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

AFTERNOON SESSION

MR. BEALES: I want to welcome everybody back for our afternoon session and thank those of you who are here for being prompt in returning.

Let me remind you again to be sure your cell phone is turned off, and that Lane Raffray is in the back of the room. If you're interested in making a public comment later this afternoon, we'd love to hear from you, and please sign up with Lane.

Our first speaker this afternoon is The Honorable Charles Allen, the Assistant Secretary of the Office of Intelligence and Analysis in DHS. He's served in this capacity since September of 2005, and also serves as the Chief Intelligence Officer, reporting directly to the Secretary of Homeland Security.

Before joining Homeland Security, Mr. Allen was the Assistant Director of the -- of Central Intelligence for Collection, since June of 1998, and chaired the National Intelligence Collection Board. He served in the CIA in -- since 1958, in a variety of positions of increasing responsibility.

Mr. Allen, I know you have a tight schedule this afternoon, and we appreciate you being with us, and look forward to hearing from you.

MR. ALLEN: Thank you very much. It's a pleasure to be here, and a pleasure to speak to the Data Privacy and Data Advisory Committee.

Let me just say that I hold a couple of hats, as you pointed out in the introduction. I report directly to Secretary Chertoff, as the Assistant Secretary for Intelligence and Analysis, and his Chief Intelligence Officer -- gives me responsibilities to oversee the intelligence activities guidance, to give direction and evaluation to the intelligence activities of the entire Department.

I also have a -- my budget is a classified budget, and I report to the Director of National Intelligence, Mike McConnell. So, I have a -- I'm a little bifurcated, but it works very well.

At Homeland Security, the Secretary has directed me to improve the quality and timeliness of intelligence across the Department, to integrate the intelligence activities, including the components, to share information and strengthen relationships with State, local, tribal, and private sectors, and to ensure that DHS has an intelligence place within the national intelligence community, and that -- we have succeeded, because I'm a member of Mike McConnell's Executive Committee; and also for improving transparency and responsiveness to the Congress.

My office, last year, was designated by Secretary Chertoff as the Department's executive agent for information sharing. Didn't ask for it. The memo showed up on my desk. That was the first I knew I was going to be the executive agent, per se.

We've created a number of mechanisms to bring together the Department's vast knowledge base and expertise, and to strengthen information sharing right across all the elements of the Department, and also to share that information appropriately with our external partners. Good intelligence is of little value if we can't put it in the hands of those who need it, and via processes that are both lawful and appropriate.

Before the attack on September the 11th, 2001, anyone over the age of 50, if you asked, where were you when President Kennedy was shot? I think everyone could tell you where they were and what they were doing when they heard the tragic news. I think, today, anyone over 15 can tell you exactly where they were and what they were doing when the planes crashed into the World Trade Center and into the Pentagon, September the 11th, 2001.

I was at CIA headquarters, as the Assistant Director of Central Intelligence, having breakfast with a Navy commander named Kirk Lippold. As many of you know, the USS Cole was under his command when it was attacked by small boats -- by a small boat on 12 October 2000 while refueling at the Port of Aden, in Yemen. At the breakfast meeting, Commander Lippold confided he was surprised the United States did not react more strongly to the attack on the USS Cole and the destruction of our embassies in East Africa,

back in August 1998. And he was -- he said, in my presence, it would take a similar event to awaken America to the threat posed by al Qaeda central leadership.

I sent him on his way to get some briefings at the agency, and, shortly after that, at 8:43, American airliners -- American Airline Flight 11 out of Boston crashed into the north tower of the World Trade Center. That -- I always think of that, because Commander Lippold's comment does come back to me. Here was a similar event that has certainly changed my life, and it changed, I'm sure, all of yours.

My middle daughter once asked me, when will things get back to normal? With -- she's anxious how she's going to raise her two grandsons -- I mean, our two -- my two grandsons. I told her that this is the way it is. This is the new normalcy. Security lines will always exist. Gone are the days of easy travel. Identification checks are more prevalent wherever you go. If you travel to London and wander the streets, for example, no less than 300 cameras will film you in an 8-hour period, because -- closed-circuit television. And there are thousands of those cameras throughout the U.K.

As we remember on 9/11, we almost -- we also must take stock of where we are today and where we need to go. America is better protected today than it was 6 years ago, and Homeland Security has had a big hand in making that possible. We have -- we have secured better air travel, sea travel in -- sea interests in this country, and we're securing our land borders. We are certainly better organized. We've improved our capabilities, and we're sharing information.

At the Federal level, we're building a more robust information-sharing capacity, and we have that greater capacity for sharing with State and local partners. Both Secretary Chertoff and Mike McConnell are firmly committed to this critical task. We have a responsibility not only to share information, but, as Mike McConnell says it, to provide it.

A lot of work needs to be done. Successful counterterrorism efforts require Federal, State, local, tribal, and private-sector entities to share information so that we can prevent, respond to, and recover from an attack upon this country.

Improving how we share information is at the heart of efforts to prevent another 9/11. Both the President and Congress have required we develop and maintain a commitment to information sharing. This requirement responds to a key lesson from many of the investigations and studies conducted after 9/11, that we did not, again, quote, connect the dots, close quote. And having served as the Assistant DCI for Collection, that hurt very much, that we didn't get our job done. I know it only too well and too painfully.

We had important information in our hands, but not in the right hands -- but not the right information in the right hands in a timely way. To fix that, the Intelligence

Reform and Terrorism Prevention Act of 2004, the law that created the Office of Director of National Intelligence, mandated an information-sharing environment. There needed to be a way to allow information sharing between and among Federal, State, and local agencies, the private sector, as well as with our foreign allies.

In March of 2006, the President appointed Ambassador Ted McNamara as the program manager for Information Sharing Environment to lead that effort. I certainly meet frequently with Ambassador McNamara, and one of my senior officers is with him for several hours this afternoon.

At the Federal level, we are making information sharing a natural part of our work by coordinating more closely with State and local, the boots on the ground, who better understand the local realities and are certainly more expert in regional issues than we are here in Washington.

Two weeks ago, I was in New York City to attend a conference hosted by the New York City's Fire Department. I met with Fire Commissioner Scoppetta, and he gave me a tour of the Fire Department's Operations Center, which was very impressive. Adjacent to that Operations Center was a room, and in that room was a classified facsimile machine, a secure telephone, and a computer terminal for accessing Department of Homeland Security classified network. I provided that equipment and that informational capability up to the New York Fire Department. Cleared firefighters working in the Command Center have access to that equipment to receive timely and actionable information on threats, and we provide, almost on a daily basis, threat warnings, threat assessments. We work so closely with the FBI in doing threat advisories in order to provide informational situational awareness to people at all levels of government.

On the other side of the coin, we realize that first responders have information that may prove valuable to the Federal Government. With information sharing, we're giving the people charged with keeping our country safe the ability to make connections they otherwise might not have seen. We didn't see it prior to September the 11th, but today I think we're enabling people to connect dots.

State and local Fusion Centers are key to the two-way flow of threat information, and I'm pleased that you all are looking into that this afternoon. They greatly enhance our ability to share information between Federal Government and our partners at the State and local level. Regional Fusion Centers will enable States, regions, and cities to combine their considerable resources and expertise.

Sharing more information, though, can be a doubled-edged sword, and you all are extremely concerned about that. We're able to access more and better information for the local and the national levels, but we have to be vigilant in what we do with it. As we do this important work, we must always keep in mind the fundamental importance of

protecting privacy and civil liberties. Our country is not defined by just our borders, it is defined by the States and the cities -- it is not defined by our States and cities, it is not defined by the many cultures of our citizens. What truly defines us as a nation is what makes us uniquely American, are the freedoms and liberties provided by our Constitution. Two hundred and twenty years ago, 39 brave men changed the course of history by signing the document that is foundation of our freedom. This, too, was a great and similar event, and, more than anything else, it is our freedoms that define us as Americans.

The men and women that I am privileged to work with in the intelligence community share a commitment to those constitutional principles and to the rule of law. I am proud, as an American, and as someone sworn to uphold the Constitution, to witness that commitment. Every intelligence officer takes that oath, I do solemnly swear that I will support and defend the Constitution of the United States. The Constitution. Not the property of the United States or its borders or -- not even the people of the United States, but the Constitution of the United States. I took this oath as a young officer at the Central Intelligence Agency in September 1958. I take this oath very seriously, and, each day, try to live by the principles embedded in it.

I must say, I was at the 60th anniversary, yesterday, of the Central Intelligence Agency, and, as I looked and met with my colleagues at the Agency, and with their families, celebrating the 60th anniversary, I was very proud, because I know each of those people believe very fervently, just as I do, in defending those freedoms.

Doesn't mean that I, alone, am responsible for ensuring our constitutional rights and privileges are protected in the intelligence world. Like I say, I'm joined by thousands of dedicated career professionals who oversee the work of the Federal agencies that are engaged in national and homeland intelligence and security efforts. Every organization in the Federal Government has an Office of General Counsel and an Inspector General. And more and more of them are establishing civil liberties and privacy officers. We're subject to oversight by the Congress. Congress created the Privacy and Civil Liberties Oversight Board that provides civil liberties advice and oversight on all Federal counterterrorism operations. And Congress required that guidelines be established to protect privacy and civil liberties in information sharing. And State and local governments have their own mechanisms for protecting civil liberties and conducting oversight.

There are many articles written about safety and freedom, security and liberty, and how we balance them. If you Google the term security and liberty, you'll find over 31,000 articles written about balancing between liberty and security. Unfortunately, there seems to be a consensus, if you have more of one, you necessarily have to have less of the other. I'm not one who believes that. I prefer to think of it this way. If we do things that add more security, then we also have to do more things to ensure our liberties are

safeguarded. They're mutual obligations of our governments, they're implanted -- implemented together. We have a -- we have a homeland security intelligence enterprise that we're building, but we will also have a privacy officer, represented here by Mr. Hugo Teufel. We also have a civil rights, civil liberties officer, represented by Dan Sutherland. So, there's all -- we always work hard to keep that balance.

