DEPARTMENT OF HOMELAND SECURITY

DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE

FULL COMMITTEE MEETING

WEDNESDAY, SEPTEMBER 19, 2007

Hilton Arlington

Gallery I and II

950 North Stafford Street

Arlington, VA 22203

MORNING SESSION

MR. HUNT: Good morning, everyone.

Again, my name is Ken Hunt, and I am the designated Federal officer for the Data Integrity -- Data Privacy and Integrity Advisory Committee. Under the Federal Advisory Committee Act, my presence is required for these meetings.

And so, without further ado, I will pass the meeting to Howard Beales, our committee chairman.

MR. BEALES: Thank you, Ken. And welcome, everybody, to the -- to the September meeting of the Advisory Committee.

The -- a couple of housekeeping matters at the beginning. The contest for the coolest cell phone ringtone is at lunch, so please turn off your cell phones so that you don't give away your secret.

And, in the back of the room is Lane Raffray, and, if you're interested in signing up for a public comment at the end of the day, you need to see Lane and put your name on the list. We would love to hear from anybody who would like to talk to us.

First item on our agenda is a privacy office update. Unfortunately, Hugo Teufel, who's the chief privacy officer at Department of Homeland Security, had a family emergency this morning and isn't here. So, in his stead is John Kropf, the deputy chief privacy officer.

John, welcome, and we look forward to hearing -- to hearing what's happening in the Privacy Office.

MR. KROPF: Thank you very much, Mr. Chairman and distinguished committee members.

And I want to say that one of the duties of a deputy is, of course, to step in when the chief privacy officer can't attend a function. So, I'm here today, and I will try to do my best to give you an update on what we've been up to since our last committee meeting.

I would summarize it simply by saying that we have been -- we've been very, very busy, and I think all of our directors have been firing on all cylinders, working as fast as they can. And I think what I'll do is, I'll just, kind of, go down our list of directors, and take it section by section, and we'll give you an update as to everything that's happened since -- I think it was early June when we last met.

I'd like to start, really, with congressional activity. The CPO, Mr. Teufel, has been up to the Hill now twice; once in July, where he was reporting and responding to the GAO recommendations for improvements to the Privacy Office. And if you -- if you recall, there was a GAO report that came out earlier this year with four recommendations, and they were essentially to develop privacy officers within each of the DHS components. And this is -- this is something that we are slowly, but steadily, working on developing. There are, now, vacancy announcements out for some of the major components. Some of the components already have them, such as US-VISIT and TSA.

The other recommendation was that we make sure we do more timely reporting. And we should be on track, for later this year, to have our next annual report in on time. And the GAO also urged us to do biannual review of our systems of records notices. So, these are all things that Mr. Teufel was able to address in his testimony, all 5 minutes of it, before Congressman Conyers.

And I will -- I would take some pleasure in noting that Linda Koontz, of the GAO, who was also up there to testify, described the DHS privacy officer as a leader among the Federal Government privacy offices, and also, in her written report, acknowledged this committee as making significant contributions in the Federal privacy world. So, I think

that's something to pause and really take note of. And -- just urge you to continue our good work together.

The second appearance that Mr. Teufel had was September 6th, before the Homeland Security Committee, on something called the National Applications Office. And this is a -- this is something that is being developed and put together; it's still in the developing phase. But you may have -- you may have read about this in the paper; it is essentially to take a function from what has been in one part of the Federal Government, and to move it over into the Department of Homeland Security to use national assets – that is, overhead satellites for homeland security purposes. And this is something that -- Mr. Teufel was called to testify upon the privacy work that we have done in developing this office to make sure that Privacy was involved. We have been involved. We have done a privacy impact assessment for the NAO. And this is something that was really over and above what is called for by law, since, by law; security systems are exempt from PIAs. Nonetheless, we've worked with the NAO to put them through the PIA process. So, that's essentially been our congressional -- our Hill testimony activity.

As far as guidance to the -- to the larger Department, we've done several memos that have gone out to the entire DHS, and one of them is a policy memo on reducing the use of Social Security numbers. That was issued in early June. That's up on our Web site. We've also done -- we've issued a number of reports. We've issued a report on data mining. That came out in July. We issued our ADVISE report in July. And our annual report, as I mentioned, is imminent; that should be coming out any day now. As far as guidance goes, we continue to be very active in trying to be a leader for the Department and for the Federal Government on doing guidance. We have a Privacy Technology Implementation Guide that's just gone out, department wide. We have updated our PIA guidance. I would call it, I guess, PIA 2.0, new and improved. We've done a PIA workshop with a DHS Security Conference that was up in Baltimore. And then we have something we call the Pig [PIHG], the Privacy Incident Handling Guidance, which is also about -- is imminent in its final issuance as -- if Hugo were here, what he would like to say is that, "This PIHG will soon fly." But it is -- it's -- again, it's sort of to provide guidance to all the components on how to respond to a privacy breach or a privacy incident.

On the international side, we've also been extremely busy. We're very pleased, actually, to have with us, at this committee, evidence of that. We have -- we are on the second week of an exchange with two of our Canadian colleagues who came down from Commissioner Stoddart's office in Canada to sit in with us. And they're both here in the audience today. And, perhaps at a break, you might take the time to chat with them. They, hopefully, have been able to learn something from us. And we know that we've learned a great deal from them. And this is really the first in what we hope will be a

series of exchanges. We hope to send one or two of our folks up to Commissioner Stoddart's office to reciprocate, and then perhaps -- we have in mind some other data-protection authorities; the U.K. might be the next one in mind. But -- so, we've been -- we've been very active trying to get these exchanges off the ground.

We also, next week, will be -- will be attending the Montreal International Data Protection Commissioners event, which is, sort of, the big event for international privacy authorities, globally. Our own director of compliance, Rebecca Richards, will be giving a presentation on PIAs. There's been a lot of interest overseas, particularly from the U.K., in how the U.S. does PIAs. And I should also note that Secretary Chertoff will be one of the keynote speakers at that event, and we consider that to be quite a significant commitment, because of his -- the level of interest that he has shown in privacy has been fantastic, and this is just a -- the -- sort of a symbol of his continued interest in privacy.

The last month, we were also doing some outreach in -- we were in Germany and in the Netherlands to talk about the U.S. privacy framework. There's -- this is sort of a continued activity of ours, where we really try to correct some misperceptions about U.S. privacy with our European friends. And this is coming on the heels of the PNR Agreement, and -- this is the Passenger Name Record Agreement which was signed by the Department and our EU counterparts at the end of June, which gave more permanence to the exchange of Passenger Name Record information from European-originating flights to the United States to share with us the passenger-name info.

One of the most significant things that I should stop and note on that agreement is -- and this is -- this was something that this office pushed for in its advisory capacity -- to have an administrative commitment to redress for non-U.S. persons under this arrangement. As you -- as you know, the Privacy Act only provides for redress for -- that is, U.S. citizens and lawful permanent residents. And one of the major criticisms that we had run into in the past was that EU citizens did not have any meaningful way to seek redress for incorrect information, or to amend their information. So, this was an administrative commitment from the highest level of the Department to provide an avenue of redress, and we consider that a very significant step on the international front.

On the compliance side, we have -- we have really been putting out quite a bit of work, and work on very large, significant, high-profile systems. I would mention -- just to tick 'em off, I'm not going to go into great detail -- but the Advanced Travel System -- that's ATS; also the APIS system; the Secure Flight System; VIS, which is the Verification System for Employment. These are major, major systems that will be handling the very high volume of records. And so, they're very notable. I think we're up, now, to -- and all of these systems, by the way, they come with systems of records notices and privacy impact assessments -- and we're up to about 101 PIAs, give or take, and I'm not sure, off

the top of my head, about SORNs, but Becky will let me know -- about 58 SORNs. So, we've been really -- we've been really pushing these out.

On the REAL ID front, we have appreciated your comments. We are -- we're very, very close to issuing a final -- a final rule. I was just looking at it yesterday. And that effort is being spearheaded by Toby Levin.

And then, I think -- I think the last thing to mention, which is quite significant, is, on August 3rd the President signed into law a -- the 9/11 recommendations bill. It has a much longer proper title than that, but that's what I'll refer to it, in shorthand. But this bill had a -- has many, many new requirements for the Department, and there are some significant requirements, especially for the Privacy Office. And we're still looking over everything that will be required of us, and we're consulting, of course, with all of our folks in-house, but, just generally, to tick off some of the new authorities and some of the new activities that we have a mandate for is -- we do have a mandate for -- to be able to conduct investigations. We're -- been given limited subpoena authority. We've -- we also have a new relationship, a much closer relationship, with the Office of the Inspector General. And there will be a new entity. It will be an independent agency-like entity that is taking the PCLOB idea, but giving them agency status. I'm not -- again, we're not quite exactly sure what this will look like in the end, but this entity is something that we will have a close reporting and coordinating role with. And we'll have -- there'll be bypass authority for our -- a lot of our reports, particularly our annual report, which is -- which is a report, then, that will have to go -- really, that will go directly to Congress and to this new -- to this new independent board without any -- the law specifically talks about having no changes from anywhere outside of the privacy office to this report, so that's what we mean when we talk about the "bypass authority."

There's also a lot of -- there's a lot of new activity that we'll have on Fusion Centers. And that's coming up on the morning program. I know we have a number of panelists who will be talking about the Fusion Center, so I won't go into that too much here. But, just to lay out some of the highlights, PIAs are now going to be part of the concept of operations, and -- for Fusion Centers—and that will be due in November. There'll be a lot of privacy training that we'll be required to do, especially for the intelligence and analysis personnel stationed in the Fusion Centers. And we'll be doing a lot of guidance and other training for State/local employees on Fusion Centers.

And there's quite a number of other additional training requirements that we'll need to staff up on to handle, including mandatory training for DHS employees on the handling of Personal Identifiable Information. And the -- I would also say that the 9/11 bill has a number of additional PIA -- PIAs that we're required to do, many of which we're already doing or have been done, but they have now been -- these requirements have been specifically codified in the 9/11 bill.

And then, finally, we have a significant number of new reports -- I think, seven or eight, depending on how you count them. One of those will be a quarterly report to Congress, which will include a discussion of the number of privacy complaints that we receive and how we handle those.

So, I think I'm going to -- I'm going to let it end there for my summary, and, at this point, if there's any -- if the commission has any -- the committee has any questions, I'll be happy to take them -- of course, backed up by a very able and well- informed staff, when -- I'm looking over at Becky and Ken when I say that.

So, thank you very much for the opportunity to report.

MR. BEALES: Thank you, John. Joanne?

MS. McNABB: I didn't -- could you tell us a little more about that new entity? I didn't understand what you said it was called, something like "pea clob."

MR. KROPF: Well, it will no longer be called the PCLOB, but it is -- it is taking that concept of having a -- well, PCLOB -- the President's Civil Rights and Civil Liberties Board -- I'm sorry, I -- sometimes I speak in acronyms without even being aware of it, because, I think, it's -- it's probably a symptom of being in the Federal Government too long. But it's -- you're familiar with the President's Civil Rights Board. And it's -- it will no longer be within the White House, but it -- it is now given -- the bill is very precise in a lot of the language about -- it is meant to be an independent, standalone entity. And it's -- it will have, I believe, five board members, one of whom will be permanent, and the others, I think, will be only on a -- paid on a -- sort of, an as- needing basis, and they all have to be confirmed by the Senate. They will –

MS. McNABB: I recognize what –

MR. KROPF: Okay.

MS. McNABB: -- you're talking about now.

MR. KROPF: Okay.

MS. McNABB: I just didn't know the acronym.

MR. KROPF: And I know that the existing PCLOB, by law, will be given 6 months to wind up its affairs. I think it will probably happen a lot sooner than that. I would -- I would imagine, probably -- certainly before Christmas.

