengthen and improve the assessment process, and I will go through a few of them here.

First, on mitigating risks -- as with the recommended procedures for conducting Privacy Impact Assessment, the CLIA questions should ask, under each category, what steps have been taken to mitigate the risks of intrusion on civil rights and civil liberties.

First Amendment rights -- when assessing the impact on particular groups or individuals, the analysis should include an examination of whether the program might chill the exercise of First Amendment rights, and how such a chilling effect may be minimized.

Those programs that involve surveillance, in particular, may make individuals wary of exercising their rights of free expression and association, and protection should be built into programs to minimize these risks.

Programs should also evaluate gender bias. When assessing the impact of particular groups or individuals, in addition to asking about the impact on racial and ethnic groups, people with disabilities and particular religions, the evaluation should also ask whether there will be a gender bias, and how any such bias may be minimized.

Also, when assessing the impact on particular groups or individuals, the Department should evaluate any profiling risk -- that is, a risk of racial, ethnic, or religious profiling -- and ask what steps have been taken to minimize those risks.

Since September 11th, we have unfortunately witnessed many examples of government programs that have relied on improper profiling -- particularly of Arab and Muslim-Americans -- so it is critical that programs take steps to eliminate such profiling.

Oversight -- the section assessing safeguards should be strengthened to require that managers develop and describe regular oversight procedures, to ensure that the impact on civil liberties will be monitored and minimized. This could include developing a system for regular audits, or reports to the public.

Accuracy -- the section assessing safeguards should also require managers to describe the steps being taken to ensure the accuracy of records regarding individuals. Too often, such as in the context of watch lists, intrusions on civil liberties are caused by inaccuracies in government databases.

The final recommendation I'll offer here today is on data and technological safeguards. The section assessing safeguards should also require managers to establish and describe procedures designed to ensure the security of databases. Technological safeguards, such as encryption of personally identifiable information, and digital watermarks, can help ensure that records are not improperly released, and that only authorized personnel have access.

Again, thank you for the opportunity to address this committee. I urge you, and the Department, to adopt this Civil Liberties Impact Assessment process, and strengthen the requirements beyond those in the preliminary proposal.

Thank you.

CHAIRMAN BEALES: Thank you so much for being with us today.

Neville Pattinson?

MR. PATTINSON: Thank you. My question is for Timothy Edgar. Obviously you said in the PIAs, there's a lot of programs that are exempt, and the CLIAs are fairly new to the scope of your group.

Obviously, you're doing assessments of various projects, as you've described. What guidance, or what material are you using to assess those programs today?

And as a second part of the question -- what impact are you having on those programs as you do those assessments and you feedback, provide that guidance?

MR. EDGAR: Well, as I said, we are operating more on an ad hoc-type basis in the sense that we don't have something like a form that we, you know, would use like a PIA

to go out and get a whole list of, or series of questions. But we do engage in visiting the program personnel, interviewing them, gathering information, looking at a concept of operations, I mean a whole series of manner -- ways in which you can get information about how a program might work.

And, in general, we have -- I think -- been fairly successful with the ODNI, and letting people know we exist, going out and they come to us, and ask us to review programs on a fairly regular basis. We also use some of the mechanisms David talked about -- you review legislative testimony, or legislative proposals, through the normal agency clearance process, and that can also result in issues coming forward.

And we have been, I'd say, very successful, because people within the intelligence community are very sensitive about, sort of the image of the intelligence community as being one that simply goes around and violates privacy. And I think, in many cases they feel that our office can help them in identifying things like the U.S. Person Rules, and other protections that exist, and documenting that they are, in fact, complying with those protections, or going -- in many cases -- many steps beyond what those protections would literally require, and then enable them to engage in their mission.

And I think that they feel that that kind of review is going to be helpful to them. Because even though some of these programs are conducted on a classified basis, it's common knowledge that programs get leaked, or mischaracterized in the press, and people have -- I think most intelligence officers that we've dealt with, anyway -- have generally understood the idea of the Washington Post test being very much a real test, not simply a hypothetical test. And they are looking for us to come in and provide that kind of guidance.