It is not always obvious how to protect the country from physical attack and safeguard privacy and civil liberties. We must worry about an -- agile, determined, technologically savvy enemies doing their best to do us grave harm.

I was briefing the House Homeland Security Committee on threat, a very candid, very open briefing on the inbound threat to the United States. Our adversaries don't, and won't, play by any rules. And that certainly applies to the threats I see. To them, the end justifies the means, and that end is the destruction of the West, and particularly the United States. If you've read the bin Laden tape of 7 September, he holds us for all the iniquities that you can imagine.

So, the question is, how do we find our enemies, while remaining true to our principles? How do we share information while protecting the privacy of Americans? How do we keep ourselves both safe and free?

Many people believe that balancing our liberty and security is a brand-new challenge. I don't think so. Our founding fathers recognized this when they wrote the Constitution. The Preamble lays out this challenge plainly. The Constitution was ordained and established to provide for the common defense, but it was also to secure the blessings of liberty to ourselves and our posterity. The Constitution was written to do both, provide for our defense, safeguard our liberty. In order to do this, our founding fathers recognized the necessity for the executive branch to share its powers with the legislative and judicial branch. And that's what we're doing today with the Secretary and the Deputy Secretary, is we're explaining the threat in a very transparent and open way.

The concept of power-sharing has roots that run deep in American tradition. In 1788, James Madison write, if angels were to govern man, neither external nor internal controls on government would be necessary. If he had bothered to look, I'm sure he would not have found any angels necessarily working. Even at that time, not everyone was an angel in the public sector. He suggested the adoption of secular safeguards against government abuse. One of those safeguards, of course, was the cycle of elections. But Madison realized that elections, by themselves, would not be sufficient. Experience has taught mankind the necessity of auxiliary precautions. Between elections, the three branches of government would have to keep a close watch on one another. Ambition must be made to counteract ambition, Madison wrote in his most famous dictum.

Thomas Jefferson wrote about the dangers of concentration of power, and recommended eternal vigilance over those serving in high office. "In questions of power," he wrote, "let no more be heard of the confidence in man, but bind him down from mischief by the chains of the Constitution."

The overwhelming majority of those who serve in the intelligence agencies are men and women of enormous integrity -- and enormous talent, I might add – among the best anywhere in public service or in the private sectors.

Yesterday, we had George Herbert Walker Bush at the 60th anniversary of CIA, and he spoke briefly -- President 41, as we call him. And I had a chance to sit -- to chat with the President. And he understands that very well, and he spoke of the greatness of the intelligence community and of the Central Intelligence Agency, which he served as head for 3 years.

Jefferson -- and there's -- he resoundingly endorses the integrity that is represented within intelligence -- Jefferson's eternal vigilance will remain necessary, though, because, inevitably, in every organization, a few will lack honor.

In the 1970s, we faced this challenge. Many of you may remember the congressional committees -- maybe not all of you, you're so young -- led by Senator Church and Representative Pike, and the investigation conducted by then-Vice President Rockefeller. I was overseas at the time, so it was almost distant to me, but we followed it very closely from overseas posts, where I was serving.

They looked at some abuses of intelligence organizations. From these -- investigation, rules were developed by the conduct of intelligence activities. The oversight committees -- the select committees were established. And I report to those select committees on the part of the Secretary and DHS intelligence. I report to Congressman -- or to Chairman Reyes, chairman of the House Permanent Subcommittee on Intelligence. I report to Senator Rockefeller, of the Senate Select Committee on Intelligence. Those oversight committees -- and I was up there yesterday, talking to the HPSI, to the House Permanent Select Committee, telling them about issues that we were addressing. And I think those select committees have served the intelligence community very well. Sometimes we -- sometimes we get unhappy with the demands being made, but they have upheld and safeguarded, I think, the vigilance for which they were charged.

Every President since the formation of the select committees has upheld rules that safeguard our privacy and civil liberties. These rules require we pursue our mission in a vigorous, innovative, responsible manner that is consistent with applicable law in the Constitution, and with the respect of the principles upon which the country is founded. Adhering to those rules has been part of the fabric of the intelligence community.

Although the task of protecting privacy while sharing information sounds like a unique problem, it really, as you can see, is not. Federal, State, and local agencies have been focused on protecting privacy when sharing information in criminal justice systems, between law enforcement agencies. Privacy is the subject of numerous Federal and State laws and policies, all of which provide protections and real guidance on how to share and protect, at the same time.

At the Federal level, we have developed recommendations for privacy guidelines for the information-sharing environment. This process has been led by the Director of National Intelligence and the Department of Justice, with close involvement of the Department of Homeland Security. These recommendations establish uniform procedures that Federal agencies must use to implement privacy protections. Under these guidelines, agencies must, among other things, identify any personal information that might be shared, determine whether and how it can be shared, and put in place a process for ensuring that privacy rules are followed, audited, and enforced.

We recognize that State and local governments face their own rules and challenges. These guidelines call for engaging with State, local, and tribal governments to develop and implement policies that provide similar protections.

It is imperative that we work in partnership to create this trusted environment, to both share and safeguard information. In doing this, we are reinforcing existing relationships and forging new ones. But our most important partnership is not with the Federal Government, or even with the State and local governments, it is with the American people. That's our most sacred trust. We cannot do our jobs, in any level of government; we cannot protect this country and our communities, without that trust. We must continually demonstrate that we're worthy of that trust. We do this by showing respect -- respect for privacy and respect for civil liberties. We do this by reaching out to the Arab American, Muslim American, and other communities that have felt especially vulnerable after September the 11th, by welcoming every community's contributions to making America safer.

In July, Dan Sutherland, the Department of -- civil rights, civil liberties officer, and I met with Muslim, Arab, Sikh, South Asian, and Middle Eastern students. We listened to their concerns and thoughts about civil rights in America. They disagreed with the notion that they live in a -- dichotomous worlds that are impossible to reconcile. In their view, while religion and nationality are different concepts, they're not mutually exclusive. For example, the consensus among Muslim students was that they felt both Muslim and American, and were very integrated into our society. If you read the unclassified key judgments of the National Intelligence Estimate, that was approved in June and issued in July, you'll see that that's very much part of the judgments made by the intelligence community under Mike McConnell.

I can tell you that I was impressed with these young men and women. They represented some of the finest qualities in American youth. I can also tell you that I left the meeting hopeful that a number of them would come and work for me, hopefully in the near future. They're very bright and very able people.

I can assure you that we're being vigorous, innovative, and responsible, both sharing and safeguarding information. We must keep our country safe while remaining true to that oath, that I took in September 1958, to support and defend the Constitution of the United States. We, in the intelligence community, have every intention of protecting this country while respect its founding principles.

Thank you very much.

MR. BEALES: Thank you very much for a very thoughtful and interesting statement.

Could you give us a sense of the outbound information from you to State and local governments through Fusion Centers? What is the -- what's the typical -- the typical alert look like? And, in particular, to what extent does it -- does it name names, if you will, or include personal information, as opposed to a more generalized threat assessment?

MR. ALLEN: It does -- it's not -- it doesn't contain personal information and specific information. We get in threats every day. They're threats. Most of them are not valid threats, but they may concern a particular area or a city or a State. We, working with the Bureau, assess this threat. We do what we call threat warning, threat assessment. If it's one we can't resolve, we'll either -- if it's at a classified level, we will transmit it at a classified level. The FBI has greater communications to the Joint Terrorism Task Forces, and they do a remarkably good job. But the same language we agreed on between ourselves, we'll send it through our classified networks. Most of this, we can send at official use level. For example, on the 7th of September, when we received the full translation of the bin Laden 26-minute videotape, first time he -- we'd seen him in 2 years, certainly a proof of life, that he was very much alive, with a -- with a beard that had been darkened, and looking a little bit more robust than, perhaps, he had in the past. What everyone was calling in -- the Fusion Centers, Homeland Security advisors -- was the fact -- you know, were there threats? And there were not threats, as we -- as this was translated by CIA's Open Source Center, when it was made available off a extremist Web site. And we were able to reassure them.

This goes on constantly. We sent out over 200 joint advisories with the Bureau last year, doing that. Now, some of the assessments can be at critical infrastructure. We can send classified things, if they're sensitive, out to the State Fusion Centers, and we can also, obviously, brief cleared people in the private sector, if they have to take some measures that can mitigate a threat against a particular private sector -- could be water and gas -- I

mean, oil and gas; it could be commercial facilities; it could be the electrical industry. This is a very routine process that we do.

Frequently, we have, like, the attacks on the 29th of June 2007, when there was an abortive effort to bomb a disco in Haymarket Street in Central London, near Picadilly. We sent our first word out at 5:40, saying, "We don't know exactly what's going on. We don't think this is necessarily translated here, but, hold on, we'll see." By the -- and then we sent out a more formal advisory with the Bureau, saying, "No, this looks like this is very much directed at the British, not to us. Don't worry."

There can be more specific threats involving, at a classified level, certain extremists who are foreign, who are trying to, perhaps, enter the country. But that's the rare occasion.

These are very routine things, done -- sometimes very timely, but we know how to do it, and we certainly -- it is not something that contains sensitive, private -- privacy information on Americans.

MR. BEALES: David Hoffman?

MR. ALLEN: And I've got time for one more question, I think.

Yes, please.

MR. DAVID HOFFMAN: Secretary Allen, thank you very much for coming in. Your remarks are very well received.

And I just wanted to ask you -- I'm particularly drawn to the concept that you were mentioning of the environment of trust and the very real threats that we have to our homeland and the need for the information, and the processing of the information. And I'm just -- we get a chance to see, firsthand -- many people don't -- the incredible efforts of some of the oversight mechanisms, like the Privacy Office of the Department of Homeland Security. Most people don't get an opportunity to see that. How do you think we're doing about creating that environment of trust with the people in the United States and people outside the United States? And what could we do better to communicate the oversight mechanisms that are there and how we are protecting to make sure that the information -- that, once it's used for this very real need of protecting the homeland, it's not used for secondary purposes that could actually harm the individual?