MR. BEALES: If I could just wiggle in the Chairman's question, here. I was interested in the report you have to do on privacy complaints. And I was wondering if you could say a little about what kinds of complaints you get, and how many.

MR. KROPF: I'm happy to do that. I know Toby Levin has been leading that effort in the office. We already have a system we're putting in place to -- it's a docketing system

that will track and follow any privacy complaints that we receive, that are -- either directly or referred to us from other components.

The legislation itself talks about privacy complaints -- privacy, with a small p -- which could be significant, because we don't know exactly what that means yet, we're still reviewing it. But is that -- is that the Privacy Act, or is it something broader than the Privacy Act? And it says from individuals, so we don't know, you know, again, who might have standing to file these requests. But we -- the legislation is very specific that we have to state the number of complaints we receive, the type of recommendations and advice that we provide on those complaints, how the complaints might be resolved, and then what action is ultimately taken on them. And this is a quarterly reporting requirement.

Is that -- does that help you -- give you a little more –

MR. BEALES: It does. Do you get complaints now? Is there -- is there a flow of complaints coming in?

MR. KROPF: I would say it's very, very small. I would describe it as smaller than a trickle. I'm going to look for Toby. But I think it's -- I think we have just a handful, at this point in time. I will mention that one of the things that we have set up is -- again, it's not required by this statute -- but we already have in existence something -- a program called TRIP, the Travel Redress Information -- Inquiry Program, which is intended to be a funnel to handle all complaints from travelers who feel that they have their information -- that we have their information incorrectly, or they're getting unnecessarily hassled and want something amended or corrected. So, that already exists and is handling these complaints. And of Toby has anything to add, I'll let her chime in.

MS. LEVIN: We receive a -- Yes, Toby, T-o-b-y, Levin, L-e-v-i-n.

We receive a lot of communications which I would define as communications from individuals. Whether they're complaints or not -- many of them are simply asking for information. As you can imagine, they see us as a resource for lots of questions regarding a lot of the different activities at the Department. So, we have identified, basically, buckets of categories of the -- with regard to the communications that we receive by e-mail or phone or fax. Many of them are informational, many of them have to do with the Patriot Act, over which we really have no say or involvement. A lot of is implementation of requiring Social Security numbers. When you open an account, for example, with a financial institution, people are asking us what -- you know, what can they do about that. So, we do a lot of forwarding of communications to other agencies, where people may be able to get additional information or resolution.

And we do receive more formal complaints from -- sometimes -- from members of the privacy community, and those -- in our next annual report, you'll see a section where those are described.

So, we're formalizing our processes now to do a better job of categorizing the communications that we do receive. And, as John said, he's received very few actual complaints. The majority of them really are requests for information or comments or opinions about issues that members of the community may have with regard to activities at the Department.

MR. BEALES: Thanks. Lance Hoffman?

MR. LANCE HOFFMAN: Thank you. Good morning. You mentioned redress, and I think that's very important, also. A question related to TRIP or other programs we have in place. I went -- this is triggered by something I read last week in the paper. It was either the Post or the New York Times, where there was a story about a woman, some music scholar, who, you know, CBP, I think, wouldn't let her into the country, but it really wasn't related to CBP, it was a -- it was over at the State Department; there was an issue there. And it looked like there was a wall of silence that had been put up. I'm not saying we did it, but I'm saying somehow we got in that chain. And I'm wondering if the Department has any way of bringing to a better resolution this seemingly, oh, I don't know Kafkaesque kind of situation than what we have now. What can we do about situations like that?

MR. KROPF: Thank you for that question. I'm familiar with the New York Times article, and I think you're right, it was ultimately a State Department issue regarding whether she would be issued a visa or not. And the issuance of visas is handled operationally by the State Department, and that is -- I'm only familiar with it from my previous experience, but I know that, under the visa issuance rules, they really don't have to tell you very much about whether you're going to be -- why you might be denied a visa.

However, in the DHS side of things, this is where we can have an effect. And I would just point out, what exists already, of course, is, we have -- we have a very strong-access statute, which is the Freedom of Information Act, which gives any individual, regardless of their citizenship or other status, the ability to access their records, and, if they're not satisfied with the agency's response, they can go all the way up into the courts to pursue that access. And then, of course, you've got the Privacy Act, which has a -- an amendment -- ability for a U.S. person or lawful permanent resident to seek to amend or redress their record.

But where we're really trying to push the envelope, at least for the privacy side of things, is to try to extend that ability to people that are not covered under the Privacy

Act. And we've done it, administratively, through our mixed-use policy, which was the very first policy that the Department pushed out from the Privacy Office. And US-VISIT was already doing this; they were already providing this kind of access and redress. And I know that some of the other components -- I believe CBP had already had a -- had something in place, as well, what they called a -- it was, at one time, called a Customer Satisfaction Unit. I think it's now back to -- they've rebranded it to something else. But the important thing is that the concept is there, and we keep pushing this concept, that if you don't have an opportunity for redress, you're going to lose the trust of the traveling public. And so, without that trust, we're not going to be able to have these systems function properly. So, we do keep trying to push and improve the idea that redress should be an avenue at least administratively open to everyone. If that helps answer your question.

MR. BEALES: I think we have time for one more short question from Tom Boyd.

MR. BOYD: You mentioned that one of your initiatives on the international front was working with our friends in the EU, to eliminate misperceptions about American privacy policies. And I wondered if you could outline some of those misperceptions.

MR. KROPF: Well, first of all, I think one extreme is that the U.S. is the "Wild West", that we have absolutely no privacy protections of any kind. And I think that there was -- there a lot of, perhaps, misperception that was generated, perhaps, during the first PNR talks, when you had law enforcement on one side of the table and privacy folks on the other, and they were talking past each other. And I think the result was, it helped spread a lot of misperceptions about exactly what we did, and that we -- what we need to be trying to explain is that we do have a independent -- we have our own -- we have -- I should – I should back up and say, we have our own privacy oversight. And I think the biggest -- the biggest issue we get into with the Europeans is, they have their model of an independent data-protection commissioner, and they don't see anything like that here. And so, they think, well, we must not have effective oversight. And what we try to do is to explain that we have a network, and a layered approach to oversight, which involves sort of a spectrum of players. It involves -- starting with the privacy office in an agency, you also have an inspector general, you have GAO, and you have Congress, and then you have even the courts. So, there is a much more complex -- it's not as neat a system to describe, but we have to emphasize that we do have a form of networked and layered oversight.

Then you get into very, very specific misperceptions -- with the PNR, for example. The last trip that we just made to Holland, there's a -- there's a perception that the PNR collects religious information, sexual preference information, your political beliefs. All of these things are -- they're absolutely filtered out from the PNR arrangement, but yet, there

is this rumor out there, flying around in the press every day, that we're collecting it. And we're not. And --

MR. BOYD: Well, let me just interrupt you there. With respect to concerns about the layered effect versus the European approach, I take it, then, that there is considerable discussion about the very different enforcement cultures that exist, the presence of private rights of action in this country, their absence in Europe, et cetera.

MR. KROPF: I'm not completely sure I understand the question, other than we -- I mean --

MR. BOYD: Well, there's a very different enforcement culture here, at multiple levels, than exists in the EU. It's one thing to have a regulatory framework that's rigid; it's another to enforce it effectively. And I think there's a lot of difference in how both systems are enforced.

MR. KROPF: Certainly -- I mean, certainly, we see that in -- we read about that in the private sector, and I remember reading a -- I think it was a Ponemon Study, where it talked about the -- there is more enforcement on the private side for privacy in the U.S. than Europe. But, I mean, in the government-to- government sharing, we still have to assure our European counterparts that their citizens will have every right to seek access and redress to their records. And that's the thing we keep stressing; that and transparency, that we publish everything for the world to see, Our SORNs and our PIAs are out there, and here's where you can go look at them.

MR. BEALES: Thank you very much, John. We appreciate your being with us today, and we appreciate your report.

Our first panel of the morning is to discuss Fusion Centers, and then we'll have another Fusion Center panel this afternoon.

Our first speaker will be Robert Riegle, who's the deputy director in the State and Local Program Office in the Office of Intelligence and Analysis in DHS. He -- as a senior intelligence officer, he spearheaded the development of relationships with many State and local government Fusion Centers, and he was co-lead in the effort to formalize policy concerning Fusion Center relationships. He's been an active participant in the Homeland Security Advisory Committee -- or Advisory Council -- and was the vetting authority for the most current version of the Global Justice Fusion Center Guidelines. Prior to DHS, he worked at Booz Allen Hamilton, in strategic communications at the Defense Intelligence Agency, and at Chevy Chase Bank.

Welcome, Mr. Riegle. And if I could ask you to limit your remarks to 10 to 15 minutes, and then we will have questions at the end. And I will introduce the other speakers, in turn.

MR. RIEGLE: Thank you. I appreciate the opportunity to present our position, in the Department of Homeland Security, on Fusion Centers. We feel it is a very important effort to the Nation's security, and we think it's also a novel and different approach to some of the historic methods for which we shared information -- specifically, threat information -- with our State and local partners.

I think the thing to begin with is to understand that, before and above anything else, these are not Federal activities. We contribute to some of the expertise within the centers. We help support them, financially. But, in the end, the centers themselves are State and locally run and derived. We find that to be important, because one of the things that has occurred in the past, and it was mentioned in the 9/11 Commission Report, is that there was a -- there was a problem with unity of effort, as far as trying to get information in a meaningful fashion to our State and local partners. It's documented that nine of the conspirators in 9/11 had some contact with State and local law enforcement during their time in the country, and that, in a couple of cases, the conspirators had been on watch lists and were -- would have been easily identified, had that information been made available to our State and local partners; specifically, at the granular level, those cops on the street and highway patrolmen that seem to have the most contact with the public at large in law enforcement and threat mitigation efforts.

We took the approach, early on in the Department of Homeland Security, that we were going to try and rely on the expertise that existed in different areas of the country, rather than trying to reinvent the wheel. And, clearly Fusion Centers were an initiative that was underway -- in many cases, prior to 9/11 -- and the States themselves had identified the need, that they needed one central facilitation point for the information exchange as it related to threats or hazards within that State; in other words, putting their information-sharing eggs in one basket so that all of the people that had equities within that threat mitigation strategy were aware of what the threats and risks really were.

And so, the Fusion Centers really spawned from the States' initiative, not an initiative by the Department. And when we began to look at some of the more troublesome aspects of our information-sharing relationship with the States, we began to recognize that these Fusion Centers could provide a valuable entry point, not only for the Department, but for the Federal Government at large. And my colleague, Ms. Sue Reingold, will speak to that particular Federal effort. But, from the Department's perspective, we understood that this would be a logical entry point. First of all, it was a comfort level with the States. It was their exchange point, not the Federal Government's exchange point. And we have found, in our relationships with the States, that the grassroots approach typically works best, where they're in their comfort zone.

Now, it created some challenges for us. Not all of the threats that States face are uniform. The threat to Massachusetts is not the same as in Arizona. Theirs is more of a

maritime consideration, versus a landlocked State like Arizona. So, what ends up happening is, if you take the approach that you're going to work in a grassroots sort of manner with the States, what you come to a conclusion of really quickly is that there's no cookie-cutter approach to these Fusion Centers that's going to work uniformly. You might find, in some areas, such as privacy, civil liberties, civil rights, baseline training of analysts, security, et cetera, where you can apply some uniformness to it, but, in general, one thing that you have to understand is, they're not going to be constructed in the same way. Their governance and own internal oversight isn't going to be the same, so it creates some challenges as you begin to move forward and work with these 50 different entities.

Now, having said that, I will tell you that we are very impressed by the States' willingness to accept some recommendations and general baseline capabilities requirements from the Federal Government; and, to that extent, we have been able to, as we've moved forward in the relationships, be able to apply some more uniform standards to how they construct themselves as they relate to the information that they receive from the Federal Government.