I think that developing a more formalized tool and set of structures is something that -- it's not just our office at ODNI, but other offices, as well, are looking at how to strengthen the ODNI's authorities.

There's been a big debate over the past few years, about -- since the stand-up of the new structure of the intelligence community -- whether the DNI has enough authority, and powers to do what he needs to do to unify the intelligence community.

And so, I think that throughout the ODNI, we are simply one of many offices that is looking for mechanisms - - formal mechanisms -- that we can use, not that there -- not that, that none exist, you know, we use the Intelligence Community Directive, the Intelligence Community Policy Memorandum, these are formal document the DNI uses, and we take advantage of those, as well.

But, I think that that throughout the DNI there’s an effort on the part of many offices to develop those more formalized structures.

MR. GERSTEN: I would like to add to that, it is important that we lessen the impression that we are acting as an Inspector General. So, the informal advice is actually oftentimes what provides a level of assurance to the program managers, that we are operating in their best interests, we are trying to serve, in a sense, as a sparring partner, so that they can improve their program.

That is why as we move forward -- and I just want to say thank you very much to Sharon, and to The Constitution Project for their recommendations, because I think they will help us improve our process -- but one note I would make is that we are attempting to make sure that this is not viewed as an adversarial process for the programs that we are reviewing. That's why I think that as we move forward, we may not want to make this a permanent, automatic fixture, to the level of a full-impact assessment for every policy or procedure or program.

What we would like is to have every program inform our office, so that we can conduct a threshold assessment to see if a full assessment is needed.

CHAIRMAN BEALES: Thank you.

If I could just ask Mr. Edgar -- does ODNI have a role in nominating people towards -- to the watch list? Or is that strictly through the component agencies?

MR. EDGAR: I -- actually, we have a very large role in that watch list process. The way that the watch list works is that each of the agencies that are what are called denominating agencies, mostly within the intelligence community, that would be -- and the FBI also, and CIA, NSA, all of the elements of the intelligence community -- have a process for sharing that information on known or suspected terrorists with the National Counterterrorism Center. And the National Counterterrorism Center is a component of the ODNI, and maintains the TIDE database, the Terrorist Identities Datamark Environment database, which is the source of all of the international terrorism nominations to the Terrorist Screening Center at the FBI. There is a separate channel for purely domestic terrorists, but the large bulk of those nominations are through the NCTC's process.

And so, one thing that our office did, and that I was heavily involved in, is worked with other agencies and the TSC to negotiate a watch list redress MOU, which is actually a public Memorandum of Understanding that is on the TSC or DOJ's website, and which identifies and details precisely how someone can make a complaint and trigger a review process that may, in fact, result in them getting off the watch list, if they are, in fact, on the watch list.

And it's a process that essentially says, if you've encountered a problem at a screening agency, whether it's DHS or another agency, you use the complaint mechanisms

that they have set up, and DHS has set up the, kind of, the most important of those, the trip process.

And as that complaint goes through that agency, if you believe that the reason that you were stopped, or the reason you were searched is because you were on a terrorist watch list, and you think you shouldn't be on one, or because you think you were misidentified for someone who's on the terrorist watch list.

The screening agency, first, has to determine whether or not you actually were on, or they think that you might be on the watch list, and whether it's an obvious mis-ID problem. And the person -- if they can't identify whether you're on or off the watch list, they would then go back to TSC, and TSC would often reach back to the NCTC, to review that watch list entry, and see whether they can disambiguate the entry, to see that this person is, in fact, is not on the watch list, or in fact, the person may be on the watch list.

And then you would review the underlying information, the intelligence information which remains, usually, classified at a fairly high level within NCTC and review that information, and perhaps even go further into the nominating agency, and try to identify whether they continue to believe that this person deserves, or should be on the watch list, based on the strength of that information.