MR. ALLEN: That's a very -- that's a crux of it all. We've got to build that trust. And I think -- what I see the Secretary -- the Secretary is a stunning individual, he and the Deputy Secretary -- but the Secretary reaches out across the broad community. The leaders of Homeland Security, the Director of National Intelligence also -- and I was just with Mike McConnell, Sunday night and all day on Monday -- he feels this very deeply, and he has his own issues to discuss. But we have to build that trust. And I believe that

our messaging has not been uniform. I don't believe that the American public -- I don't even believe that Congress necessarily understands -- based on conversation on Capitol Hill with a variety of people on both sides of the aisle and both houses of Congress -- understands the extensive oversight, the extensive review that goes on to protect liberties. The fact that I have -- I have four officers on my staff who are attorneys, who rigorously have to educate our people on how to handle U.S. persons data. Every one has to take rigorous training each year on how to protect and manage and handle U.S. persons data and not -- and purge data that's nonrelevant.

I think there's -- I think there's a poor understanding across the executive branch. I think there's a poor understanding in the congressional branch. It -- we are not doing the job -- to some degrees, we have to partner with you. I have to partner with Hugo. Hugo is an incredible privacy officer -- tough, hard, fair -- but he's a person that –where we can sit and communicate. But I think we have to do more of this jointly, because it is -- it is not there. And the important thing, I think, is the training -- the training, right across the board, of all intelligence and security organizations, is the purging of files, ensuring that we have careful audits. The fact that we have, you know, inspector generals, General Accounting officers -- Office -- we have, I think, significant oversight. I'm -- at times, we grate, here in the intelligence community, on the oversight committees of intelligence. They do a very tough job.

But, again, I think our messaging is very poor. I don't think there's a -- we've got to build trust and partnership with you all -- privacy, civil rights, civil liberty officers. We have to have a very strong partnership. And I think we have to speak, together. We may not always agree. We -- there may be differences. But the fact that I think the American public -- I think, generally, they do put their trust in the government. I don't believe they distrust the government. But -- and, I think, in times of crisis, they look to us. And -- but in day-to-day business -- we will be attacked again, I have no doubt of that. As Scott Redd said, the other day in an interview in Time magazine, where he was very eloquent -- he runs the National Counterterrorism Center -- we can't stop all attacks. What we have to do is stop a devastating attack that will hurt us politically, economically, psychologically, like September the 11th. We're working very hard to do it.

But I believe we can balance liberty, while also having security. It's not an either/or. You don't have less of one and more of the other; you balance the two. But I think we're -- we have to work more closely with you.

MR. TEUFEL: I just wanted to say -- okay, well, if I knew how to operate this -- I wanted to say that I can't think of anyone else that I would rather be in front of a committee with than Charlie Allen. And it seems that we happen to be in front of committees increasingly more often these days.

It -- you mentioned trust, David. And trust if very important. The Department is a very interesting place. There's military folks -- the Coast Guard -- there's lots of law enforcement, and there -- and then there are intelligence people. And they all are wary of people outside of their own communities. And to Charlie's and Intelligence and Analysis's credit, the I&A folks and Charlie have -- they get it. They've brought us, and they work very closely with us to make sure that what they do on behalf of the American people is done right, and that privacy is respected.

And so, I'm very grateful that Charlie came to talk to you all today, and it's a pleasure working with Charlie. And it's too bad we don't have more time, because Charlie has great stories and can -- and just amazing experiences that he can -- he can relate. And --

So, thank you very much, Charlie.

MR. ALLEN: Thank you.

MR. BEALES: Thank you very much. We really appreciate your being with us.

And, you know, if there -- if there's anything specific we can do where we can help, that's part of what we're here for. So –

MR. ALLEN: Thank you very much.

MR. BEALES: Our next speaker is Alex Joel, who's the civil liberties protection officer of the Office of the Director of National Intelligence. He reports directly to the Director. He was appointed to this position by Director John Negroponte in December of 2005. He joined the CIA's Office of General Counsel in October of 2002. Prior to that, he served as the privacy technology and e-commerce attorney for Marriott International, and was part of creating Marriott's first privacy officer position. And, before that, he was a technology attorney at the law firm of Shaw, Pittman, Potts & Trowbridge, and a U.S. Army Judge Advocate General Corps officer.

Mr. Joel, welcome, and thank you for being with us.

MR. JOEL: Thank you for inviting me. Thank you for having me here in front of you. Thank you for having me here, Hugo. I very much appreciate the invitation. I work -- I have the privilege of working closely with Hugo Teufel and the rest of his highly accomplished privacy staff at DHS. So, it is very much an honor to be here, and I thank you for that opportunity.

I almost don't feel the need to be here after hearing that excellent speech from Charlie Allen. When the head of an intelligence component of the intelligence community, as Charlie Allen is, comes in and talks in such eloquent terms about the balancing of privacy and civil liberties with national security, as he just did, I think that

that illustrates the commitment that I -- we all hope exists, and I happen to believe exists, at all levels of the intelligence community. So, I think that is excellent.

I am the -- and I do want to talk about the issue of trust, because I do think that that is something we struggle with a lot, and have to think about and work on at all levels -- I am the civil liberties protection officer for the DNI, as you said. And my position was established by the IRTPA, the same statute that created the Director of National Intelligence. As you know, that statute established the DNA in the wake -- the DNI -- in the wake of 9/11, trying to better lead the intelligence community to connect the dots, prevent another 9/11 attack from happening. And when Congress created that -- the position of the Office of the Director of National Intelligence, they also created my position, and I believe they did so in recognition of the fact that protecting civil liberties had to be at the heart of national intelligence. As we were uniting the intelligence community, they also felt that we needed a position to focus on our most bedrock values at the same time.

I do advise the DNI on privacy civil liberties issues. And as Charlie Allen said, he, like everybody in the intelligence community, takes an oath, as do I, do support and defend the Constitution. So, we are all protecting our Nation's values, not just my office and not just Charlie.

You know, as the first person to hold this position, I thought it would be useful to just give a little bit more, sort of, a personal flavor of my background for you all, since this is the first time you've met with me personally.

As you mentioned, when 9/11 happened, I was the privacy and e-commerce attorney for Marriott International. I loved -- that was a great job -- I loved that job. And I knew I had to do something for the country, and I was, sort of, exploring different ways of doing something for my -- for public service. I had been a JAG before, so it would be a matter of reentering public service at that time. And the Department of Homeland Security hadn't been set up yet, as you recall. And, at that time, they had been thinking of an Office of Homeland Security. So, I remember writing to Governor Tom Ridge, when he was over at Pennsylvania -- still in Pennsylvania -- saying, "You know, maybe you need something like a private/public partnership kind of guy. Maybe I could do that for you." And it was at the recommendation of somebody in the prior administration that I even thought of applying to the CIA. It hadn't even occurred to me to go in that direction. But I did it, because I felt, well, here's an opportunity to take the plunge and do something in the national security area.

I was an attorney at the CIA, working on intelligence matters for 3 years, and then, when the IRTPA passed, Ambassador Negroponte was the first Director of National Intelligence. He wasn't named until May. And I was actually detailed over to the DNI as an attorney in June of '05. So, I was one of the very first people that was over at the DNI,

and my specific task was to help define the role of the civil liberties protection officer. I was named the interim person to hold the position, given my privacy background and my keen interest in civil liberties matters. And I helped define the position. And, around the December timeframe, Ambassador Negroponte asked me to assume the duties on a permanent basis, which I did. And so, now I work for Mike McConnell on a -- as the -- as the DNI.

I was very glad to hear Charlie Allen talk about the concept of balance. And the way that he did it is a concept that I have, myself, talked about in the past on many occasions. I actually like to visualize it as a scale. And so, if you think about it as a scale -- I like to think in terms of metaphors. Of course, metaphors don't always work. But I -- but it actually helps in how I approach my job, because it's a very difficult challenge that we all face, and how do we do this balancing?

And, you know, like he said, I think you have to do both, but it's always easy to just say that. You hear that as a platitude a lot, We have to do both. We have to do both. But what does it actually mean? You know, how can you do both? And so, when people think of it as a scale, they think, Okay, we're going to do more on the national security side. And, of course, we have to do more on the national security side. I think that's a lesson from 9/11. Obviously, we need to do more on the national security side to prevent another 9/11 from happening. So, you're weighing down the national security side of the scale. And so, people say, Well, naturally, you're giving up on the civil liberties side of the scale. And I actually saw this -- I don't know if you saw this front-line documentary called Spying on the Home Front, I believe it was. And they had a clip of a former FBI officer, at one point -- agent -- saying, Well, if I give you more security, I've got to take away some of your liberties. So, he was doing this with his hands. And I was saying, Well, you know, he has -- you know, no individual FBI officer has the right to make that decision, obviously. So, you know, if you're going to give more -- if you're going to do more on the national security side of the scale, I'm thinking, What are the protections I'm going to add on the civil liberties side of the scale? How am I going to counterbalance what we're doing on the national security side of the scale with additional protections on the civil liberties side of the scale? What kind of safeguards am I going to add?

And I think technology -- because I think that's a special interest of this committee -- is a very nice example of that. So, technology can be used on both sides of the scale. You can use technology to help on the national security side of the scale, obviously. You can also use technology to help protect privacy. And I -- we've actually commissioned a couple of studies to help us figure out, Can we use technology to help with privacy protection? You know, both long- term research -- is there long-term research going down the line to use technology in a way to protect privacy? And is there currently available technology that could be used to help protect privacy in the shorter term? So,

I'm happy to talk about that, if you're interested in some further discussions. But, obviously, there's tension between the two, so we're always alert to those and trying to figure out how to -- how that comes up.