One thing we have to be sensitive to, though, is, that is information flowing from the Federal Government to them, where we do have some legal and statutory authorities, constitutional authorities, et cetera, that help us in the control of our information and how that might be handled. The laws in the States, however, are not all the same. Some sunshine laws vary from State to State. Some States don't have it. Some States have laws that actually limit what information can be shared with the Federal Government. So, it makes it a little bit of a challenge for us to try and determine what's the best approach in any given State; however, we know, as a baseline, there's certain things that need to be protected, and we try to approach it from the -- from the proactive stance of saying, Here's some recommendations or best practices that we think will work uniformly. And, to our satisfaction, and to our thankfulness, the States have agreed to adopt these. There has not been a State yet, that has a Fusion Center, that has not agreed to the baseline levels of protections in certain areas dealing with Fusion Centers and dealing with the handling of information, primarily U.S. persons information. So, we've been very fortunate to be able to bring the States into sort of an environment that we, at the Federal Government, have to work under every day.

And I try to emphasize, in these sorts of forums, that we do not see, nor have we in the past seen, any level of concern -- we haven't seen a plethora, for instance, of concerns by private individuals, where they've reported back to us that they have strong concerns. As a matter of fact, to date, in our program, which has been in existence for 15 months now, we have yet to receive a privacy violation from one of the States or from a concerned individual out in the State and local terrain that we've had to address at the Federal level.

So, if you were to ask me today, am I aware of any violations, my answer to you would be no, we do not know that there are any citizens that have made any formal complaints to Fusion Centers concerning their private information.

One of the things that I would like to focus on now is -- giving you sort of a baseline understanding of where we're at programmatically -- is some of the things that the Federal Government is currently working on that have an effect on the program as we move forward, one of which was released a couple of weeks ago, and that's the -- and signed into law -- that's the 9/11 Commission Act, Public Law 110-53. There's a focus in that law on ensuring that the Federal Government maintains some oversight in the area of civil liberties, civil rights, and privacy. As an example, in Fusion Centers, and it's been codified into law. That serves two purposes, one which is to make sure that we, as a program -- and also, Sue Reingold is a national Federal manager of this effort -- understand the importance of these things to Congress. And it also validates the fact that Congress really understands the need and supports these Fusion Centers. But with that comes a host of reporting requirements that previously weren't codified into law that now, sort of, act -- or, in effect, act as a -- as an insurance policy. Civil liberties, civil rights, and privacy were foremost among those recommendations, that training be conducted to that extent. We have committed over $400,000 to the -- to the -- to the Privacy and Civil Liberties Offices within the Department of Homeland Security to work with other Federal partners to establish and ensure that a baseline level of understanding and training in those areas is put in effect.

This is also true in other areas, such as the training of analysts, the baseline capabilities, understanding of what we would look at it as to what qualifies an analyst. Some other areas are operational security; of course, the protection of sensitive United States national security information.

So, all of these things were codified under this public law, and we think that's a good thing. We had, prior to the public law being released, reached out to the Civil Liberties and Civil Rights Office and the Privacy Office to really begin to implement a good training program earlier than required by Congress, but this certainly helps us, and it certainly helps us in the -- in the visibility aspect, that now we can show our State and local partners, in public law, why we need to do these things. And they've been -- they've been, so far, vary accommodating to that.

Of course, with that comes increased congressional scrutiny. I think we've seen, in the newspapers recently, a lot of concern about the National Applications Office and a -- certainly my program -- a State and Local Fusion Center Program Office has been increased scrutiny. We welcome that. We think that's a good thing. That is not something that we find onerous, it's something that we, as citizens, are in favor of. We have to live in

the neighborhoods and communities for which we try to protect, from a threat perspective.

Been some very strong successes in Fusion Centers. I'm going to leave some of those, to outline, to my State colleague here, Mr. Wobbleton. But the Fusion Centers in the national network of Fusion Centers are a very good thing. It does bridge that gap, where that law enforcement officer who makes a stop in a State can get a better handle on whether or not, at the national level, there is a concern about a particular individual or a particular incident. It is a gap that needed to be filled, and it is being filled effectively, and, to the best of our knowledge, it's being filled in compliance with all laws, not only at the national level, but the individual laws that have been developed at the State and local level.

So, I welcome your comments. I look forward to the opportunity to talk more about the Fusion Centers. And I also extend the opportunity to any of the panel members that would be interested in a personal visit to one of these centers, or to our program office, to make that available to you. We have done, so far, probably in the rough order of magnitude, several hundred of these visits for congressional staff and other interested citizens, to include the American Civil Liberties Union, the Constitution Project, et cetera. So, I extend that opportunity to you, as well, and I look forward to any comments you may have.

Thank you.

MR. BEALES: Thank you very much, Mr. Riegle. Our second speaker will be Lieutenant Jeff Wobbleton, from the Maryland State Police, Homeland Security and Intelligence Division. Mr. -- or Lieutenant Wobbleton is currently assigned as the watch commander to the Maryland Coordination and Analysis Center, where he's served for 2 and a half years. In his 23-year career, he's been assistant barracks commander, domestic violence assistance commander, criminal section supervisor, he's done drug investigation and canine patrol and road patrol, and he's received numerous commendations, including a lifesaving award, superintendent commendations, and other letters of commendation.

Welcome, Mr. Wobbleton, and we look forward to hearing from you.

MR. WOBBLETON: Thank you. And I'd like to – on behalf of the men and women of the MCAC. the Maryland Coordination and Analysis Center, I would like to thank you for the invitation here, to, number one, tell you what Fusion Centers are, and what the capabilities are; and what they are not, and what we don't do.

I just want to give a little overview of where we've started out. November of 2003 -- right after 9/11, the executive management inside of Maryland saw that there was a -- disjointed information. A lot of the law enforcement agencies had 1-800 numbers everywhere, of Call us for information. There was three or four different law enforcement

agencies that the phone would be answered. But no real one place where all this information would come, and the information was disjointed, we couldn't all put it together.

So, after this, they rode up to New York, and, on the way back, said, "Hey, look, we need to do something about this. This information is not going, it's not flowing, it's not coming in, and it's not going out." So, what they started to do was -- is the Antiterrorism Advisory Council -- it's headed by U.S. Attorney's Office, Mr. Harvey Eisenberg -- and formed what is now called MCAC, the Maryland Coordination and Analysis Center, which now is called a Fusion Center. We're one of the first Fusion Centers in the Nation to actually set up a -- this Fusion Center process. Has there been a lot of bumps and bruises? Yes. Has it been a learning experience? If anybody would have told me, at the National Fusion Center Conference last year, we would have had over 500 people attending a Fusion Conference, I would have called them that they were crazy. There was about five Fusion Centers back in 2003, and, just recently, this thing has actually expanded.

Just want to go over a couple of incidents that -- what we can do and what we've done in the past. The Baltimore Tunnel incident was run out of MCAC. Two of the lessons learned, we've learned out of that, one of them is that the Federal Government was providing information that was not necessarily accurate, and that there was another -- there was another disconnect there. The other thing was private sector. We had a huge lesson learned about the private sector, I'll go into in a second. But with the Federal Government, DHS stepped up to the plate and formed a trusted partner relationship. That's what Fusion Centers are all about, is forming trusted relationships with our law enforcement, first responders, private sector. That's what this makes -- that's what makes Fusion Centers work, day in and day out, and that's how we keep the men and women safe on the street every day, is by forming trusted relationships.

We sat down with DHS, and we reviewed the Baltimore Tunnel incident, what we did right and what we did wrong. We found out that there was a disconnect with the Federal Government, that they were providing information out that was not necessarily accurate, and we wanted to close that disconnect. That's when DHS has decided to put a -- an INA person inside of the Fusion Centers. That is our connection with the Federal Government. We use that connection to get to the National Operations Center or any other Federal entity in there that needs information. We use the DHS INA person.

The second part of it was the private sector. Private sector, we see as a big, huge issue. MCAC originally started off with a private-sector working group of 20. Our private-sector working group now is well over 400 entities that are now working in conjunction. We also are working in conjunction with the ISAC council to try figure out what is the -- what is the role of the private sector, and how can we both benefit? During

the Baltimore Tunnel incident, what's sitting above the Harbor Tunnel is the -- Constellation Energy, one of the main North-South Corridors for electric. We learned that, Hey, look, we do need to share some type of information, and how that needs to be shared is what we're working through right now.

Where we are now. The present. Privacy policy is a big -- is a big issue. I was just in New Hampshire yesterday with the Northeast Regional Information Sharing Group. That's where all the Fusion Centers get together. We were in New Hampshire yesterday, and spent all day yesterday with Department of Justice, working over privacy policy, what can we do, what we can't do, looking -- taking a look at revamping, or taking a look at readjusting how we do our privacy policies, readjusting to -- what's the current trends, training within our own departments, making sure that all of our individuals inside of MCAC, and the people we share with, that they understand what privacy policy is all about.

We also have formed, inside of MCAC, as our U.S. Attorney's Offices has -- we're going to do our own internal review of policy with some retired Federal judges and Federal prosecutors, bringing 'em in and taking a look at our policy, and making sure it is -- making sure it's right.

So, it is very important to us. We are very transparent. If you go and look on Google, the Maryland Coordination and Analysis Center, you can learn everything about us. Our presentation is out there. We're hiding nothing. We encourage visits. We've had a ton of visits from anywhere from White House appointees on down to the men and women that we – our customers every day, the law enforcement and fire and EMS in there.

Governance and CONOPS, each one of the Fusion Centers are currently working on and revamping or readjusting their governance structure, how it looks, and also CONOPS and what we can do and what we can't do.

One of the other -- one of the other -- I like to use real, live incidents that we deal with, day in and day out, to give you, kind of, an overview of what we can do. During the Virginia Tech shooting, the Virginia Fusion Center was putting out information, keeping the other Fusion Centers aware of what's going on. Do they need to know what's going on? And do we need to protect the universities? Do we need to send personnel out there? Do we need to -- what, operationally, do we need to do, to take care of protecting people inside of Maryland? So, a Fusion- Center-to-Fusion-Center concept, we can pretty much solve all the problems.

One of the things -- one of the stories I like to tell is that one of our counties was actively working a homicide. An individual shot and killed his wife, and the only thing that they had to go on was a telephone number. And they called us and said, Hey, look,

we need some help with this. Can you give us some information on -- we're trying to find this guy. We took the pay-phone number, and, lo and behold, it was down in a place called Harlan, Kentucky. Harlan, Kentucky has 15 eating establishments -- 13 are fast-food, two of 'em are sit-down. Beside that pay phone was located was a Holiday Inn. Also, there's one road in and one road out. So, we have the ability to, number one, get the picture, find out what he's wanted for. We have a kind of a general idea of where he is now. Well, what do you do with that information? Prior to the Fusion Centers -- okay, you're going to go now, Kentucky, what do I do with Kentucky? How do I do this, or where am I going to go with this information? Well, it was pretty easy. We called the Kentucky Fusion Center, they put us in touch with the Harlan, Kentucky law enforcement authorities, sent them the e- mail. Forty-five minutes later, that guy was arrested, because of that bulletin, by an individual that was on patrol. Forty-five minutes later, a murderer was off the street. That's one of the things that we do.

How about a plane that's involved in a no-fly infringement, and then, 2 months later, is involved in another no-fly infringement. Putting the pieces of the puzzle together, that's the other thing that we do.

At MCAC, one of the questions we get all the time -- do we collect information on people? No, we don't. We bring information, we analyze it, and then we disseminate it back out. Whether the information is from the Federal Government, local government, or State government, it's brought in. How does it affect Maryland entities? And then we push it out to our Maryland trusted partners.