So that MOU, we participated in helping to negotiate, and it does include some of the things that were described here, and includes, essentially, a requirement that all of these reviews take place, and that the people essentially go back and look at that information, and see whether there's any other information that may either confirm and strengthen that watch list entry, or may tend to indicate that the entry was incorrect, or is not correct now.

In addition to the watch list redress process, our office has worked with personnel at NCTC on reviewing their quality assurance efforts, so they have an effort to proactively go through that –

CHAIRMAN BEALES: If I could just interrupt for a second.

MS. FRANKLIN, thank you very much, we appreciate you being with us, despite the constraints of your schedule, and I'm sorry we didn't give you enough time.

MS. FRANKLIN: Thank you, sorry.

MR. GERSTEN: So -- so that's definitely a big part of the effort of our -- has been a big part of the effort of our office.

And I'm actually going to be traveling to California for a -- next week -- for a roundtable discussion with Arab and Muslim leaders that has, facilitated by DHS, to let them know about that process, and what we have done to formalize it and put in place an MOU that outlines each of those steps.

CHAIRMAN BEALES: Do you have any sense of what the numbers are, of how many people are actually on the watch list who complain, and how many of those, then, get removed as a result of the review?

MR. EDGAR: I would not want to guess those, I mean, I do -- I've seen those numbers, but I would want to go back and check to make sure that I have the right numbers before describing them.

I think that the answer is that there -- without getting into actual numbers, which I'm afraid if I say it will be wrong -- there's a significant number of complaints –not a overwhelming number of complaints – that do get through to TSC and NCTC, and I think part of the reason for that is that the large volume of complaints of travelers either don't involve the watch list at all, because, of course a traveler going through a screening process could have any number of reasons why they would complain about it, and those that apparently involve the watch list can often be quickly screened out by the screening agency as being obvious misidentifications.

And you just, you know, when -- many of the airlines use reservation systems and other systems that are relatively antiquated, and that may not provide enough information to easily match, or not match, a particular watch list entry.

And so, once you've gone through the complaint process, it may be relatively easy to say, "Okay, this person is obviously not the person on the watch list."

What we see are generally those where the person actually is on the watch list, or where it's such a -- it's a very unclear situation in which it looks like the person has exactly the same name, or other information that makes it a more unusual situation than the typical mis-ID situation.

But, yes, we do -- I mean, I'd say that we do get a number of complaints on a regular basis, and people are, in fact, removed from the watch list on a regular basis, as a result of complaints, and as a result of quality assurance and in the ordinary course of the way the watch list is supposed to operate.

So, somebody may be nominated, and if the investigation shows that there doesn't appear to be any terrorism nexus, or that the original suspicion is discounted, then they are, in fact, removed from the watch list, and that's just part of the ordinary operation of that whole system.

MR. GERSTEN: I might be able to add at least one statistic that might be useful. In the recent rollout of Checkpoint Evolution, I believe, the Department provided to the media a statistic or an example of how Checkpoint Evolution is supposed to improve this process. And they mentioned in their information to the press that one airline, in particular, on a typical day would have several thousand individuals who were, in some way, inconvenienced because of a misidentification, or a mismatch, or an improper

capture of the information necessary to determine that that individual was the person on the terrorist screening watch list. Out of those several thousand, only two ended up being actual hits. So, that just gives you a general sense of the magnitude of the misidentification problem that we're trying to provide some improvement for.

MR. EDGAR: And so, I'd say that we're dealing with a subset of that misidentification problem, where the, you know, the DHS and airline situation is something that I think is -- it is a very significant problem, that they are addressing through trying to update and improve their systems.

Our -- our responsibility is to ensure that we have enough information, or that we provide as much information as we possibly can -- intelligence information – that would then allow people to easily disambiguate.