In terms of my duties, they are laid out in the statute, just as Hugo's are, and Dan Sutherland's, and the Department of Homeland Security. Mine are in the National Security Act. And it's in Section 103(d) or -- you know, codified at 50 U.S.C. 403(d). There are actually several different statutory duties. I think the ones that most stand out, at least for me -- and, I think, are of most interest to you -- are one and four.

My first duty is to ensure that the protection of civil liberties and privacy is appropriately incorporated in the policies and procedures developed for, and implemented by, the Office of the Director of National Intelligence and the elements of the intelligence community within the National Intelligence Program, which means, basically, I'm looking at the intelligence agencies and making sure their policies and procedures have adequate protections for privacy and civil liberties. So, that goes beyond the ODNI itself and looks at the intelligence community agencies as a whole.

The fourth duty is to ensure that the use of technologies sustain and do not erode privacy protections relating to the use, collection, and disclosure of personal information.

I like those two, not only because of their scope and breadth, but because I think they capture this technology and policy kind of a -- two perspectives that come up a lot in privacy and civil liberties contexts.

I think, recently, of course, the 9/11 Commission Recommendations Act was passed that added a whole additional layer of obligations and reporting requirements to privacy and civil liberties offices, Hugo's office and my office included in that.

As, you know, Charlie mentioned, you know, there are a whole bunch of different offices and oversight involved, as well. I just want to give you more of a flavor of that. I don't -- you know, I apologize if I'm repeating what you may have heard from others, in terms of what the intelligence community is all about. And Charlie mentioned a little bit about the Church and Pike Committee hearings, but I really want to emphasize that, because I think that's critical. And I don't know to what extent, Hugo, you've had prior discussions about that.

MR. TEUFEL: I mentioned we have copies of the Pike and Church and Rockefeller Commission –

MR. KROPF: Right.

MR. TEUFEL: -- hearings. And it's because of you, and it's very important to us as we do our oversight in the intelligence community.

MR. JOEL: Okay. Right. Well, I'll just go into a little bit of detail.

I mean, we do believe, as Charlie said, that that is part of the fabric of the intelligence community. As General Hayden said in one of his landmark speeches, it helps define who we are. We -- these rules that came out of that are codified in Executive Order 12333, which President Reagan signed. He -- they had previously been in an executive order by President Ford which was issued immediately after the Church Committee had held its hearings. They were then reissued by -- in an executive order by President Carter, and then it was President Reagan. And they're still in effect today.

And they're sometimes shorthanded by the term U.S. person rule, so you'll hear this phrase in the intelligence community a lot -- the U.S. person rules. And these are the rules, that each agency actually has, which are either the Executive Order 12333 rules or implementing procedures under Executive Order 12333 that the attorney general has to approve in conjunction with the head of each agency. And, typically, the rules date back to the 1980s. Each agency typically would put it in place soon after -- soon after President Reagan signed it. For example, DOD's rules date back to 1982 and are -- they're still operating under their 1982 set of rules.

So, these rules are quite restrictive. They affect -- obviously, you have to follow the Constitution. Everyone's bound by the Constitution, of course. You have to follow the statutes. And, even then, after you go through those checks, you then have to follow these particular sets of rules, how you collect, retain, and disseminate information about U.S. persons. And the whole point of these rules is to avoid the kinds of domestic-spying kinds of problems that resulted in the abuses of the mid-1970s which were disclosed by Church and Pike. And so, when I teach this with intelligence community agencies, we do go over some of those abuses and problems.

So, those are the rules. And, we do, of course, have Offices of General Counsel. One of the Church Committee findings was that Offices of General Counsels were too small and were cut out of the loop in some of those activities; so, they have to be beefed up.

We have Offices of Inspector General. And you can only -- you only need to take a look at what the Department of Justice's Inspector General has been, you know, investigating and disclosing, in terms of the FBI's use of National Security Letters, to see how independent and robust those Inspector Generals' offices are. I view them as a critical part of what I call the civil liberties protection infrastructure inside the intelligence community. They're a very important part of the executive branch oversight mechanisms, and I view them as an important piece of the overall structure.

And then, of course, we have other offices. There's my office -- I'm brand new, so, the intelligence community's agencies have to figure out, who am I? I'm neither fish nor fowl, so I'm not an inspector general, I'm not an Office of General Counsel. I'm a separate, independent office. When -- I'm sure when Hugo's office was created, and when Dan

Sutherland's office was created, DHS had to sort of figure out what those offices were. Those are, again, separate oversight and advice offices focusing on privacy/civil liberties. I think that's very important to have, somebody who's not in the Office of General Counsel, not in the Office of Inspector General, focused on, specifically, these issues. I think it plays a very important role. But it's a role that has to be carefully defined, structured, and explained.

And we've had additional developments. You know, FBI has created a separate unit within their Office of General Counsel, focused exclusively in privacy and civil liberties. They're also creating, or have created -- I have to verify exactly where that is -- a compliance unit, as well, that's independent of that. Other agencies are looking to create privacy and civil liberties offices. The new statute has required certain key departments and agencies to name privacy and civil liberties officers, of course, reporting directly to the heads of their agencies. Obviously, we have the Privacy and Civil Liberties Oversight Board for counterterrorism matters, and they're now an independent agency, so that's a new development. So, there's a whole infrastructure here. And not -- it's not my job to replace what these agencies have been doing, or -- in the past, in terms of complying with these U.S. person rules, but, rather, I view my job to work with and through them to identify what I call new pressure points on this infrastructure that have come up since 9/11. And so, not -- of course, I have to look at the infrastructure itself to make sure it's working properly, and it's not perfect. You know, nothing ever is. It's an incredibly complex organization. And, you know, no one is ever perfect. In a -- in an organization as complex as the intelligence community, which, let's remind ourselves, 16 separate elements, 15 of which are embedded in other departments. So, very complex organization structure. It's not going to work perfectly. So, we always have to look at that to see, you know, are things working well? What needs to be improved? And then we have to look at the new pressure points after 9/11, new threat environment, new data, new technology, new laws, new authorities, new mechanisms, like my office, you know, How do we all interrelate, how do we make sure that the rules, the institutions, the people, and the processes are all working in as optimal a way as we can?

How much time do I have? I'm probably going on too long.

MR. BEALES: Until 2:00.

MR. JOEL: Til 2:00.

MR. BEALES: But we would love to ask questions.

MR. JOEL: All right. So, I'll stop talking quickly.

Let me -- so, that's, generally, the overview -- let me go into, sort of -- I know you guys are -- this is sort of Fusion Center Day for you, right? So – all right – so, let me quickly get into the information -- I'll skip what else I had to say -- I'll just get quickly into

the information-sharing environment. I think you've already been told what the – that is. Right? So, you have a sense for the information-sharing environment, don't need me to go into that again. Right? Right. Okay.

So, you -- the privacy -- the guidelines that are required to protect privacy and civil liberties in the information-sharing environment, that's required by the IRTPA. So, there is a requirement for that.

What people don't often realize is that there's also an executive order to share terrorism information. I don't know if you are aware of that. But that's Executive Order 13888, which precedes the Information -- the IRTPA -- that also mandates the sharing of terrorism information. It also requires the protection of privacy and civil liberties in the sharing of terrorism information. So, I always make sure to key -- carry that with me wherever I go, as well as the IRTPA. I've got my props. Of course, we don't forget the Constitution, which I carry with me everywhere I go.

So, when you think about protecting privacy and civil liberties in the -- while you're sharing terrorism information, you get -- you get this classic issue of balance, right? So, how do you share at -- on the one -- or share, on the one hand, and protect privacy, on the other -- how do you do both, again? So, you're sharing, you're doing more on the national security side. What are the protections you're going to add? How are you going to do that? So, for me, the key is balance and how do you -- how do you add those protections?

I think what we did with the guidelines -- so, the guidelines were issued in response to the statutory requirement, as well as the executive order requirement, to protect privacy and civil liberties. They're available on www.isegov. There is explanations there on the process that we're -- that we're taking to – with these guidelines.

The guidelines, sort of, strike this balance by requiring agencies to follow uniform procedures to implement specific protections based on legal and policy requirements and privacy best practices customized to fit their own legal and mission requirements. And, basically, what it boils down to is, we quickly recognized there were going to be one- size-fits-all solutions, no silver-bullet answers. You can pick your -- pick your metaphor. And so, imagine this was your task. You've got to -- you've got to facilitate the sharing of terrorism information, because that's the mission of the information-sharing environment, to stop another 9/11, to allow agencies to connect the dots, and you have to protect privacy. You don't have the luxury of wiping the slate clean and starting over. Or maybe you do. Maybe you do. Okay? So, we've all watched 24, and we all see what Jack Bauer does. Let's set aside interrogations, because I don't want to go there, but let's just talk about access to information. And so, you watch Jack Bauer. And there have been some people who have made suggestions along these lines, including -- you could read -- there's a suggestion about going to an authorized-use standard that we are required to

report on, and you could read -- I don't think this was the intent, but you could read some of these suggestions, just to go along these lines. If you wipe the slate clean, and you can say, I'm Jack Bauer. I'm with the CTU. I have an authorized counterterrorism purpose. I'm in an audited environment. I get to see any information I want, as long as I'm in an audited environment, regardless of all the laws and rules and regulations out there. Okay? Jack Bauer, CTU, get to see anything I want in the information-sharing environment. That would be one way to do it. It would require an act of Congress, I would think. You'd have to get a statute that would say, notwithstanding any other law to the contrary, bam, bam, bam, bam. That would be option A.

In the time available, and in order to get through what we had, and, given all of the privacy and civil liberties implications I saw with that approach, which were significant, in my view, just -- let's just keep it at that.

Option B. Option B is to recognize there are a multiplicity of privacy policies and laws out there already. There's the Privacy Act, there's e-Gov, there's a -- there's at least -- we start counting -- at least 108, and then we stopped -- 108 separate agency-specific policies and laws and -- that apply to different types of rule -- data, different types of agencies, depending on what they're doing and how they're doing it, that protect privacy of different types of information.