So, those are just some of the things that Fusion Centers do, and we don't do. As we move along here, Fusion Centers are an untapped wealth of information. They provide us with the access and the information to not only the other States, but also to the Federal Government. And we look forward to working with the private sector. The private sector is probably one of the biggest issues that we have nowadays that we need to try to work on, and we need to try to figure out. One of the things we're using in the private sector is the reach-back effect. We don't want the private-sector information, proprietary information. We don't want that. What we do want is that, if a LNG tanker is going up the Chesapeake Bay, and somebody fires a missile on it, what will happen to the tanker? It's easy to go to the LNG people and say, Hey, look, here's a scenario. What will happen? They're the experts, so they give us the advice that we need so we can answer those questions.

So, again, I thank you for the opportunity to come here and give -- provide a little bit of information about what Fusion Centers do.

Thank you.

MR. BEALES: Thank you very much. I, at least, look forward to the opportunity to ask you some questions in a few minutes.

Our third speaker today is Sue Reingold, who's the deputy program manager of the Information Sharing Environment Program in the Management Office of the Office of the Director of National Intelligence, where she's been since November of 2005. She was previously the associate director of the Office of State and Local Government Coordination. And her portfolio included coordination and oversight of activities supporting State and local interests in the areas of information sharing and collaboration, infrastructure protection, and science and technology. Before she joined DHS at its inception, she managed the State and Local Outreach at the Critical Infrastructure Assurance Office.

Welcome, Ms. Reingold, and we look forward to hearing from you.

MS. REINGOLD: Thank you for that kind introduction. I really appreciate the opportunity to be here today, and also really commend the Advisory Committee for focusing on the issue of State and major urban area Fusion Centers.

These Fusion Centers really area a critical component of a national information-sharing environment, but their participation -- it also does present some information privacy challenges. And, as you just heard in the couple of references to the new 9/11 Act, in particular the Act does require DHS to complete a report on the privacy and civil liberties impact of the Fusion Center initiative, that Rob was just talking about, by August 2008. And my office looks forward to working with DHS on that.

I guess today my remarks regarding Fusion Centers, they're design to provide a national perspective, and I want to make, I guess, at the outset, three central points.

And the first point is that Federal interaction in partnership with State and major urban area Fusion Centers is not about bringing State and local law enforcement into the intelligence community. As you've heard from the two others here with me, we're talking about -- it's really about trusted relationships to enhance sharing.

The second point I wanted to make is that State and local governments carry out their counter terrorism responsibilities within the context of their core mission, which is protecting local communities from crime, violence, and disorder. And it's important to understand that it's not a separate mission, it's about what they do every day.

And I guess the third point is that, within the context of the information-sharing environment, Fusion Centers will leverage existing information- sharing processes and information flows that are compliant with State, local, and Federal laws and regulations, like 28 C.F.R., Part 23; and that most existing information exchanges or information flows really already have their own privacy rules and protections. And, again, just as an example, 28 C.F.R., Part 23. So, it's not like we're trying to do something new. We need to

look at what the information exchanges are, what existing rules are, and then -- and then look to fill some of the gaps.

As I just mentioned, because State and local and tribal Governors -- they incorporate counter terrorism activities as part of the daily efforts to provide emergency and nonemergency services to the public. As a result, they're really part of this national capability, both as first preventers and first responders. And, as part of confronting the challenges of allowing them to perform these responsibilities, and also our job at the Federal level, we really have to transform our policies, our procedures, really, the way that we do business, and can't forget, the whole point of transforming our workplace cultures in order to reinforce information sharing as the rule, as opposed to the exception. And so, as a result, I, along with Ambassador Ted McNamara, lead the office that's been tasked to coordinate and facilitate this improved information sharing among those who need it to counter terrorism. And that means confronting two major challenges. You've heard a little bit -- some reference to this from my colleagues here. The first is that, at the Federal level, we have to rapidly share information related to terrorism with those outside the Federal Government, so that they can protect our local communities. And we have to provide that information in a format that supports the way our non-Federal partners do business. The other point is that there needs to be an effective process for gathering, analyzing, and sharing locally-generated terrorism information with other localities, States, and Federal Government, which is how this whole Fusion Center concept evolved. And, most importantly, we need to do these things in a manner that protects the information privacy and legal rights of Americans.

So, to give you some background into how the – what I do day to day fits in with the work of my Federal partners -- specifically, DHS and FBI -- in December 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act, and -- which called for the creation of the Information Sharing Environment, or the ISE. And the ISE really operates as a trusted partnership, as we've talked about, among all levels of government, to facilitate the sharing of terrorism- related information, homeland security information, law enforcement information related to terrorism. The 9/11 bill that was just passed by Congress also added WMD information related to terrorism to the Information Sharing Environment.

So, just from the standpoint of the ISE itself is the business processes, the protocols, the policies, as well as the information technology that enables the sharing of information across Federal, State, local, tribal, our private-sector partners, as well as our foreign partners. And it was the same law, the Intelligence Reform Act, that established my office, the Office of the Program Manager, and provided it with this government wide authority to plan, oversee, and manage the Information Sharing Environment. The law also created an Information Sharing Council, that's made up of 17 different Federal

departments and agencies, to advise the President and the Program Manager on the development of these policies and protocols and guidelines, and to ensure proper coordination among all participants. Part of the Council -- we also have State and local and private- sector participation through existing channels, through DHS and Department of Justice and groups that have been set up to represent those communities

To get specifically to Fusion Centers and how they fit into the Information Sharing Environment, to guide efforts to establish the environment, the President, in December of 2005, issued a memo to the heads of executive departments and agencies that had guidelines and requirements for the Information Sharing Environment. And what he did is, he set out some very specific priorities for the ISE and required departments and agencies to come back with recommendations. And these guideline reports were submitted to the President, and approved for implementation a year later, in November 2006. One of the specific areas that the President outlined as a critical priority was to develop a framework for information sharing across Federal, State, local, tribal governments and the private sector. And my office worked very closely with Department of Justice, DHS, FBI, National Counterterrorism Center, other Federal agencies, but also, right from the beginning, with State Homeland Security directors, law enforcement, fire, and other public safety officials from across the Nation, as well as the critical infrastructure sector partnership structure for the private sector, to develop this framework and the recommendations that the President approved.

Two things came out of these recommendations that are in progress right now. First was this -- as Jeff mentioned, sometimes there's a lot of information that comes from the Federal Government that can be confusing or perhaps not accurate, so the first recommendation that came out of this was: establish, at the Federal level, an interagency capability that's responsible for coordinating a production and timely dissemination of terrorism-related information, specifically for State, local, tribal, and private- sector partners, and do that at a -- at a level of classification, preferably unclassified, that can actually be used day to day to take action. The second, and what we're here -- and what this is all about today -- was improving collaboration at the State and local level by leveraging this, this effort, where we have State and major area information Fusion Centers, and actually, from a Federal perspective, working together to develop and make sure that we have a national integrated network of these centers.

So, basically, these recommendations that were approved by the President were based on the recognition of -- whether we call this information sharing and, at the State and local level, integrated justice, intelligence-led policing, information sharing -- the whole point is that we really – to enhance the protection of our local communities, it depends upon effective gathering, analysis, and sharing of intelligence and other sorts of information.

So, the point is that, from a national perspective, State and major area Fusion Centers will be the focus, but not exclusive points within States and urban regions, for receiving, developing, and sharing terrorism information. And the vision for these Fusion Centers is that they will become critical nodes connecting the Information Sharing Environment and enabling these trusted partnerships, and they'll be the institutions on whom we can all depend to -- you've heard the phrase connect the -- connect the dots at the State and local levels.

So, the idea is that the Fusion Centers will have a capacity to receive Federal information and further disseminate that to State, local, tribal authorities, private-sector entities within their jurisdiction, and do that in coordination with Federal officials, and that they'll also have the capacity to gather, process, interpret, and disseminate local and State information to other localities, States, and at the Federal level.

And so, the Federal Government continues to work closely with our State, local, and tribal officials to define the role of Fusion Centers within the Information Sharing Environment. And we recognize that the roles envisioned for these centers is challenging, and it's difficult. And we're working hard together to make sure that this a success.

So that the centers will blend Federal and local information and produce informational products that support the needs of law enforcement executives as they develop the strategy priorities for the departments, and, at the same time, produce information that supports the needs of fire chiefs, first responders, sheriffs, HAZMAT, police officers, State troopers, EMS personnel, who all work with community members to prevent and respond to crime, violence, and disorder.

So, again, I can't emphasize enough that all of these efforts be -- as part of working in the Information Sharing Environment, which is, again, by law, focused on terrorism-related information -- but these centers -- the whole point of their success is that they focus on day-to-day emergency response, crime control efforts, and other critical public safety activities, and that we know, really, that, in most of the country, it's not feasible for these Fusion Centers just to focus on terrorism information alone. For them to be enduring institutions, they have to serve the broader needs of the community, and they have to have the capacity to recognize a potential terrorism threat. And, again, this can be achieved in the context of an all-crimes or an all-hazards approach, which, in many cases, for all of them, is the most cost-effective way to approach pulling together these centers.

So, their long-term value really comes from their ability to gather, evaluate, and analyze all crimes and all hazards and all threat information, and that includes terrorism information. Again, we're not asking for these Fusion Centers to become part of the intelligence community, that we recognize and -- Rob, first off, talked about this -- that the Fusion Centers are owned and managed by State and local governments and that they support other governmental activities. The goal is that when there's a nexus to terrorist

activity, and that's discovered, that sharing information with each other and with Federal authorities will be second nature and there will be a coordinated mechanism to do so through this integrated national network of Fusion Centers.

So, the whole point is that they'll support national efforts to combat terrorism and local efforts to prevent crime, reduce fear, and improve the quality of life in communities across the country.

So, I think, just, again, from a national perspective and with all the activity that's going on, what we're trying to do is capture the momentum for the Fusion Center effort and try to adopt a common information-sharing culture that's going to serve and protect future generations, and so that the support and guidance from groups such as yours is really essential and very helpful and useful to integrate issues, in terms of making sure that we're paying attention to, and getting the right advice on, protecting the information privacy and legal rights of all Americans.

And so, I thank you very much, and I'll look forward to our discussion.

MR. BEALES: Thank you very much, Ms. Reingold.

If I could just start -- and I guess this maybe best directed to Lieutenant Wobbleton -- I'm interested in how a Fusion Center gets involved, in an operational sense. And maybe if you -- if we think about a situation where a police officer stops a car, runs the license number, it turns out to be a bad "guy." In what circumstances does a Fusion Center get involved? And how does that happen?

MR. WOBBLETON: I guess the best case I can give is that, on Interstate 95, a Maryland trooper, prior to 9/11, did stop one of the terrorists. Now, when an individual, or a trooper, a police officer stops an individual that's on a terrorist screening center watch list, basically what happens, the dispatcher will run the information, it'll pop up on the screen, call in a 1-800 Terrorist Screening Center. And what we are trying to accomplish here is that the officer needs to worry about -- at 2 o'clock in the morning, they need to worry about their safety, and they should only worry about the safety. So, what the center will do is contact the Terrorist Screening Center, find out what's going on, and provide that information back to them about what they need to worry about, do they need to worry about, and, "Oh, by the way -- our investigative arm within MCAC is the JTTF, and we operate off of the Guardian system, which is the FBI's system -- and, Oh, by the way, if the person -- you need help, we'll get you help immediately, because we have the connectivity for not only the local departments, but we also have the connectivity the Federal department." So, we'll do the background information, bring it in, analyze it, and then ship it right back out. And if they need assistance, we'll give them assistance right away. So, we have access not only to local, State, but also Federal information that we can, kind of, give a big picture -- what I call a "full plate of spaghetti" -- provide that full

plate of spaghetti back to that individual, so you know they're not out there piecemealing, where I'm going to have a little bit here, and the meatballs are going be over here, but I'm going to give 'em that whole big plate, right in front of 'em, so they really don't have to work too hard. And, you know, they're going to stay safe and they're going to home tonight.