And then, I do think that it's not well known that we do actually have a process where somebody who is not a mis-ID, but is, in fact, on the watch list, and was nominated by somebody who thought they were a known or suspected terrorist, that that does also get reviewed. And that people are removed when that information appears to be either incorrect, or not supporting the watch list status of that person.

So, for example, someone might have been put on a No-Fly List, and then downgraded to a selectee, or something like that.

CHAIRMAN BEALES: Maybe we could follow up with you and get the numbers about that, because I think that would be useful.

John Sabo?

MR. SABO: Thank you very much.

A quick question for both of you, in that the President signed an Executive Order May 7th, establishing this new controlled classified information mandate for the government, to replace all of the overlapping, sensitive, but unclassified data-sharing, and in the categorization, and the controls associated with them.

And the Executive Order talks about implementing it consistent with protecting the information privacy rights, and other legal rights of Americans, et cetera. I'm wondering if either of you or both of you are involved in developing implementation guidance that would capture that requirement of the Executive Order, that is, as you put into place your procedures, that, you know, civil rights and legal rights of Americans are protected. Are you -- is either office doing that? Are you involved, like there's an Information Sharing Council that's been established -- are you involved with that?

MR. GERSTEN: In DHS, we are involved in the Information Sharing Coordinating Council and Governance Board, established to vet these issues and the issue of sensitive, but unclassified, secure, sensitive security information -- all of the various categories.

Those issues did come up last year, and we did review the policies, and we were pleased with the outcome. We do think that as the policy gets implemented, that our office will need to provide rigorous oversight to ensure that these categories are not being used improperly. So, that will -- the question will be what systems are put in place going forward to ensure that our office can have a vantage point to review and provide some oversight.

MR. EDGAR: I'd agree with that, and I'd echo that -- we have been involved, also, in this effort, because this effort around controlled, unclassified information is part of the PMISE, the Program Management Information Sharing Environment, which again is an element of ODNI. So, we have visibility into that.

And I would say that, in general, this should be -- if implemented properly -- a system that would improve the government's ability to protect information privacy and other legal rights, because it's replacing an ad hoc process of essentially different agencies being able to claim that certain types of information are sensitive but unclassified, controlled or FOUO is sometimes a term used, For Official Use Only. And those categories have never really been neatly outlined in the way that they were under the CUI order.

And as a result, I expect that there should be a significant improvement in government transparency, as agencies have to, essentially, justify their claiming of these exemption categories, as well as protection of privacy, for the information that needs to be protected.

I think that the Program Manager -- I helped facilitate some meetings with privacy and civil liberties organizations, and also open government organizations on this effort, a couple of meetings that we had with them. And they were quite supportive of the effort, generally, because I think there was an understanding that the classification system, you know, is a system for national security information and has certain requirements, and guides, and, you know, may itself, you know, need some reform.

But that this other system of controlled unclassified information, that there was lots of sensitive information the government had that was not classified -- maybe sensitive for privacy reasons, maybe sensitive for law enforcement sensitivities, or homeland security sensitivities or other reasons, that clearly needed to be protected, but that was not being protected in a systematic way, it was being protected on an agency-by-agency basis.

And I think that this system should -- if implemented properly -- be consistent with privacy and civil liberties, but obviously as you pointed out, we do need to review and make sure that that's happening, and we also need to make sure that that's happening, and we also need to make sure that if there are any conflicts between the government's

need to protect sensitive information, and privacy or other legal rights, that we step in to look at how those conflicts might be resolved.

CHAIRMAN BEALES: Joe Alhadeff?

MR. ALHADEFF: Thank you.

I guess this is a question for both, but perhaps more for Mr. Edgar.

The concept that you suggested of a slightly more ad hoc process, partially because of the non-mandated nature of systems that don't require a PIA analysis was something I wanted to just explore a little further, because while I understand the rationale and it may actually even be a more customized experience, because of the way that you guys are using interviews and other methods to actually review these systems, I'm trying to figure out how you develop auditability in that system. Because it seems like it's also a very subjective process, and so you don't have a template that's comparable across procedures.