Now, you may think that's sector-specific, it's inadequate, it's spotty. I actually think it's quite comprehensive. Be that as it may, it's the reality. Agencies are already sharing terrorism information. Of course they are. They're doing it in a way that's consistent with their authorities, with their mission requirements, and with the laws and policies as apply to them.

So, when you get into that situation, what you have to do is come up with guidelines that don't stop necessary sharing from occurring, but, instead, impose a regular process for those agencies to follow to enable that sharing to occur, but make sure that it occurs in an environment where they are putting in place the right processes and checks and balances, and making sure that they're putting in place the appropriate protections and safeguards for sharing the information in a consistent way that's consistent with privacy best practices, which is what the privacy guidelines were intended to do.

So, what we've done since then is created a guide to help the Federal agencies implement the privacy guidelines in greater detail. So, we've published that guide. It's up on www.ise.gov. It goes into greater detail to explain to agencies how to take the general guidance from the guidelines -- the general requirements of the guidelines -- and actually implement them into privacy protection policies at the agency level.

In terms of Fusion Centers, the privacy guidelines -- and I'm running out of time -- the privacy guidelines require agencies to work through the governance structure that we've set up, which is the Privacy Guidelines Committee -- which I co-chair, along with the Department of Justice, with very heavy involvement from the Department of Homeland Security -- to work with Fusion Centers, State and local and tribal representatives on making sure that they have privacy policies and protections in place that are at least as comprehensive as those that we're requiring of Federal agencies before we allow sharing to occur.

I'm sorry that I didn't manage my time better, and I want to leave time for you to ask questions.

MR. BEALES: All right. Well, I think we have time for a couple. And I -- we appreciate you being here.

John Sabo?

MR. SABO: Thanks very much.

There's a big -- just to be quick -- there's a big gulf between the tremendous concepts in the Constitution and operations on the ground. And -- for those of us -- I do some work in information sharing, so I work in the private sector, and I'm on this committee, and we look at a lot of the systems that are being built to implement the business processes that implement the regs that implement the laws that support the Constitution. And, at that business-system level, particularly with the information-sharing environment, we need to manage the information, manage the flows, manage the identity, access, controls authenticate the individuals. And you're doing this in a hugely distributed environment which never existed before. You're dealing with tribal, State, local, private sector, the intelligence community, and agencies. This has never existed before.

And what I'd like you to address is how you're seeing the government, whether it's DHS or DNI, put some thinking and structure into the baseline controls needed for security and the baseline controls needed for privacy.

One example, HSPD-12 -- I think it's 12 -- which deals with FIPS 201 -- which led NIST to write FIPS 201 specifically to address identity credentials for Federal employees and contractors, a whole Federal information-processing system manual on that. And yet, I don't see that type of structured approach to the security baseline controls and privacy controls for this information-sharing environment.

And if the work is going on, in that instance, I guess I'd be interested in knowing what that is. And, if not, do you have any views about, you know, its importance, or not, and who should be doing it?

MR. JOEL: Right. Well, it's going to depend on who is responsible for putting together those plans. And so, I'm not sure exactly who the bellybutton is on the project you're working on. But if you can give me that information --

MR. SABO: No, it's not -- it's a general question.

MR. JOEL: Okay.

MR. SABO: In other words, if -- we heard, earlier, about Homeland Security Information Network. That network is built already. Information is being shared with private sector, State, local, with Fusion Centers. Fusion Centers are being funded by the Federal Government. I'm not being accusatory. I just have limited time. I'm trying to, you know, get this in before the Chairman gavels me down. But what I'm trying to say to you is, who is -- who is responsible for leading this government wide effort to develop the types of security controls? They don't have to be granular, they don't have to be down to the specifics, but they do have to be broad enough so that you could go out to the Fusion Centers and say, this is your "baseline security model". --

MR. JOEL: Right.

MR. SABO: -- that you should demonstrate.

MR. JOEL: Well, at the program --

MR. SABO: So, who should do that?

MR. JOEL: -- managers -- it depends on -- I mean, because I'm not sure exactly -- it depends on -- if it's a program manager of the information-sharing- environment-led architecture planning effort, then I would look to the program manager's office to identify for me who the key players are, and then we would make sure that those guys are baking in the right kind of planning and privacy and security controls that you're talking about. If it's, for example, a DHS-led effort, then I would hope that they're doing their privacy impact assessments, et cetera, at DHS.

So, it's -- it's, unfortunately, an incredibly complex beast, and part of the issue is going to be just identifying who the person is in control of the particular project or planning effort, and then making sure that person is in touch with their privacy officer. So, our -- we have a Privacy Guidelines Committee that meets monthly, and their job -- they're the senior privacy officials for each agency -- their job is to make sure they're connected with the people in their agency who are participating in the ISC and doing all these things. And so -- it's not perfect – and so, sometimes the information flows within the Federal agencies aren't perfect. But, hopefully, by meeting regularly and making sure we're connected with the program manager's office and understand what the planning is going on, we can get the information shared. So, if you're aware of an effort, it would just help me to know what that effort is, just to make sure that I have -- I'm getting

information to the right people that -- to make sure we're all connecting in the right way. But that's the way the system should work.

MR. BEALES: Lance Hoffman?

MR. LANCE HOFFMAN: Thank you.

You mentioned, earlier, I think, at the beginning of your testimony -- I think you -- I heard you mentioning privacy research. And just now –

MR. JOEL: Yes.

MR. LANCE HOFFMAN: -- just now, you mentioned baking in things at the right time and so forth. We've had some testimony earlier, before this committee, about how research isn't really easily funded, it's almost radioactive -- privacy research, when you propose it. For example, in the Christian Science Monitor of February 9th, 2006, there was a interview with Latanya Sweeney, who testified a year earlier before this committee, and she talked about a request for proposal by ONR, on behalf of DHS, outlining data technology research, and meshed closely with the technology cited in the ADVISE documents at the time. That proposal didn't provide any funding for privacy technology or research. We've seen a litany, now, of ADVISE and CAPS-2 and TIA and a number of things come and go and bite the dust, more or less.

My question for you is, In your opinion, how can we better incentivize, in DHS -- and in the Federal Government, but especially in DHS -- long-term research into privacy so that we learn how to safeguard it better, building it in, rather than bolting it on later, and build it into new systems that are being proposed to DHS? How can we better -- do a better job of incentivizing privacy research?

MR. JOEL: Well, I wouldn't presume to advise DHS on that. I'll just say that, in the DNI, we have something called IARPA -- the Intelligence Advanced Research Projects -- Activity, I think -- anyway, it's a science and technology organization, and the folks involved in that have, so far, been very supportive of privacy protection technology research.

Now, I say "so far," because budget pressures are upon us, and who knows how the budget -- how the budget issues will shake out in the future. But, so far, they have been very supportive of privacy protection technology research. So, I'm crossing my fingers and hoping that they will continue to be, in the future.

But I think -- I think -- and I think that's very important, because I think you put a stake in the ground, and you say, "Hey, technology is really important for the future of national security, and privacy protection is part of that future, as well as everything else."

MR. BEALES: Dan Caprio?

MR. CAPRIO: Thank you. Secretary Allen, in his comments, mentioned the need for building trust and confidence and reaching out to that broader --

MR. KROPF: Oh, yeah. Trust, yeah.

MR. CAPRIO: And you mentioned your internal responsibilities or statutory duties to policies and procedures within DNI, and then ensuring the use of technology, that it doesn't erode privacy and civil liberties. So, what do you see as the -- I mean, both --on both sides, the opportunity and the challenges to external outreach?

MR. JOEL: Yeah, external outreach is a -- is, I think -- you know, just to go to the issue of trust, I mean, obviously, we -- that's a -- that's a major challenge these days. You can just look at the media and the newspapers. And we do try to engage in outreach. We do meet with the privacy and civil liberties advocacy groups. We meet with Members of Congress and staffers a lot, on a variety of issues. I make myself available for the media. And so, it's -- it's difficult.

I guess I would say -- I would say just a few things on that topic. One is, I am a firm believer in congressional oversight. I mean, I do think that when you're dealing with classified information, and you are not able to explain to the American people what is actually going on inside the walls because they are secret -- these things are secret, and we have to keep them secret in order to keep the country safe -- we have to rely on what I call agents of transparency. We have to rely on other means to provide proxies for transparency, to provide reassurance. And one of them is congressional oversight. And so, I'm a firm believer in that. And so, we try to provide transparency to the Congress. And that's what we're trying to do right now. And, you know, hopefully that will help in that -- in that area.

The Privacy and Civil Liberties Oversight Board is another mechanism. It's now going to be made independent. So, that's a transition period. But certainly we have worked very closely with the Privacy and Civil Liberties Oversight Board. We have given them access to a lot of information, they have seen a lot, and they are still -- we are still working very closely with them. They are fine individuals and have, you know, provided, I think, a lot of value, in terms of providing oversight and fulfilling their statutory duties. And so, we work through that channel, as well.

Then, the third thing is that we have pushed a -- hard -- and I think the intelligence community has come a long way toward explaining what it does in much more detail than it ever has in its history. And I think there are people inside the intelligence community that feel like that has put certain sources and methods at risk. But, on the other hand, you know, you, sort of, do the balancing, and people like me say, well, maybe some of these risks are worth taking for purposes of transparency and trust. So, we -- we're constantly having these discussions, and can we -- can we redefine the secret?

Can we -- can we draw the circle a little more tightly? Can we say more? Can we say more to reassure people? But there are concerns that the more we say, the more clearly we say it, the less we will have access to the particular source and method that is helping us produce intelligence for purposes of national security. So, it's constant challenge.

The other thing I'll say is that, not only is this not a unique time in history, because we've constantly faced this throughout our history, and we always think, like, ooh, this is the first time we ever had this issue. It's always been with -- if you study history, not -- our history, it's always been with us. And if you look around the world, despite what, you know, you might read, in terms of the newspapers, I mean, other countries face this exact oversight challenge. I'm getting the hook here.