MR. BEALES: In the -- in your -- you stopped the car on I-95, and the officer presumably runs the license number. Is -- that's not through you.

MR. WOBBLETON: No, sir. That'll be through the local dispatcher, wherever it be, State, local --

MR. BEALES: Okay. And the terrorist -- the watch-list connection pops up there, and --

MR. WOBBLETON: That's –

MR. BEALES: -- then -- does that automatically come to you, or is it at the discretion of the local dispatcher, or is it the local officer? I -- that's what I'm trying to understand.

MR. WOBBLETON: Right. It'll stay with the local officer, and it's -- and it is -- the local officers would have -- they have the option of calling the Terrorist Screening Center directly and dealing with them directly.

MR. BEALES: Okay. Or they might call you and –

MR. WOBBLETON: Correct. What we're trying to –

MR. BEALES: -- and deal through you.

MR. WOBBLETON: Right, correct. What we're trying to do in Maryland is say, Hey, look, call us, we'll take care of the background information. We're taking some of the work away from them, but then we'll -- like I told you, we're giving that full plate of spaghetti back to them so they don't have to work as hard. We know the ins and outs of the State, local, and Federal governments. It's easy -- it's easier for us to navigate the system than it is for each one of the -- each one of the agencies -- the 225 law enforcement agencies out there to -- Okay, what do I do with this information --

MR. BEALES: Right.

MR. WOBBLETON: -- and who do I contact? And then, Well, if it is somebody that I need to contact, then I need help -- well, what do I do with that? Well, it's pretty easy, we provide that one- stop shop, Call us, we'll take care of all your problems and make sure you're safe.

MR. BEALES: Okay. Joe Alhadeff?

MR. ALHADEFF: Thank you. And thank you for the presentations. They were very informative.

I guess I've got a two-part question, and it's not -- you know, it doesn't go to whether we need sharing of information or whether we need centers that can facilitate that sharing. I think that's clear, that they're needed and they have a beneficial effect. And I understand the need to share information in a very quick and effective fashion.

Where I get some concerns is the fact that some of the information that we're sharing will obviously then stay within the local systems, themselves, and may be shared between localities because some of that has now become part of the local information. And, as you go from a -- to a State-to- State-sharing model of what was originally Federal information -- Is there a way that that information is tagged? -- so there's an idea of where that information came from and what rules may apply to that information that may be different from State rules -- is part one. And then, since some State systems may contain this information, to what extent are those systems that may connect to the Fusion Centers and the Fusion Centers themselves filing formal privacy impact assessments?

Thank you.

MR. RIEGLE: I'll start on one piece of it, and that is the piece that deals with the actual information flow.

We don't store information in databases after the information is collected and archived. That -- typically, that information is from existing databases, and then a picture is gleaned from that information. If there is no reasonable belief that this person is engaged in any inappropriate activities, then it's immediately expunged, we don't hold onto it. If there is a report that's made because the person has a reasonable belief that this person may be involved in some inappropriate activity, it's handled just like it would be handled under any 28 C.F.R., Part 23, issue. Most States have adopted -- to the best of my knowledge, all States have adopted that standard within their centers. Obviously, that has to be reviewed periodically. And if it's not -- if it's not required to support an ongoing investigation, then it's released.

I think there's some confusion, to the extent that I -- I think people think that these centers are in there just, sort of, combing through data, coming up --

MR. ALHADEFF: Yeah.

MR. RIEGLE: -- you know, dots on people. And that's just not the case. It's just –

MR. ALHADEFF: Yeah. No.

MR. RIEGLE: -- typically –

MR. ALHADEFF: Let me try to give you a more specific example. A group of people are traveling through someplace. There is a concept that they may or may not be doing something. Someone's running a check, trying to figure out if they are. Maybe there are name similarities. You come back, you get some hits on them. That information is going to get populated in a database in a local system somewhere, because you got a hit of some kind, which may no longer be a valid hit after further investigation gets done. But that vestige of that information, because you don't -- I'm not saying the Fusion Center is holding it, but a State system somewhere may be holding it. And so, I guess my concern is not what's being held in the Fusion Center, because I think it's mostly a pass-through, it's what's being held in the ultimate State system that may have collected some of this information because there was a legitimate suspicion. And then, can we be sure that that information gets expunged?

MR. RIEGLE: Well, I think that's -- that would be an unusual case that you're describing, because I don't know of any State that really would return that back to a database, that I'm aware of. But, you know, I'd have to look into that. I think Jeff would be better suited to describe to you what databases there are. But let's us an example of where we might want to verify whether somebody's driver's license information was correct during a stop, something like that, or did they have a want or a warrant or something like that. That information would already reside in the -- in a database, and we would say, Okay, this guy's got a want or a warrant for, you know, X, Y, or Z, whatever that case may be. There isn't -- outside of the suspicious activity reporting that would be not germane to that particular episode, there isn't any sort of database that deals with that. When a suspicious activity is recorded, it goes into a suspicious activity database, and that particular database would then be required -- whether or not that was under intelligence oversight or 28 C.F.R., Part 23, determined by whether it's law enforcement or intelligence-related -- would have to go -- undergo the same level of scrutiny that it goes -- that any information, you know, residing in those two channels undergoes.

Is it possible that somebody is pulled over on a stop, and that a record is run against -- or their license plate is run against a database? Yes, that's possible. But that, in and of itself, doesn't provide any -- doesn't provide any sort of meaningful insight, as far as if it happens again. All it informs you of is that the person was stopped before for speeding or whatever that activity might have been.

So, once it rises to the level that there is a reasonable suspicion or a reasonable belief, it's kept in a database. If it's not, it's no more or less different than if you have a routine traffic stop in any environment, outside the Fusion Center or not, whether these centers were created or not. In other words, there isn't some sort of secret box that it goes

in, if it hasn't risen to the level that it has reasonable suspicion under 28 C.F.R., Part 23, or reasonable belief in the intelligence community.

MR. WOBBLETON: Let me take a shot at this. Two ways. One of 'em, if the suspicious activity comes in through a tip report, at least MCAC, we send it to the Guardian system. Our investigative arm is the JTTF. And they would take care of it. So, it's into the Guardian system.

Let me try to go the other way of -- and try to -- try to equate this whole thing to -- every day, law enforcement respond to suspicious activity. It could be just about anything, from the dog barked, to nothing. And those incidents would go, usually, into a Cat RMS or a run sheet or whatever, and they would just be put in there, and it -- nothing happens. It's closed out on the card, and nothing ever -- is ever become of it. So -- but if something arises to the level of suspicion, and it's investigated and has to do with a U.S. person, and we follow the guidelines of 28 C.F.R., and, if there's no suspicious activity, it's got to go out. We can't collect information that has no criminal predicate. So, I hope that answered it.

MR. ALHADEFF: And part two?

MS. REINGOLD: Remind us of part two, sorry.

MR. ALHADEFF: Part two was the privacy impact assessments on State systems.

MS. REINGOLD: Yeah. And that's actually the point I guess I was going to make, is that, you know, with good reason in the -- the 9/11 Commission Act, where Congress is requiring -- they're actually requiring a privacy report on, Take a look at this Fusion Center program and take a look at privacy issues. So, I mean, some of your points are well taken, in terms of -- we need to take a look at the critical information flows through the Fusion Centers with regard to the States and the major urban areas, and take a look at some of these things. So, I think you heard how things are being handled. But, from the standpoint of comprehensively taking a look at all these things, that still needs to be done. And, no, there aren't complete answers to all your questions, because some of that needs -- we need to take a look at that.

MR. BEALES: Charles Palmer?

MR. PALMER: Thank you.

A question for Deputy Director Riegle. You said that you haven't recalled -- you haven't received – excuse me—any privacy complaints. Two questions. One, do you think the public knows how to go about filing such a grievance? And that is, have you been proactive in any way in seeking such feedback? And, two, do you have any feel for how aware of these centers -- or how aware the public is of these centers' existence? I

mean, if I asked my mom, have you ever heard of a Fusion Center in Louisiana? I bet I know what I'm going to get, a nuclear-energy response. [Laughter.]

MR. PALMER: So, those are my questions.

MR. RIEGLE: I think you -- were you referring to my comments earlier?

MR. PALMER: Yes, I was.

MR. RIEGLE: Okay. You said Reingold. So -- we have a similar name, but we're not married, just so we clear that up. [Laughter.]

MR. RIEGLE: Yeah, I think it depends. It's a State-by-State -- it's based upon the individual centers. Some of these centers are very embryonic, they haven't been up long. So, is there a certain level of public scrutiny? Probably not. Keep in mind, though, that, almost in every case, these centers are supported by, you know, State legislatures. Money has to flow into 'em. They're not a big secret. They've been widely discussed in the press. There's been a number of articles that, I would say, following on John's comments, I think are a little bit unfair. They call them domestic spy programs, which -- we know that's illegal. So, I think the public scrutiny would be more than you might imagine. And, in addition to that, it's unfavorable, so it gets the hackles of everybody that has any issue with their State and local government up. So, I don't think they're near as obscure as you might imagine them to be.

In every case, these Fusion Centers -- that we're aware of; of course, we don't hear every detail of everyday events at every Fusion Center -- but in every case we're aware of where we have our Federal officers, there is a procedure in place for somebody that has some sort of question or comment or concern about their personal information -- there is a procedure for them to address that with that particular fusion center.

As Ms. Reingold just expressed, is there work that needs to be done? Yes, there is. This program was established -- that I operate, that I run -- was established in August of 2006. It's still a relatively new program. We're -- we are trying to learn as we go. We're sort of, you know, under the -- after 9/11, many programs are sort of bolting the wings on in flight. However, we believe in our indicators, we believe in the evidence that's presented to us. And our indicators and evidence, at this point in time, do not lead us to believe that there's any sort of widespread problems, as far as the personal information of U.S. citizens in these Fusion Centers. We do respect the fact that there's a potential for that, and that the -- that that possibility exists. But we have to believe in our indicators. That's true with the intelligence community, and that's true with the legal community. You go on the evidence you have, and we don't have any evidence to support that now.

If you ask somebody living in Louisiana, Do you know what LASAFE is? -- the Louisiana Fusion Center -- I would venture to say you'd have to come across a number of citizens before you would ever know. But if you went to LA and asked them about the

JRIC in LA, which is widely publicized and has a lot of political visibility, most would probably say yes. So, it's just really dependent upon the area of the country that we're talking about.

MR. PALMER: Would Lieutenant Wobbleton have a comment?

MR. WOBBLETON: I would have to -- the only additional comment to that would be that the publicity of the -- of the centers -- that's a very -- we operate in a very political environment, so it's incumbent upon each State to determine, Well, do you want to publicize, not publicize? Do you -- so, it varies from State to State. I know our law enforcement community and our fire and EMS community and our private sector, we're very well known. We're very well known throughout the United States and the Nation. But if you go to an individual person on the street -- well, you know what? I take that back. One of the things that we do, we publicize -- we have overhead signs, messages on the highways, and it's 1-800-492- TIPS, call in your terrorism -- or suspicious- activity tips. So, we publicize that on the billboards. Does anybody know where it goes to? No. But it comes to us. So, do we -- does it provide an opportunity for private citizens to report that activity of -- I don't know, what's -- what to do with it. I'm driving down the highway, and I'm from New York, and I'm in Maryland. Well, what's the best thing for me to do? Why, oh, look, 1-800-492-TIPS, call in suspicious activity. They're filming the Bay Bridge. We provide that for any citizen to call in. The biggest part of that is that we get the information, we send it right back to the locals, of, Hey, look, can you locate this vehicle in -- what's the activity? And then, at the same time, put it in the Guardian system and notify JTTF, Hey, we have this particular incident going on. Hopefully, that answered your question.