And I think that's an important issue, in terms of also looking at the, you know, any kind of documentation, whether it's a new civil liberties form that's going to be used, or even an existing PIA. And that really is the question of how do you systematize a process so that you know that it's reliable and you have hallmarks across which it's auditable, so that you know it's been correctly?

And I think that becomes important as we look at new technological environments, where more and more technologies are assembled in a dynamic fashion, in order to meet a service need that comes up, so that you don't necessarily know what components are being organized into a solution, and it may be dynamically organized.

And while that may not be the mainstream case today, in 10 years that may very well be the way the solutions are organized, so that you may not be able to have a quick template system and flexibility in the system is important, but how you systemize that flexibility is also tremendously important.

MR. EDGAR: I guess I would agree with that, part of the reason for our ad hoc approach has been making a virtue out of necessity. You know, our office has four people, and so looking at all of the programs in the intelligence community is something of a challenge for us to pursue anything than an ad hoc basis, where we essentially triage and look at the programs that are most important.

As I said, we are in fact, getting additional folks, there is some controversy in Congress, people who think the ODNI is way too big and bureaucratic, we don't feel that that's a problem for our office, and I can tell you that a lot of people in other offices of ODNI feel the same way. I do think that there's a bit of schizophrenia in setting up an office designed to integrate and unify an entire intelligence enterprise, and then complaining when they want to hire staff to do that.

And, you know, it might be nice to say that everybody should go out and just do their jobs, you know, every police officer, you know, if you think about a major police department, gee, let's have all police officers, and no managers. I mean that -- that wouldn't work.

So, I think that that -- that's one answer, I think that you're making excellent points about the need for auditability across systems, I don't want to leave the misimpression that the programs that we've review do not necessarily have audits -- it really just depends on the program. In some cases, they're audited quite regularly, and quite rigorously. The example that I would -- that comes to mind is the -- the National Security Agency's programs, all of them, not just the one that is really of most interest in Congress, have very rigorous audit and oversight compliance rules, and has a directorate of oversight compliance that is really one on which we're relying in terms of looking at what -- you know, what violations or concerns or issues or problems that might be identified are.

So, it depends on the nature of the program. In some cases there's very heavy audit, in some cases there may not be audit, or there may be a less heavy audit, but I take your point, I think that having a more formal template and structure, that we would then employ would be something that would be of value to our office.

We would, of course, need the resources to do that, and I think that -- that it would be useful to have some flexibility. And part of the reason for flexibility would be the need to maintain our ability to provide advice on a more informal basis, that may take place very early on in the course of a program.

One thing that we've found, I think, which is a kind of a victim of being our own success, especially in science and technology area, people will come to us, and they have an idea of what they'd like to do, they think there may be some privacy or civil liberties issues, they want to get our advice and they may not have -- this may not be a program that exists, yet. It may not be a program that exists at anything other than an idea form.

You know, one thing that we would want to work into that is an ability for us to say, "Okay, here's some of the issues that you need to be paying attention to, and here's the appropriate time for us to do something more formal." You know, if that program's cut later in the budget, if they decide not to pursue it for other reasons, it may not be one that we told them they can't pursue, it may be one that they've decided for other reasons, not to pursue, you know, would be a misuse of our resources to have gone through a large, formal process for something like that.

But I think those are issues that we could address in the framework of having a tool available to us that would look at these issues on a more formal basis, as you suggest, which I think, we're, you know, we definitely agree with.

MR. GERSTEN: I just wanted to make one clarification. The auditability I was talking about was not the programs that you guys are overseeing, but as you develop more staffing, how you audit your own process.

MR. EDGAR: That's a very good point. Very good point, I think that's an excellent point, and it's one where, you know, we could probably, you know, do some work to improve how we would do that, and this is part of what we would do in setting up these kinds of tools.