VOICE: No, you're not.

MR. JOEL: Other countries face this same intelligence oversight challenge. We're not unique. Other countries have intelligence services. Other countries do things in a secret way. And other countries go through different levels of anguish about how to conduct intelligence oversight over classified activities. And so, we have -- I am very proud to be in our system of government. I mean, we have a very good system of government. It is not perfect. You know, I'm not saying that we do everything perfectly well. So -- but we do have a pretty good system.

MR. TEUFEL: Have you ever noticed how lawyers will talk to fill up the available amount of time? [Laughter.]

MR. JOEL: Yes. I, too -- I overstayed. Sorry –

MR. TEUFEL: I'm just saying that. I just -- I wanted to stop, to thank Alex for coming down to talk to you all. And John Kropf and I are going to be leaving, because we have a previously scheduled meeting that we've got to -- we've got to go to. But I wanted to thank Alex for coming.

And, also, I just wanted to acknowledge everybody who's here in the audience. Privacy matters – and it sometimes surprises us, in the Privacy Office, that don't get more of a turnout. So, those of you who are here, and you're not just staffers and representatives of the media, I want to thank you all for coming to our quarterly meeting here in D.C. And I hope the next time we have one in D.C., we see -- we see all of you, and more.

So, thank you, Alex. And my thanks to the committee. I'm going to be stepping out, here, for a meeting I've got elsewhere. So --

MR. BEALES: We'll miss you, Hugo. And thank you very much, Mr. Joel, for coming to join us.

This afternoon, we're going to hear about what I'm sure will be a somewhat different perspective on Fusion Centers in our -- in our afternoon panel. I think -- I think I want to do what we did this morning, and introduce the speakers in turn, and then hold the committee's questions til the end. I'd like to ask you to limit your remarks to 10 to 15 minutes so that -- so that there will be time for questions. And I just wanted to note, for those of you who are following the agenda, that Greg Nojeim, who's scheduled to be on this program, is ill today, and as – was unable to be here.

So, we will begin with Lillie Coney, who's the associate director of -- and the EPIC coordinator, of the National Committee for Voting Integrity, at the Electronic Privacy Information Center. She served on the Brennan Center Task Forces, on the Security and Usability of Voting Systems, and she is a member of a Committee on Guidelines for Implementation of Voter Registration Databases. She's also the coordinator for the Privacy Coalition, and she's served as a public policy coordinator for the Association of Computing Machinery, and as special assistant to Representative Sheila Jackson Lee on a variety of issues. She has over 20 years of experience working with a wide range of science and technology issues.

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

MS. CONEY: I would like thank the Data Privacy and Integrity Advisory Committee for inviting the Electronic Privacy Information Center to offer comments at today's meeting on Fusion Centers.

EPIC is a public-interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.

EPIC takes public positions only on matters of concern to consumers and as an advocate for civil liberty and privacy protection. Our panel presentation today is about the emergence of internet worked communication infrastructure that could facilitate the creation of a modern surveillance society. The name given to the criminal justice national security component of this endeavor are Information Fusion Centers.

Fusion Centers are an amalgamation of commercial and public-sector resources for the purpose of optimizing the collection, analysis, and sharing of information on individuals. To achieve this objective, underlying communication infrastructure must support access to identity data networks. Some believe that the right mix of technologies will enable the authentication of identification documents, facilitate checkpoints to screen for persons on watch lists, control border entries and exits, track purchases, use of credit, better coordinate activities or private and government entities, locate criminals, and predict crime before it happens.

Fusion Centers are being proposed as a means to bringing together information for distributed sources for the purpose of collection, retention, analysis, and dissemination. The term Fusion Center was first coined by the Department of Defense, and refers to the fusing of information for analysis purposes.

On November 9th, 2002, the New York Times disclosed a massive DOD Fusion Center project managed by the Defense Advanced Research Project Agency, known as Total Information Awareness. DARPA was developing a tracking system intended to detect terrorists through analyzing troves of information. The project called for the development of a revolutionary technology for ultra large, all-source information repositories, which would contain information from multiple sources to create a virtual centralized grand database. In September 2003, Congress eliminated funding for the controversial project and closed the Pentagon's Information Awareness Office, which had developed TIA.

Another Fusion Center initiative was the Multi-State Anti-Terrorism Information Exchange, also known as MATRIX. MATRIX was a prototype database run – system run by the State of Florida and Seisint, a private company. Built by a consortium of State law enforcement agencies, MATRIX proposed to combine public records and private-record data from multiple databases and data and analysis tools. The program collapsed when it was disclosed to the public, and States were pressured by residents to withdraw from the program. In March 2004, the MATRIX project was on its last gasp when the States of New York and Wisconsin withdrew their participation in the project.

The latest government Information Fusion Center initiative. In December 2004, the push for a national Fusion Center initiative received a boost when the Department of Justice-sponsored Global Infrastructure Standards Working Group published A Framework for Justice Information Sharing: Service- Oriented Architecture. In August 2005, the Global Justice Information Sharing Initiative of the Department of Justice published the Fusion Center Guidelines.

The guidelines stated, the principal role of Fusion Centers is to compile, analyze, and disseminate criminal terrorist information and intelligence and other information, including, but not limited to, threat, public safety, law enforcement, public health, social services, and public works, to support efforts to anticipate, identify, prevent, and/or monitor criminal terrorist activity. This criminal information and intelligence should be both strategic and tactical.

The Department of Homeland Security set out an objective to create, by 2008, a network of Fusion Centers that could facilitate data-sharing across jurisdictions and functions supported by multidisciplinary teams dispersed throughout a national network of information hives.

The process of turning this proposal into hardware and software moved forward. The frame -- A Framework for Justice Information Sharing: Service- Oriented Architecture reported that it was in the process of developing guidelines based on extendable markup language standards. This computer programming language provides users with a data-sharing capability that would not require the replacement or redesign of existing systems. This programming language allows the identification of fields of information through the use of a translation feature that accomplishes its task between systems being -- that contain information and those of the requestor.

In this process, the source of the data and the recipient do not need to change their computer networks to participate in the information-sharing network.

Fusion Center data sources. Appendix C of the Guidelines on Fusion Center Development -- detail lists of entities that -- which should be approached and included in the process of developing local/State Fusion Center efforts. The range of data sought by fusion centers include all sources of financial records, all contacts with the criminal justice system by criminal and noncriminals, all tribal, local, State, Federal, private, and university law enforcement records, U.S. postal inspectors, all forms of education, daycare, preschool, primary, secondary schools, colleges, and universities, and technical schools, government-issued licenses and permits, medical records, public health -- which include public health, ambulance, hospital, mental health clinics, and primary-care physicians, hospitality and lodging, gaming industry, telecommunications service providers, military and defense, industrial-based entities, U.S. Post Offices, postal and shipping services, private security, which would include alarm companies, armored- car companies, investment -- investigative firms, corporate security offices, private security companies, public works, social services, and transportation. One particularly interesting thing about social services, they listed welfare fraud as one of the areas that would be used or monitored by Fusion Centers.

Along with a host -- to restrict and control access to information -- along with a host of local, State, and Federal law enforcement agencies, private companies also participate in the public safety Fusion Center group that helped develop the guidelines. These companies included Walt Disney World Company, Fidelity Investment, Microsoft Corporation, and Archer Daniels Midland.

The goal is to, within the Fusion Center environment, integrate nontraditional customers of information and intelligence. The process would involve fusing of information based on an identified threat, criminal predicate, or public safety by the seamless collection, collating, blending, analyzing, disseminating, and use of information intelligence. The intelligence and analysis of information will be based on the needs of Fusion Center participants. The list of participants include all level of law enforcement,

national intelligence community, defense, and private-sector entities, making the applications of the data-mining project limitless.

The focus of Fusion Centers is on information collection as a means of determining crime trends with an eye toward predicting crime before it occurs. The four major desired outcomes for Fusion Center are: the reduction of the incident of crime, suppression of criminal activity, the regulation of noncriminal conduct, the provision of services.

There are questions about the focus on privacy and civil liberties considerations within the development of the Global Justice Information Sharing Initiative and Department of Homeland Security Fusion Center guidelines. The guidelines were published in the summer of 2005, but the Global Privacy and Information Quality Working Group issued its final report, "A Privacy Policy Development Guide and Implementation Templates," in October 2006. While the report lauded the importance of privacy protections from conception through implementation of Fusion Centers, it said that, about the building -- it said this about the building of a project team, "The project team should have access to subject-matter experts in areas of privacy law and technical system design and operation, as well as skilled writers, but these individuals do not necessarily have to be members of the team."

The Privacy Act of 1974, which is Public Law 93-579, was created in response to concerns about how the creation and use of computerized databases might impact individual privacy rights. If safeguards -- it safeguards privacy through creating four procedural and substantive rights in personal data. First, it requires government agencies to show an individual any record kept on him or her. Second, it requires agencies to follow certain principles, called fair information practices, when gathering, handling personal data. Third, it places restrictions on how agencies can share an individual's data with other people and agencies. Fourth, and finally, it lets individuals sue the government for violating its provisions.

The foundation of the Privacy Act are the elements of the Code of Fair Information Practices that are codified by that law. The Code of Fair Information Practices is cited three times in the Fusion Center Privacy Policy Development Guideline and Implementation Templates. But it doesn't define what those fair information practices are.

There are reasons to be troubled by the development of Fusion Centers without clear policy oversight mechanisms in place. For example, the Washington Post reported, on June 14th in 2007, that the Federal Bureau of Investigations conducted a self- audit of 10 percent of its records on National Security Letter use, and found 1,000 violations. The majority of the violations were associated with obtaining telephone records from telecommunications service providers. The FBI acted in the wake of criticism and – which – that resulted from an earlier Department of Justice Inspector General report that

determined the FBI abused the National Security Letter authority established by the Privacy Act -- by the Patriot Act.