MR. BEALES: Neville Pattinson?

MR. PATTINSON: Thank you. I think I'm a -- much of more of an educated person on Fusion Centers due to the three people's testimony, and I thank you for that, this morning.

I have a question, really, about data integrity that goes into the system and gets assimilated and goes out. As a first part, how is that data integrity achieved, as far as validating information? And then, during the assimilation and the dissemination, how is that integrity assured? That's the first part of the question.

The second is, really, about the controls of the access of that disseminated information. How is it protected? Is there -- you know, are you e-mailing it to folks? Is it -- is it on secure Web sites? Is it going to their pages? Is it username and password protected? What's the protections made to protect the access to that information?

So, it's a question, I guess, for the panel, as a whole, but certainly from a practitioner, I'm sure that Lieutenant Wobbleton will have some comments. Thank you.

MR. WOBBLETON: Data integrity -- we'll -- let me start off with the dissemination of information. We rely heavily on classifications of the information. So, if it's -- of course, if it's classified, we have -- we follow the handling procedures, and it really can't -- can't really do a lot about that. LES and unclassified information, again, most of the information we would send out -- we'll start with the private sector -- unclassified information, non-law- enforcement-sensitive information -- send it out to the private-sector community over here. Here is the latest trends. Sometimes the Federal Government may provide a unclassified report that may need to go down to the private sector, focusing on water, sewage, energy, somewhere that they may need to get, so we'll use our e-mail distribution list to get that -- to get that out.

I have to be very careful about data integrity, because I like to know what definitions of what data integrity is, and what are you -- what's your definition of what data is. And, again, I go back to -- MCAC does not store any information of any kind on persons, inside.

So, we take the U.S. persons or people out of the equation, then we go -- now we're down to incident- based information or threat information that needs to go out. And, again, there's a couple of ways we could do it. If it's something immediate we need to take care of, we have a -- an intel contact in each one of our counties. If it's something -- let me use -- this is -- it's kind of funny, but it -- it's true -- is that, during the hot spell of the summer months, down on the Eastern Shore, we have a big population of chicken farmers down there, and there was a large amount of chickens that were killed off. And they called us up and said, hey, look, if you see a large amount of chickens ending up at the landfills, don't be alarmed. This is what it's all about. It's funny, but if we don't have a handle on the situation and do rumor control and put that information out beforehand, we could have a huge mess.

So, we've got that information, and we send it out to our partners, of, Hey, look, this is what's going on. Don't push the panic button. And I've had a number of incidents where some other agency would push the panic button, and we would send out resources -- i.e., we'd send out people in fire trucks or law enforcement or somebody in a police car, jeopardizing their lives. If we go, and we take the 5 minutes to make the two phone calls that we had to make, we found out that, okay, this incident really didn't happen. It happened 2 weeks ago. So, we're not going to -- if that -- God forbid that the fire truck goes up to the next intersection and is involved in an accident, and somebody's killed. We don't want that. We want to make sure that the information we receive is verified. And if we need to send somebody out, we're only going to send 'em out on legitimate issues or legitimate complaints that we need to worry about.

Hopefully, that answers your question.

MR. PATTINSON: Yeah, certainly that gives the, kind of, integrity side of things, thank you. And it's -- kind of, the concern there is that -- you know, Can terrorism be used to trigger an event through the Fusion Centers? And so, I like the idea that you've got checks and balances to validate and verify that information; otherwise, you know, that could -- the very centers could be used to send flashes through, nationally, that could cause us to respond erroneously, or confuse us in that information. So, data verification and integrity is important.

Then the access to this information -- private sector, you're doing e-mails and so on. That's what I understand. Confidential or classified information, what are the access controls for those? Is that through, you know, specific IT systems, or -- what are the -- what are the processes there?

MR. RIEGLE: Let me -- I'm glad you followed on with that, because that's an important issue.

Unclassified information can still be sensitive information, in many respects, so there are some systems and portals that are in place that are access-controlled, and they would follow the same Federal -- they're typically Federal systems, and if they -- in come cases, like the HSIN State site, that's still a Federal system, but it's been put together and built for the State with the same level of access controls and data integrity, guidelines, that govern all Federal systems, which -- you know, we read about the Chinese hacking into DOD, into the SECDEF's office, so, I mean, it's as good as we know it to be, and as robust as we think it needs to be presently, until we're proven wrong.

Having said that, there are a number of portals that have very special interest within the Department of Homeland Security that are restricted to people that have a need to know.

The basic floor for information-sharing with the intelligence community and law enforcement community to date is still the need to know. Do you have a legitimate need to know? And if that's a documented need to know, then we'll give you systems accesses to where that information can be revealed. Have there been spills where law enforcement information was spilled to the open Internet? Yes, that has happened, just like the access to the DOD systems. I mean, nothing is 100 percent. But in every case where we share information, it is, you know, very thoroughly scrutinized who are the appropriate people.

Now, having said that, I think there's also a cultural aspect that we need to be realistic about here. The 9/11 Commission Report, in general, pushed the Federal Government to sharing information to a fault. In other words, we'd rather put things at risk and make sure that people have the right information than err on the conservative side, where somebody that needs that information doesn't get it, and there's a gap. So, if you were in the intelligence community, as an example, when I first came into the

intelligence community during the cold war, if you had a piece of legitimate intelligence or threat information, that was your relevancy to the community, and that was the culture, and you protected that to the point that you would eat the piece of paper it was on if it was going to be exposed. And that would be true for law enforcement information, as well.

Now we're at the point, after 9/11, where it is quite obvious that the first thing that you need to consider when you have a piece of threat information in your hands is, who do I need to get this information to, to mitigate that threat? Well, that is heresy to old cold-war intelligence officers, so it's a very difficult cultural shift to make.

I think, at the present time, we're still making that shift, and so, we actually over classify -- tend to over classify information, which is unfortunate, because much -- this information doesn't do any good until it gets to the person that can mitigate that threat. That, typically, is the local first responder. But, in every case, regardless of whether it's classified or unclassified, or whether it's sensitive, but unclassified, it's on a system that has some level of protection identified by the basic premise of, Do you have a need to know?

Now, on the secret-level systems, the Department of Homeland Security and the Federal Bureau of Investigation have come to the conclusion that there is a legitimate need, in some instances, for State and locals to have access to classified information and to classified information systems. Those systems checks are the same. They don't go from the Federal Government system to a State system. Everything done on the classified level, so anything above the unclassified level is on a Federal system. There is no linkage to a State system.

The opposite holds true for the States, though. Their law-enforcement-sensitive information, which might, at the Federal level, oftentimes be classified because it would reveal sources and methods, is on their systems, and it oftentimes goes up to a classified system from their law-enforcement-sensitive system, which still has checks and balances. So, it's still a very conservative process, how information is handled, stored, and disseminated. It is not ever intended that we're going to make information publicly available on threats, because we're not in the business of educating our adversaries, and we need to be sensitive to that. Even though people have a legitimate need to know, we also want to make sure that it's -- only the people that have the need to know get that information.

MS. REINGOLD: And if I could just also add, from a national perspective, all the various elements that you mentioned, of information assurance -- obviously, there -- across the Federal Government, there are -- there are already many efforts and initiatives and roles -- responsibilities that are taken by OMB, you know, across the Federal enterprise, DOD working together with the intelligence community and others -- DHS,

DOJ -- to basically, in the course of, just, whatever type of information it may be, to have standard information assurance, protocols and standards, and NIST and other standards bodies. From the perspective of the program manager, it's our responsibility to leverage all these existing efforts and extend that across the Information Sharing Environment. And that would be across, basically, all levels of classification.

So, Rob just talked about classified information. Obviously, that -- we extend the Federal rules to our State and local and private-sector partners, much the same way, you know, for years, there's been an industrial security program for our Federal contractors, and those rules are in place. So, it's a matter of extending that to what I'll call our Federal -- our State, local, and private-sector partners, in making sure that there's also a robust program.

On the sensitive-but-unclassified, I had mentioned the President's priorities for the Information Sharing Environment. In addition to the Federal, State, local framework I had talked about, another area that he asked for recommendations was to come up with a standardized way across the Federal Government that we can handle sensitive, but unclassified, information. So, that -- there's a report that is going through interagency coordination, and should be going to the President shortly, that actually lays out a new regime for controlled unclassified information that standardizes the handling. Again, we brought our State, local, and private-sector partners into that discussion. As the Federal Government, we can't compel or require, outside the Federal Government, people to abide by Federal rules, but, through all our discussions, we've gotten every indication that this will not be difficult to extend and -- in terms of into the State, local, and private-sector environment, that they can easily take on these procedures. So, there's a lot of work ongoing to address the issues that you've raised.

MR. BEALES: Joanne McNabb?

MS. McNABB: I was interested to hear that MCAC has privacy policies and is creating a review panel of outside people to review them. And I wonder if -- this question is for whoever has the answer -- how common it is for the Fusion Centers to have written, elaborated privacy policies and outside advisory review boards related to privacy and civil liberties.

MR. RIEGLE: Quite common, because we require it before they can spend any Federal money. So, if you hold -- you know, and it's not a carrot-and-stick approach. You can't use that. I mean, you can't make the carrot be that you won't use the stick. So, in other words, you can't just threaten to withhold money in order to get compliance in those areas.

As a -- as a matter of baseline capability within the grant guidance, and also within the National Fusion Center Guidelines, we ask that each Fusion Center, before they use

Federal dollars, that they agree to certain baseline requirements of -- one of which is the development of a policy.

Now, what we had done early on is, we had just left it there, you need to develop a policy. We've taken a different tack, where we're proactively sending people out to say, here is a best practice of a policy. This is, kind of, what we mean when we say, 'This is a policy that would meet the threshold for you to be able to exercise the grant money or to, you know, consider yourself as a part of this national network.'

And Jeff described a recent activity through the joint grants office between Department of Homeland Security and Department of Justice, working with the experts in the privacy offices in both -- in the civil liberties offices and both -- Alex Joel is involved in this -- to set up a standard that says, Here's what we're really looking for. Instead of leaving it to your imagination what we intended, now we're taking a more concrete step of moving forward and saying, This is exactly what we're looking for.

And now what we are doing in these regional meetings that Jeff described is, we're walking them through that process, and saying, here's what you would have to do. Here's some of the basic considerations.

The baseline capabilities doesn't leave it there, it also requires annual refresher training in civil liberties and civil rights, and other areas, too – operational security, you know, areas of concern to the Federal Government, as far as the protection of information, as well. So, it's been a -- been a -- a slow, uphill climb, but, I think, recently we've gotten a lot of momentum behind it, and a lot of it occurred because we're getting people together in one forum and saying, Here's what we mean. And that helps, sort of, unify the process.

MS. REINGOLD: And in addition to privacy guidelines, it also requires a privacy officer, much as, recently, you know, all Federal agencies are required to have a privacy officer. So -- and when Alex is here -- Alex Joel -- this afternoon, I'm sure he'll be talking a little bit more about the privacy guidelines that have been developed, and you can get into more details with him.

MS. McNABB: And how about an advisory board at the local level, is that common?

MR. WOBBLETON: I don't know if it's common or not. It's something that MCAC has decided to do, to take a look at everything, to make sure that we are following in the guidelines of 28 C.F.R. and we're not doing anything wrong. We do not want to mess this up. We want to do the right things. We want to make sure we are, again, transparent, and we do listen to our trusted partners of the DHS and DOJ. And we want to make sure that we're doing the -- nobody has written the book on Fusion Centers and how to operate 'em. So, like Rob said, yeah, we are -- we've strapped our -- bolted our wings on, and we're

flying; as we're going along, these hiccups come up, and we don't let 'em sit for 6, 8 months. We go, and we take care of the problems and make sure all the other Fusion Centers are talking, and make sure all the other Fusion Centers have the same thing. It's a -- it's a network that we've set up, and we do not want to mess this up.