MR. GERSTEN: I'm glad you made that clarification, because I was about to respond to the question of audit trails and information sharing, I thought maybe you were referring back to your question to Dan Sutherland earlier. And, of course, audit trails are important, however, in some of the information-sharing programs that we see, the programs that need audit trails the most, are the ones that are most difficult to create those trails for. Programs that share information with State and locals, for instance.

I really think, though, that part of your question gets to a style of leadership in providing and improving civil rights and civil liberties in the types of security and intelligence and law enforcement programs that we are supposed to be involved with. We could have the strict enforcement approach, where we receive cases and complaints from the public, and attempt to enforce the statutes with a heavy hammer, working very closely with the Inspector General Office. We could have an approach to civil rights and civil liberties leadership that provides – give us opportunities to provide advice and review and consent and so forth with program managers and leadership in the Department.

Or we can take the approach that I think our office, through the leadership of Dan Sutherland, has promoted, and that is to promote a culture of civil rights and civil liberties throughout the Department and throughout the partnerships that the Department has with other agencies -- through training and collaboration on various projects.

But again, I think, getting back to your clarified question of audit trails within our own office, we fully intend to have a process for ensuring that the impact assessments themselves do not become unwieldy and lead to, I guess you would call, wide-ranging conclusions that could be misinterpreted. We fully intend to avert the kind of mission creep that can occur when civil rights and civil liberties offices have traditionally provided advice that could be misinterpreted.

So, there will be an audit trail, and there will, of course, also be an audit trail describing who, within a program office we met with, what the advice was that we gave to them. However, I don't -- I don't think it would be healthy for us to provide that kind of information at the end of the process, it might, in a sense, shut down the conversation

in the future, we want to be able to work with these offices, not have them feel that we are, somehow trying to stop them from doing their job.

Yeah, I'd like to chime in with just two -- two additional observations. One is that we are actually under a reporting obligation as a result of the 9/11 Commission reform -- additional implementation act, or whatever it's called -- from last year. So, we do have that sense of accountability of having to describe what we're doing in a report on a quarterly basis, to a whole host of Congressional committees, not just intelligence committees, and of course some of that may be in a classified annex for us.

The other thing that comes to mind is a story about David's concern -- it is a real concern for us, we had a particular project that we were pursuing that was intended to assist the community in formulating rules of the road and good practices with respect to a -- our efforts at open source information. And essentially, there was some misunderstanding that we were engaged in some kind of investigation or audit, and that has caused us no end of problems.

And so, it is a real problem when your office's efforts to, essentially, create good government solutions that will empower and help the program do its function in a way that will withstand any kind of scrutiny that might be applied to it, is misconstrued. And people tend to not want to share information, they tend to not want to meet with you. Of course, you can always try to use the hammer of your authority or the DNI, or whatever you want to do, but it's just not a -- it's a real problem, I guess is the way I'd put it.

Is that -- that it's not simply that we're, sort of, you know, overly concerned about ruffling feathers, it's that, you know, we'll ruffle feathers fine when we think it's necessary. But, if there's a misunderstanding about the nature of what we're doing, it can really impede the effectiveness of our work. And delay, you know, what could be a project that would actually provide very useful guidance to the community.

So, it's something that I think both of our offices have experienced from time to time, and so it’s very important that a Privacy and Civil Liberties Officer at any department or agency, maintain a level of trust, not only within that organization, you know, but with the Director and with others, so that we are someone who is sought as an advice, and I think -- sought advice for.

I think the Inspector General already serves an important function of having that ability to come in, in a way, with that hammer. And that -- that is a very different role, it's a different job, it has different statutory rights, and obligations and responsibilities and powers, you know, different reporting responsibilities -- and it's a very effective tool.

And it would not be effective for our offices to attempt to, essentially, do their job without their authorities and powers, because we couldn't do their job as well, and they're already doing their job, and there's a job that we need to do. And it's a job about

compliance, and about getting together good practices, and making the organization, hopefully, look good next time the Inspector General comes calling, next time the Congressional oversight committees come calling, they can look and say, "Hey, you did what you're supposed to do."