There are no statutory definitions for "terrorism" or "terrorist organizations." This must be addressed. There must be a clear statutory definition of the word terrorism and terrorist, as well as the phrase terrorist organization, because, without clear definition, it's very difficult for an organization or an entity to narrow the scope and define its activity in this particular area.

A Law Enforcement Assistant and Partnership Strategy Report published by the minority staff of the 109th Congress Committee on Homeland Security provided the following account by Chief Ellen Hanson of the city of Lenexa, Kansas, on her attempts to train the maintenance staff of local apartments and places of hotel or hospitality and accommodation. Local efforts -- she's -- this account -- and I quote, "Local efforts to inform the public are an effective way to stay on top of information gathering of possible terrorist -- or gathering possible terrorist activity. Here in Lenexa, we have incorporated this element into our crime resistant community policing program. We conduct regular trainings with the maintenance and rental staff of apartment complexes, motels, and storage facilities. We show them how to spot and identify things like printed terrorist materials and propaganda, and unique weapons of mass destruction, like suicide bomb vests and briefcases. We build up a level of trust and familiarity that encourages them to pass on any suspicious information to our officers. They have confidence that the follow-up will be handled responsibly, and they also understand that they have an opportunity to play an important part in local efforts to prevent acts of terrorism."

According to reports, there are 43 current/planned Fusion Centers that are of -- that we are aware of at this time. Investigations conducted by the Congressional Research Service, ACLU, EPIC, and others, raise more questions than are answered about the real-world implications of the Department of Homeland Security's role in the development of intelligent Fusion Centers.

EPIC concluded that intelligence Fusion Center development and implementation is unfocused and undirected. The appropriate supervision, guidance, and oversight necessary to assure privacy, civil liberty, and civil rights protections are imperative. Information Fusion Centers present grave threats to privacy and civil liberties. There are too many unanswered questions regarding the creation, purpose, and use of Fusion Centers. Advocates working in the public's interest, academic researchers, legal scholars, attorneys, the courts, and journalists all play a role -- a vital role in checking the application of systems of surveillance to ensure that our freedoms and liberties are retained.

We make several recommendations. The Department of Homeland Security should fully disclose the location, jurisdiction served, and amount of Federal funding

provided to each intelligence Fusion Center operating within the United States. We've seen figures of $380 million in grants, but we need to know if that's accurate and if that's fully up to date.

Funding of intelligent Fusion Centers should be suspended until a full Federal privacy impact assessment is conducted on each one's operation, and the involvement of each Federal Government agency in the development and -- of Fusion Centers.

An IG investigation of information Fusion Centers should be launched to review their compliance with existing Federal laws intended to protect due process, privacy, civil liberty, and civil rights.

Federal reporting requirements should direct that each information Fusion Center make public the names of all Federal, State, local, and private partners.

Annual reports from each Fusion Center on the number of arrests, prosecutions, and convictions, by category of offense, which are directly related to the information Fusion Centers -- to the particular information Fusion Center's operation.

All information collected, analyzed, or shared must comply, at a minimum, with the Federal Privacy Act, and, where stronger State statute exists, the additional protections afforded must apply.

And, finally, accountability and oversight with the -- with administrative, criminal, and civil penalties should apply. Thank you.

MR. BEALES: Thank you very much, Ms. Coney. Our next speaker will be Sharon Bradford Franklin, who is the senior counsel of The Constitution Project. She works principally with the project's bipartisan Liberty and Security Committee, which seeks to protect America's civil liberties. From 2001 through 2005, she was the executive director of the Washington Council of Lawyers, which is a voluntary bar association to promote pro bono and public interest law. She spent 10 years as a civil rights lawyer in the Civil Rights Division of the Department of Justice and at the Federal Communications Commission.

Ms. Franklin, welcome, and we look forward to hearing from you.

MS. FRANKLIN: Thank you for inviting me here to speak today. The Constitution Project is an independent think tank that promotes and defends constitutional safeguards. We pull together bipartisan coalitions of leaders, and work with them to create consensus recommendations for policy reforms.

Unlike my colleagues here on this panel today, I will not discuss reforms for the operation of Fusion Centers, but ways in which the Department of Homeland Security can work with and through the Fusion Centers to promote policies that protect both our security and our civil liberties. Specifically, I want to speak to you today about our

recommendations regarding public video surveillance systems, and briefly, as well, about our recommendations for the use of terrorist watch lists. And, hopefully, you've all been given copies of our two reports on those subjects. Last March, I had the opportunity to speak on a panel at the first National Fusion Center Conference about The Constitution Project's guidelines for public video surveillance. I began my presentation to this audience, comprised of State and local law enforcement officials, by asking them raise their hands if they believed that video surveillance can be an effective law enforcement tool. Not surprisingly, most raised their hands.

Next, I briefly described the power of modern technology that might permit a system of networked cameras to track an individual around town and create a digital dossier of his or her daily life. But, because I noted that this was a fairly law-abiding crowd, I then asked how many wouldn't mind if their entire daily lives were captured on film for government officials to review. Not one person raised a hand.

Since this crowd likely had no criminal activity to hide, I had expected a substantial number to raise their hands, and I had planned to continue by noting some of the potential pitfalls involved. My next questions would have been to ask, "Think about whether you have, or maybe someone you know really well has, ever entered a psychiatrist's office or an Alcoholics Anonymous meeting or an infertility clinic or maybe the meeting of some nontraditional political or religious group. Now, you don't really need to raise your hands this time, but I want you to think again, how many are really comfortable having your entire daily life captured on video footage for government officials to view."

But I never got to those questions. I never had to point out to that law enforcement crowd that there are plenty of perfectly legal activities that most of us would prefer to keep private, even though we may need to enter public spaces to engage in those activities. They knew that the powerful technology of video surveillance cameras is subject to abuse, even by well-intentioned officers.

But this message is not getting through to political leaders in cities and towns across the country. In recent weeks, we have seen news coverage of new camera systems being installed or considered in communities ranging from Dallas, Texas, and Lansing, Michigan, to Vacaville, California, and Palm Beach, Florida. But few, if any, of these jurisdictions are adopting privacy policies, or even considering ways to minimize the impact of the cameras on residents' civil liberties.

The Constitution Project's Guidelines for Public Video Surveillance sets forth a series of practical recommendations to help protect our civil liberties and privacy rights in these situations. This report contains the bipartisan consensus recommendations of our project's Liberty and Security Committee, a group of experts from across the political spectrum. As our report notes, although existing studies raise serious questions about the

effectiveness of surveillance systems in preventing crime, there is some anecdotal evidence that such footage may be helpful in investigating and prosecuting criminal acts after the fact. Thus, if State and local officials decide to establish video surveillance systems, they can follow The Constitution Project's guidelines to minimize the intrusion on individual rights and establish systems that will only capture the footage that law enforcement officials really need for their law enforcement purposes.

Most importantly, we recommend that communities use publicly accountable procedures for establishing any public video surveillance system. When a community seeks to establish a permanent system of cameras, this process should include a full public comment period and a cost-benefit analysis to ensure that the surveillance system is designed to fit the community's law enforcement needs, its available staffing, and its budget. For specific emergency law enforcement investigations, a judicial approval process can provide this accountability instead.

Our guidelines also recommend a series of rules to regulate the use of the systems once they're up and running. For example, law enforcement should be required to obtain specific approval before using technologies that are even more intrusive on individual privacy rights, such as automatic identification or tracking of a given individual.

Our video surveillance report also includes model legislation to enable communities to easily enact these guidelines into law. With such rules in place, communities can ensure that any public surveillance cameras will only serve legitimate law enforcement purposes, so that law-abiding residents really will have nothing to fear from them.

The Department of Homeland Security is funding many of these video surveillance systems that are being installed across the country. We have been pleased that various people at Department of Homeland Security, and particularly some contacts in the Office of Intelligence and Analysis, have been receptive to The Constitution Project's guidance, have understood that technology is developing faster than the law in this area, and have helped us to distribute the report at various conferences. But the Grants and Contracts Division of DHS is still awarding money for surveillance systems, with no privacy requirements attached and no guidance provided.

We urge the Department of Homeland Security to require that, when a video surveillance system is established using a DHS grant, that the community must adopt the program through an open public process and establish a privacy policy, including requirements for minimizing the impact on residents' privacy rights and safeguards for data integrity. As an interim step, DHS could ensure that each community receiving a grant to fund video cameras was handed a copy of The Constitution Project's guidelines or provided with the Internet link to find the report online, and advise that this is a

helpful resource to enable the community to establish a system that will protect its residents' rights.

Also, many of the principles we discuss in our guidelines for public video surveillance, including prohibiting government agencies from doing an end run around privacy protections by simply obtaining private camera feeds or private data, have application, generally, to privacy issues facing Fusion Centers.

I also want to tell you briefly about The Constitution Project's recommendations for the use of terrorist watch lists. As outlined in our report, our bipartisan Liberty and Security Committee recommends that the use of such lists be strictly limited and that the government should adopt important reforms for situations in which such lists are used, to promote fairness and accuracy. Most importantly, we recommend that the government should adopt a set of standardized procedures to improve the accuracy of watch lists at the front end, at the time that names are actually added to the list, and before they are used. This includes setting clear written standards for when an individual's name may actually be added to a watch list.

DHS should work with Fusion Center staff, who use watch lists to improve the accuracy of these lists. Not only do watch-list errors burden travelers, but the extensive number of errors on such lists, as documented in a series of recent government reports, threatens the ability counterterrorism officials to focus resources on actual terrorist threats.

In both these areas, video surveillance and terrorist watch lists, DHS has an opportunity to work with and through Fusion Centers, not only to enhance our security, but also to protect our civil liberties.

Thank you.

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

Our third speaker today will be Michael German, who's policy counsel for the American Civil Liberties Union. He joined the ACLU in October of 2006, and he's a former 16-year veteran of the FBI, where he served as a special agent in domestic terrorism and bank fraud and public corruption investigations. In 2004, he resigned from the FBI and formed Hotei Consulting, where he urged Congress to adopt better intelligence policies in the wake of 9/11.