MS. McNABB: Thank you.

MR. BEALES: Could I ask for a 1- to 2-minute tutorial on what the heck's in 28 C.F.R., Part 23?

MR. RIEGLE: Well, it is -- it is a -- it's a Federal application, it's not a State and local application. State and locals have to adopt that on their own. In most cases that I'm aware of, the States have taken it. But, in general, it provides the guidelines, most notably, for the person that's in a -- effecting an information request out in the field, what the thresholds are, what that information can and can't be used for, et cetera, et cetera.

Now, these guidelines for law enforcement are very similar -- and they're widely known. I mean, if you ask all law enforcement persons that have ever gone through an academy, this is, you know, sort of Policing 101, sort of -- same thing as Miranda. In the intelligence community, it's not as familiar. And so, what you end up having is, you've got different oversight rules. One of the complaints of the State and locals is that you've got different -- and multiple systems. And we have different multiple systems in many case -- because the oversight is different. The oversight for the intelligence community is different than the oversight for the law enforcement community. Because most of these centers were stood up under the backbone of the law enforcement activity, they're very familiar with 28 C.F.R., and they don't fall under national intelligence programs, per se. Really, the people that come from the intelligence community that would be funded by national intelligence program money would fall under that oversight. So, what you end up having is, you have very similar rules. There are some minor distinctions in how you can handle the information, how long you can retain it. The thresholds are very similar. It's really the retention and storage that's a little bit different. And I'm not -- it -- I'm a lawyer, but I'm not a lawyer that specializes in that area, so I'd leave that to our attorney, and Tim Bailey could probably give you some – a clearer insight to it.

But, in general, it's just basic guidelines for policing, and handling information on people when you are policing, same thing as in the intelligence community, Executive Order 12333.

I would also add to the -- to the comment that Jeff was making. When we look at these information systems, I think it's a fair point to make that most of the information that we're talking about is threat information that reveals itself in less specific terms. It could be geopolitical information on Cuba, for instance, that would affect South Florida. It can be information that deals with a very broad threat that al Qaeda made, you know,

through a video from al Zahari or somebody like that. It doesn't go into these granular -- typically, go into these granular issues, where U.S. persons are identified. That -- that's really the rare exception, that some threat is revealed that identifies the perpetrator within that threat. That's unusual, and, typically, an arrest is effected right after that, if they come across this individual.

So, I want to just emphasize that the bulk of the information that we share with State and locals is very broad in its perspective. It doesn't really go down to that level that you would see very specific information on very specific individuals. That's quite the exception, not the rule.

MR. BEALES: Ramon Barquin?

MR. BARQUIN: I have a -- I think, a reasonable understanding and -- vis-à-vis the role of Fusion Centers, in terms of the vertical flow, meaning Federal, down to the State, and the need to bring it together; and in the other direction, if there's potential intelligence. My question has to do with what I heard -- obviously, for all sorts of good reasons, there seems to be an emerging horizontal network of Fusion Center to Fusion Center, State to State, local to local. And are there some issues there that we might need at least to be concerned about and make sure that we've got the proper check and balances? I mean, I go back to the Lieutenant's comment about the importance of the developing -- the development of trust and the relationships. And I'm all for trust. Trust also tends to open the door when you've got the shark on the other side, going back to Saturday Night Live. So -- question.

MR. RIEGLE: I'll start, and then let -- or have Jeff finish.

I think the thing to understand is that the environment that we're in, the threat environment we're in currently, is not necessarily to determine terrorism, but oftentimes to rule it out. And where the national network, the State-to-State piece comes into play is during an actual incident. That's when you typically see the importance of it.

So, if we go back to the case that Jeff mentioned earlier, the Virginia Tech incident, what happens immediately after that's revealed on the news is, every State wants to know, Is my State likely to suffer the same set of circumstances? And, of course, if you go back to the day that VA Tech occurred, what CNN was saying is that it was a Chinese immigrant that was -- that arrived on U.S. soil a year previously, and so, you know, is Chinese -- does that lend itself to terrorism? Possibly, in the mind of many State university officials, it could. So, the job, really, of this horizontal piece oftentimes is to rule that out.

So, in this particular case, we were able to -- and I'll just, kind of, walk you through it so you understand the importance of it -- we receive information from the Virginia State Police, who have the lead investigative authority on that, not the campus police,

because they don't have jurisdiction over capital crimes. That information goes to the Fusion Center, of which a piece is that there is a gun, there's a serial number. We run that serial number through the law enforcement support center in Vermont. So, it went from that Fusion Center to the Vermont Fusion Center, where the law enforcement support center for the -- for Department of Homeland Security is located at. That Fusion-Center-to-Fusion-Center information goes back when we know that the gun was identified by the owner, who was also a victim -- you know, it was self-imposed, but -- so, we can -- we can pretty quickly determine, based upon that information, that this isn't a terrorism-related event. We knew, for instance, within a matter of hours, after talking to the mother of the victim, that the person had some mental health issues, and that this likely wasn't a situation where it was going to be related to -- you know, wasn't going to have an effect on other campuses. And they need to know that, because it's expensive to gear up to protect a university, number one, but then, in addition to that, we have that obligation to calm the public fear. That's where you see the State-to- State connectivity.

Another example would be the Luxor bombing. That bombing was in Las Vegas. Every hotel in America wants to know, am I going to be a victim? And we knew, as soon as we got the victim's ID and it was run through the Fusion Center in Las Vegas, that they had prior domestic disturbance complaints where the victim was -- did identify that he felt threatened by his spouse. So, you can then take that information and apply some sanity to it and say, is it likely related to other events, or are other events likely to occur? No.

And that's the benefit in the State center. You don't have to go to the national level for us to determine -- they can see, by themselves, or for themselves, that these aren't really issues. So, in this realm that we live in, where many things are -- rule out terrorism, especially industrial plant accidents, et cetera, et cetera -- that's where you see that benefit occur.

And then, I also want to identify that we have a -- in Department of Homeland Security, a Lessons Learned and Best Practices Web site that people can go to. And it didn't get addressed in the last question. But that's an area where we can give an example of a policy -- privacy policy that people can download and begin to look at, as well. So, I wanted to get that in before we broke, today.

MR. WOBBLETON: I just want to go into the practices of trusted relationship. Number one, we have nondisclosure statements that everybody has to sign. And if you do disseminate the information, there are things that we can do.

Now, if we're talking about classified information, already we have rules about classification and -- so, those are pretty clear.

So, if an individual -- I give Rob some trusted information, and then Rob goes and sends it out to everywhere and his mother, well, the trust is now gone, and that -- Rob no longer is going to get that information. This is a very fragile environment that we're in right now, trusted relationships. And I think everybody in the Fusion Center atmosphere understands about the sensitivity of the information, is that if you get the information, and you make the wrong step or you do the wrong thing -- I keep going back to -- we're jeopardizing lives. The people that are going to get on the fire truck, the people who are going to get in the police car -- we're jeopardizing their lives. And if we keep that in mind while we're doing this whole thing, then, you know, those trusted relationships will last, and they'll work. And those conversations -- you – this whole process is about human-to-human contact. It's nice to have all these systems and e-mail and everything else, but what it's all about is -- I call Rob Riegle up and say, "Hey, what is actually going on? And what -- hey, by the way, what can I disseminate, and what is good?" Because we have to remember, also, these are ongoing investigations that we don't want to impede the investigation, we don't want to get in their way; we want to support what they're doing, but, at the same time, we want to let everybody else know, "Hey, look, you need to worry about this," or, "No, you don't need to worry about this." And it's all about picking the phone up and saying, "What can I do for you, and how can I help you, and how can I help the people in Maryland?"

MR. BARQUIN: I just want to -- because I understand the genesis and the role and the importance to rule out terrorism. The question is, Once you have established the legitimacy of the Fusion Centers, the role they play, and once you now have established -- know that horizontal network among Fusion Centers, et cetera -- for reasons other than terrorism -- homeland security now gets out of the question -- and, do we have at least a potential -- a potential set of issues that we need to establish checks and balances, vis-a-vis privacy?

MR. WOBBLETON: I'm glad you brought that point up. The focus -- or the discussion here focused a lot of on terrorism. A lot of the Fusion Centers, to include MCAC are -- we are all-crimes. Some of the Fusion Centers are all-crimes, all-hazards. So, terrorism is just one part of it -- what we deal with every day. There may be a drug house somewhere else that we may need, or there may be a homicide somewhere else, or, if it's a first responder, we may -- in Maryland, we have the Maryland Emergency Management -- that side of the house that -- we need to deal with them. During Katrina, when Maryland went down to help out in Katrina, providing them information to make sure they're -- that they're protected down there. So, if we -- Fusion Centers cannot focus strictly on terrorism. It's all-crimes, and a lot of 'em are all- crimes, all-hazards.

Do we need to put checks and balances in place? I agree with you. What they are -- we're open for discussion. And, as we go along, the privacy policy may need to be

expanded, may need a little adjustment here and there. We're open for suggestions, like I -- earlier, before -- transparency, that's what we're all about. We listen to everything. We listen to suggestions. We listen to suggestions of the Federal Government. We adopt their policies of privacy and how we handle information. It's all about the partnership and the trusted partnership of -- as we move this thing along.

MS. REINGOLD: And so, in answer to your -- the short answer to your question is, yes, in terms of, there are some issues here. But the good news is -- and Jeff referred to it -- that there's -- a lot of other States have come together regionally. He mentioned the northeast, there's a southeast, and others, as well, so that there is actually a way to basically come together and have those discussions, and, you know, map out what are the information-sharing protocols, what's the concept of operations, and work through some of those things. So, absolutely, that guidance and the role of this board and the role of DHS is important in that.

MR. BEALES: I think we have time for one more question.

Larry Ponemon?

MR. PONEMON: Thank you. I really appreciate your discussion this morning. It's very informative.

Hypothetical question now. What happens when a Fusion Center blows up? I mean, not in the nuclear sense, but things just happen. So, there's the wrongful use or misuse of someone's sensitive information, or perhaps there's a data leak, and it gets into the wrong hands. Ultimately, who is accountable? And how will the public be informed? Or should they be informed? Does that actually compromise our ability to find the bad guys and bring 'em to justice?

Can I start with the Lieutenant?

Thank you.

MR. WOBBLETON: At least in MCAC, we have what is called our Antiterrorism Advisory Council that's overseen by the U.S. Attorney's Office. So, that's, kind of, our governing body. It's made up of 16 executives -- 13 are State and local and include two of the fire chiefs; and then there's three Federal Government agencies that oversees what MCAC does, day to day, and how we function, and which way we're going. So, that's going to be our governing body of how we're going to operate.

I guess, one of your other questions was misuse of the information or leaks of the information. I guess, the best way to handle that would be that we operate under the guidelines -- we are operating out of FBI space, so we follow FBI guidelines of information dissemination and handling of leaks. To this date -- I've been there 2 and a half years. The system -- we've been operating for almost 4 years. We've never run into that

problem. But, again, the privacy policy addresses the mishandling of information. And I go back to -- training is a big part of what we do every day, working with DHS and privacy policies, and making sure the men and women that operate 24 hours a day, 7 days a week, they understand about the use of the information, and making sure that the checks and balances are in there.

Hopefully –

MR. PONEMON: But in –

MR. WOBBLETON: -- that answered you.

MR. PONEMON: But is there one person, for example, that has ultimate accountability in your organization for privacy issues, or is it a shared responsibility across the entire center?

MR. WOBBLETON: I think every person in the center has a responsibility about the information and where it's disseminated to. No one person is there 24 hours a day. And hopefully -- I don't -- I don't know if we're on the same wavelength or same thinking track here, but each person in there needs to understand about information and how it's used and where it goes to. The one central person, or the one person at the end of the day, day-to-day operations, will be the director of the MCAC. That will be the person that's responsible for anything and everything that's coming in, going out, and he answers to the ATAC.