And I think your point is you need to be able to audit that process, you need to be able to show that document, that process. So, not only did they avoid the problems, but they can actually show they went through a process that helped them do that. And I think that's a very good set of observations for us.

CHAIRMAN BEALES: Lance Hoffman?

MR. HOFFMAN: This is for MR. GERSTEN.

I looked over the set of questions you provided us, and they look pretty good. I had a -- I was a -- I had a question on a couple of them, though, I didn't quite understand, and maybe you can you help me out here, how they really relate to civil rights and civil liberties. And they were two related to the influence of government -- all of the other questions make perfect sense to me. But a couple at the bottom of page 1 say, "Would the program increase the authority, control, or influence of the Federal government in its relationship with State or local governments?" and the other one is same question, but with regards to the private sector.

Now, I understand civil liberties and civil rights, I think, when it comes as applied to individuals. But why are these questions -- what are these intended to get at?

MR. GERSTEN: Well, I think what they're getting at is that when authority is disbursed between various levels of government, it's less likely that a single agency can accumulate unhealthy power over individual lives. There is a healthy balance between Federal and State governments, the constitution creates this delicate balance, and it also helps to prevent the accumulation of excess power in the States, or our national government.

All other sovereign powers, save those prohibited by the constitution, have powers reserved to the people. And I think that what we're getting at here is that if a program, for instance, began to usurp the role of a State, that program would impact civil rights and civil liberties.

It may, in some ways, it may be to the benefit of certain rights -- if a State is not doing enough to ensure the rights of its citizens, and a State program essentially comes in and does more, then perhaps that would be a good thing. However, it should be something that we examine, and so it should be something that we assess in our review of the program, that's why that question is there.

MR. HOFFMAN: Okay, my only -- my only concern would be, I was wondering, if I were trying to stand up such a program, if I were the program proposer, if you will, and maybe it's just because I'm not an attorney, but I've seen plenty of programs proposed by people who are not attorneys. I do understand, I think, this balancing act between the various levels of government and the private sector. I would be hard-pressed to say, Oh, he's asking me for a dissertation on the proper roles of the various levels of government, I was just wondering about the wording a little bit.

MR. GERSTEN: Well, I'm glad you asked this follow up, because I think that I need to clear up one misconception, and that is that, unlike a Privacy Impact Assessment, where the Privacy Officer may submit the questions and expect the Program Officer to respond and fill out the questions, we do not provide the questions with the expectation that the Program Manager has the expertise in all of these areas -- I think that would be expecting too much.

It's not expecting too much for the Program Officer to understand his system enough to tell whether or not personally identifiable information is impacted. However, for a Program Manager to understand, as you noted, the balance of powers, State rights versus Federal rights, as well as other questions that we've laid out, we'd be asking too much.

I should also note that we intend to work with the General Counsel Office in conducting our Impact Assessments, both the counsel to the component that -- where the program originates from, and then also our headquarters General Counsel.

And as Tim noted earlier, we are attempting to not just address the legal issues -- we're looking at the policy implications. Because, of course, there are many times when something is perfectly legal, but it just does not make good policy sense. Or there are many times when something could be worded in such a way to give authority, to grant authority to an agency or a program to do something that, from easy inspection, would violate civil rights and civil liberties.

CHAIRMAN BEALES: Gentlemen, I want to thank you both for being with us today, we really appreciate your time and the information. This has been most helpful.

Our agenda says that we're now going to turn to subcommittee reports, but I think we actually ought to turn to lunch, and put subcommittee reports at the end of the day. And continue from there.

If you would please be back -- although we are ending late, we will start on time, promptly, at 1:00, so please be back at 1:00. If you are interested in signing up for public comments, please do so at the table just outside the room, and we look forward to hearing from anybody who wants to make a comment.

Thank you, and we'll see you again at 1:00 p.m., promptly.