So, hopefully that answers that question.

MR. PONEMON: So, in -- just -- and this is just a hypothetical, of course, but if there were problems or issues, that it -- you would have a procedure, internally, to get that to the appropriate person, the person responsible for the Fusion Center.

MR. WOBBLETON: Yeah --

MR. PONEMON: So, ultimately, that person is accountable for a privacy-related breach or some event that resulted in the misuse of information.

MR. WOBBLETON: Yes, sir.

MR. PONEMON: Okay.

MR. WOBBLETON: Short answer, yes, sir.

MR. PONEMON: All right, good. Good. Thank you.

MS. REINGOLD: Yeah. And I think it's fair to say -- I mean, because these are owned and operated by the States, the buck stops with the Governor, from the standpoint -- it's a State function. Now, there -- for those functions that the Fusion Centers perform that are national functions that support national objectives, obviously the Federal

Government has the oversight and the obligation to work with the Fusion Centers. And Rob also mentioned, if those Fusion Centers accept Federal funds, then we also have -- in terms of the leverage and can require certain things. So -- but from the standpoint of -- they are -- you know, these aren't Federal entities, they're State entities, so -- so, obviously, it comes down to the Governor, ultimately, and his employees.

MR. PONEMON: Actually, may I ask a question for Mr. Riegle? Because it's relating to that point, and I think it's very important. If the Department of Homeland Security is funding a Fusion Center, and the – I think that there are hundreds of millions of dollars being spent today, and probably it's being -- it's a good investment, because we need to do this. But, at the end of the day, what would happen if there's a Fusion Center that has a pattern of not respecting the privacy rights of citizens in that State? Would that affect the funding decision?

MR. RIEGLE: Yes. I –

MR. PONEMON: Thank you.

MR. RIEGLE: -- think the important thing behind that is that it would affect the -- it would affect the funding of the Fusion Center, but typically we would do something more proactive, which would be to go in and obviously try to educate on where the behavior failed.

I think where you're at risk, if you wanted to really kind of identify it, is -- let's say, for instance, you receive a public health threat. Well, that information is governed under a different set of laws from a -- from a privacy point of view, under HIPAA, let's say, if it was a case of a person that had TB, like the gentleman that was flying around, trying to contaminate North America. If you had that particular case, you know, obviously the correct way to deal with that is that we have an individual that has TB, anybody that had any contact with the person, displaying these symptoms in that area, would be X. But it doesn't mean that you've got to identify that individual, per se. But let's say that leaked. Probably not an egregious thing, since it's already out in the press, in that case. But let's say it did leak. Then it becomes an education issue. Could you withhold their money? Yes, you could. But what you would try to do first, proactively, is to educate them. And we do have those mechanisms in place.

I would say this. One of the things that we put ourselves at risk for when we -- when we support these centers, from a Federal perspective, is, there is no Plan B. If you shut that down, there isn't another node within that State that supports that functions. That's why these things do have a little fragility, as Lieutenant Wobbleton was describing. There isn't anything else. And so, right now, when you put all your information-sharing eggs in that basket, and that basket hits the floor, proverbially, then you do put the national network at some risk. And that is a weakness. And it underscores why it's so

important that we do follow these guidelines and that we are proactive and that we do stay vigilant on it, because there is nothing else. There's no other mechanism for passing this information. We have almost wholly used and leveraged this system. So, we need to be sensitive to that.

MR. PONEMON: Thank you.

MR. BEALES: I think we can try to slide in one more question here. Tom Boyd?

MR. BOYD: Thank you. I'll be brief -- or as brief as I can be.

It's important for us -- and this, by the way has been a very informative presentation, and I want to thank you all for that; I think we all do -- but it's important for us to try to separate fact from fiction. This afternoon, EPIC will testify. I'm looking forward to their testimony, as well. But we've been -- we've been provided the materials by EPIC, and included among those materials are -- is the claim that Fusion Centers are really government efforts to, quote, establish operational domestic surveillance programs, close quote. I wanted to give you an opportunity to respond to that kind of an accusation. That's a politically- charged phrase, obviously, but would you like to respond?

MR. RIEGLE: Well, phrased in that manner, it's illegal. We don't have a domestics collection authority, nor do we pretend to have that authority. Are there -- is there information out there that's been legally obtained by local law enforcement that we are entitled to know, if it exposes or reveals a threat to the United States of America? Sure we are. But we do not have a domestics collection capability. We don't intend on having that. We do not task these Fusion Centers to go out and collect on U.S. persons, because they have authorities under law enforcement at the local level that we at the Federal level don't possess. No. And there's no evidence to support that charge, and it's baseless. But in a politically sensitive environment, we understand that. We understand that the potential exists and that the concern is based upon that potential. And we recognize the importance of demonstrating to the American public and to the overseers, based upon your own particular affiliation, that we are in compliance with the law. There is, to my -- the best of knowledge, not a center that would be unwilling, at any time, 24 hours a day, to bring in an outside observer to watch their activities. I know of no such center. And I think, again, we have to be careful that we follow evidence and not hyperbole. If we see there is a problem, we are going to be the first to react to that, because we do understand the fragility of this network. And we're hypersensitive to the fact that we cannot have these perceptions out in the American public. It does us a great disservice if we do.

Thank you.

MR. BEALES: I want to thank all three of you. This has been a most informative session. We appreciate your patience with our questions and your willingness to spend your time with us this morning. So, thank you very much for being with us.

It's time now for us to turn to our subcommittee reports to find out what's really happening. And we will start with the Data Integrity and Information Protection Subcommittee, co-chaired by Charles Palmer and Ramon Barquin. And I think Charles has the report.

MR. PALMER: Thank you, sir. The subcommittee met yesterday after a bit of a hiatus. We were so pleased with our work on the RFID paper that we've been casting around for a similar -- similarly important topic. And we came up with one.

One of the aspects of the responsibilities of this full committee is often overlooked, and that is the integrity word, something very near and dear to Ramon's heart. And so, Ramon and I had begun exploring how we might delve into that -- its importance, its awareness, what do people think about it? And the question does keep coming up, as it just did with the previous panel.

The definition of terms, like data quality, physical integrity. What does it mean -- backup and recovery? What is the effect of backup and recovery processes on these things? And how policies governing the use of specific bits and pieces of data might be somehow glommed or stuck to that data so that its maintenance and verification of its integrity, as well as other things that might be associated with it, would follow that data as it flows through systems.

So, we were thinking real hard on this. But, as often happens, a higher-priority request came in this week. So, now the subcommittee is going to, sort of, set aside that integrity question. We're not going to let it go, we're going to set it aside. And, instead, we'll explore various aspects of anonymization and de-identification, some terms that come up often in our work here.

There seems to be a considerable amount of confusion about what these terms mean, when one or the other is appropriate, if either, and what, actually, one has to do to accomplish them, if one can at all. We want to explore, perhaps, another framework approach to advise the disparate components of DHS as to what they might do to decide if this stuff is appropriate for their needs or not. And many of these areas -- anonymization, anonymizers, if that's what you're familiar with, de-identification -- these are known to be a -- we realize these are areas of active research, really hard problems. Some of the geeks in the crowd are probably just rolling their eyes, saying we can't do it. And maybe you can't. The question we are going to explore is, What aspects of these topics can be used to solve some of the problems that the components have?

So, we'll be working with the Privacy Office, in light of the fact that this is a very hard topic, to bound this exploration and ensure that what we do serves the needs of DHS.

We will continue to pursue this line of inquiry, and we hope to provide a report at the next meeting, depending on how successful we are in bounding the effort.

Ramon, would you like to add to -- so, that's our report.

MR. BEALES: Thank you very much. The Privacy Architecture Subcommittee, Joanne McNabb and Jim Harper.

MS. McNABB: We are working on three different projects right now, two of which we expect to have a draft report on for the March meeting of this committee to present to the full committee. And one of those is related to additions to the -- to incorporating privacy considerations in the guidance provided to State and local applicants for DHS grants, to be able to feed our recommendations, ideally, into the 2009 grant program. And another -- so, that's one – two, also for March, is we will be providing a draft of some guidance on -- a privacy proficiency framework that can be used by DHS in developing training programs for Fusion Center staff and, potentially, for DHS employees elsewhere, as well. And we'll have a draft of that also in March. And, third - -

MR. HARPER: Where Joanne will highlight the prospective successes, I'll highlight the past failure.

We've continued to work -- and still are working -- on the assessment we've tried to do on how changes in technology have eroded privacy protecting policies and practices over time. Working the ISPAB group, I presented to them on our work at one point since we last met. It's a big challenge to try to meld together the varieties of thinking that have been done on fair information practices, our framework document, and categorizing the kinds of changes in technology, and then assessing how all these -- how all these meet together in a matrix that may extend to thousands of -- thousands of points.

But we'll continue to discuss and work on it, in one or another, and try to come up with some more theoretical work that -- my ideal goal is to actually simplify all this stuff. By -- I think, by looking at it through the right lens, we can make this stuff more simple so that implementers on the ground have a better time protecting privacy and all the values, policymakers have a better time protecting privacy and all the values that relate to -- so, no success yet, but maybe.

MR. BEALES: It's certainly a worthy goal. And, finally, the Data Acquisition and Use Subcommittee, David Hoffman.

MR. DAVID HOFFMAN: Thank you, Howard. I'd like to start by first continuing to solicit public input and comment on our existing documents that we have ratified as a committee in the past and are posted on the DHS Privacy Office Web site. We take all of the comments seriously, and review all of them; and all of those documents are intended to be living documents, and we will revise them accordingly when we get input in.

Second thing I would like to do is to talk briefly about the work that we are engaged in. We are looking at the sharing of personal information in the emergency management situations, and how best to provide practical guidance to FEMA and to other components of the agency who need to share information in situations where an emergency would happen.

And I'd like to take this opportunity to specifically thank the members of the staff in the Privacy Office. I think those viewing the Privacy Office from the outside cannot completely comprehend the level of dedication and diligence that the folks in the office have, how incredibly supportive they have been in helping the committee get a hold of the information that we need. The American public is well served by these public servants acting in this capacity.

In -- particularly in respect to our emergency management project, we are looking at how privacy can be comprehended proactively up front by FEMA in setting up its information-sharing relationships so that, after an emergency happens, privacy issues do not in any way inappropriately slow down the variety of things that the agency and the Department are going to have to accomplish. For example, finding people who are lost, providing benefits, authenticating people who are going and doing disaster recovery on the ground. This is a huge task, given the number of local and State governments that potentially would have to be interacted with and the timelines that you talk about having to need to get information shared and the lack of infrastructure that may be available at that point in time. So, we have had discussions with folks from FEMA, are learning considerably about the different models that they have for sharing information, and are feeling good that there are some processes in place to make sure that, when information is shared, that there are obligations that go with the data. We're looking to, hopefully, provide some very practical guidance, given our expertise in -- from members of the committee -- doing similar sharing environments in our own lives in the private sector, to allow that to be done, perhaps, more simply and in a very proactive way prior to the event happening.

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

Let me take this brief opportunity to do something I probably should have done at the beginning, and that's welcome our newest member, Dan Caprio, onto the Advisory Committee. As I'm sure you noticed, people putting their tents up, which is our signal that you want to talk. And I'm sure you will. Dan I worked together at the FTC, and I look forward to working with you again.

We will now break for lunch and our administrative session. Please be back, because we will start promptly at 1 o'clock. So, please back here in time to be in your seat and ready to listen at 1 o'clock. And if you want to sign up for public comments, please

find Lane Raffray, in the back of the room. We would love to hear from you later this afternoon.

So, thank you all.