Mr. German, welcome. We look forward to hearing from you.

MR. GERMAN: Thank you very much. Thanks for inviting me and my colleagues working on these issues.

The timing of this meeting actually was very good, because the ACLU has been preparing a report on Fusion Centers to explain what's wrong with Fusion Centers from

our perspective. It's very good timing, but not great timing, because the report's not done yet -- [Laughter.]

MR. GERMAN: -- so I couldn't unroll it at this meeting, unfortunately. But it should be out in a few weeks, and I'll make sure you all get it.

And one of the primary problems that we found with Fusion Centers was that there has not been enough public discussion of what these Fusion Centers are intended to do and what they are doing. And that's why I applaud the committee for having an open hearing, because this is the type of discussion that we need to have, because these things are already being created.

Rather than go through everything we found wrong in our 40-page report, I want to leave some suspense out there so you'll be interested in reading it. And let me just focus on one area that we have some concerns, and that is who's participating in these Fusion Centers, and what their participation actually means.

The first level of participants appear, from our research, to be multi-jurisdictional law enforcement agencies. And, you know, obviously, if you look at the 9/11 Commission recommendations -- and I think we would all hope that law enforcement would work cooperatively together across jurisdictions and across levels in their ability to share information -- appropriately and legally acquired information with other law enforcement agencies -- should be applauded.

The problem that we find with the Fusion Centers- and some of your questions that I've heard today actually have been very good, trying to nail this down, although I don't think you really got an adequate answer, is who's really in charge of these entities -- and, you know, whether it's the Federal Government who's providing the funds and some of the manpower, the State governments that are nominally in charge of them, or the localities that also participate, because, of course, the accountability depends on whose rules are being applied and offers the opportunity for what I call, in the report, policy shopping, in which these law enforcement agencies would use the least restrictive agencies' policies in obtaining information and analyzing information, and the most restrictive policies, in terms of prohibiting public or congressional oversight.

And if you think that perhaps that's just the paranoid rantings of civil libertarians, I'd like to just read you a portion of a magazine article that I found that discussed a trade conference, called the MetaCarta Public Sector User Group Meeting that was held here in Virginia in May. A -- an intelligence analyst from the North Central Texas Fusion Center spoke. The center focuses on prevention and early warnings for the region. It gets involved with issues related to gangs, crime, and border security in connection with local and Federal authorities. Perfectly acceptable. Of particular interest to many at the meeting was the way the center accesses and uses data from local agencies. It does not

host the data, but, rather, refreshes them regularly. That means analysts are not subject to the Freedom of Information Act or being dragged into court. The analyst described the center as a sort of Wild West for analysts, in that they can use a variety of technologies before politics catches up and limits their options.

That, of course, is our -- the civil libertarian's nightmare, that, you know, we're building an infrastructure that design -- that is designed to prevent accountability. And that's why it's so important that the work that you do, both in getting that knowledge out to the public, but also in compelling the government to create guidelines so that we know what these institutions are doing, is very -- is appropriate.

The second level of participants are non-law- enforcement entities, both in the public sector and the private sector. And our concern with their participation in what is essentially law enforcement function is the breakdown of the arm's-length relationship between these non-law-enforcement agencies and the law enforcement agencies who are ultimately responsible for the security of their community. And, you know, what I've learned from my own experience in law enforcement, but also what's documented in the Inspector General report on the FBI's misuse of its National Security Letter authority, is that when that arm's-length relationship is broken down, and personal relationships are allowed to develop, the legal protections fall to the wayside. And if you look at the IG report, they find that the FBI supervisors and headquarters had developed relationships with the subpoena compliance authorities at the telecommunications companies which allowed them to forego the process of actually securing legal process, either National Security Letters or grand jury subpoenas, and, instead, just simply write a letter, saying, "Hey, we'll get you one later," and still obtain the documents. And, of course, what the IG found was, those -- that legal process never actually happened, and the FBI was getting documents illegally.

That occurred, not just with the telecommunication companies, which, believe it or not, were actually contracted to do that, but also with the Federal Reserve Bank, where the FBI was getting financial records of individuals by this breakdown of the system, without any legal process.

I also have a concern, the ACLU has a concern, with the private-sector participation, not just in what information they could give to the government and -- with this breakdown of the arm's- length relationship, but what information they're receiving from these Fusion Centers, as well. There are a number of Fusion Centers that already have private-sector participation, and obviously there are some legal issues regarding what information they're allowed to see. But, without knowing who it -- what authorities are in charge, you don't know who is policing that. And you can imagine- for example, Boeing is supposed to have an analyst inside the Washington State Fusion Center. Now, Boeing is obviously a defense contractor. And if they have access to the security

vulnerabilities of everyone -- every entity in their State, you could imagine that they can make a lot of money by putting contracts together, not to mention that, if their competitors are providing this information, that they would have the ability to really use their access to the Fusion Center information inappropriately.

And, finally, the third participant that we're concerned about in the Fusion Centers is the military. And military personnel, both National Guard and Active Duty U.S. Army personnel, are involved in some of these Fusion Centers. And, of course, having the military involved in domestic law enforcement is a big problem. And, you know, one of the hallmarks of our liberty is that we don't allow that. And, while it might be nice to say that those entities are only involved in force-protection issues, if there's a critical incident happening, and everybody's running around trying to solve the problem, I doubt very seriously that somebody would be willing to sit on their hands and do nothing to support that effort. But that's why strict guidelines have to be put in place, so we know what the rules are and who's responsible for making sure that they're followed.

I think it's -- one of the things that's very important -- the -- when Secretary Allen talked about the idea that in the -- you know, that the threat isn't going away and that we're just going to have to get used to this sort of a surveillance society -- I don't believe that the surveillance society is inevitable. We would have to build it. But, unfortunately, we are building it, and the Fusion Centers are part of it, without enough discussion and evaluation of whether these techniques actually work. We've talked about the video surveillance, for example, you know, and Secretary Allen mentioned the ring of steel, the thousands of cameras that surround London. But what you have to remember is, that ring of steel did not prevent four suicide bombers from placing backpacks on their back, walking into a subway and blowing it up. Likewise, it didn't prevent four more people, using the exact same source and method, doing it again 2 weeks later, nor did it prevent this latest series of attempted car bombings that only failed because they were bad bomb makers, not because there was -- the surveillance system works. And if we're investing all of this money in these programs, we should first determine whether they work; because, once they're built, it's going to be hard to get rid of them.

And the final thing that's important to mention is why these Fusion Centers came about, in the first place. You know, the Federal Government had a mechanism for sharing antiterrorist, counterterrorist information with State and local entities, and that was the Joint Terrorism Task Forces. But what the State and local authorities found was that it was inadequate because of the classification rules regarding that intelligence. And they said that they -- because of this need to know structure that was built in, in government -- Federal Government classification rules, they weren't getting the information that they felt they needed, so they created their own information- sharing networks, which became these Fusion Centers.

But if you read the recent Congressional Research Service report on Fusion Centers, towards the back of the report it talks about what's not going right with the Fusion Centers. And what the participants say is, they're still having problems, because the Federal Government has not changed its classification rules. And the information, even though they're getting clearances to receive it, can't be shared back with their officers on the street and with the other stakeholders. So, the problem hasn't changed. Fusion Centers aren't fixing that problem. And if you really want to address what the problem with the information sharing is, that's what you have to address, not creating these new systems.

So, with that, I'll leave the -- and hopefully get you a report in the next couple of weeks.

So, thank you very much.

MR. BEALES: Well, thank you for being here, and we'll look forward to the report when it -- when it is available. And we'll read it with interest.

Tom Boyd?

MR. BOYD: Thank you, Howard.

The question I guess -- I have a couple of 'em, actually -- my first question is -- Ms. Coney -- the creation of Fusion Centers is extraordinarily important, and it also raises, as you have pointed out in your statement, both orally and in writing, a lot of very important questions. Page 9 of your statement lists a series of concerns. Speaking for me, personally, though, I think it's counterproductive, when EPIC documents characterize a Fusion Center as, quote, Federal Government efforts to establish operational domestic surveillance programs, close quote. Now, is that -- those are politically combustible words -- is that a characterization you embrace? And, if so, can you tell us some information that supports that characterization?

MS. CONEY: 380 million Federal dollars supports that statement. The Department of Homeland Security is providing grants in the establishment and furtherance of the development of Fusion Centers. The – Global wrote initiative – the initiating documents for the development of Fusion Centers, the guidelines documents that accompany that, along with the architectural recommendations for the building of Fusion Centers, the architectural component. Global is an advisory arm for the Department of Justice. These are not strictly local efforts that are developing the guidelines.

MR. BOYD: No, I understand that, and I --

MS. CONEY: Right.

MR. BOYD: -- and I'm -- I don't think who's funding them is at issue.

MS. CONEY: Okay --

MR. BOYD: My question is, Is it a domestic surveillance program, yes or no?

MS. CONEY: Oh, absolutely.

MR. BOYD: And, if so --

MS. CONEY: Absolutely.

MR. BOYD: -- what is your proof?

MS. CONEY: It is absolutely a domestic program –

MR. BOYD: And what is your –

MS. CONEY: -- focusing on surveillance.

MR. BOYD: -- what is your support for that?

MS. CONEY: They're developed and being initiated within the continental United States. These are not outside the United States --

MR. BOYD: I understand that, but --

MS. CONEY: -- the targets are not outside the United States. They're focused on activities -- not just focused on terrorism, but on criminal activities and even outlining they want to be able to do predictive work regarding criminal activities.

MR. BOYD: But you used the phrase national surveillance -- a domestic surveillance --

MS. CONEY: Exactly, because --

MR. BOYD: -- programs.

MS. CONEY: -- the way the architecture is designed -- you can be in a Fusion Center in Kentucky, but you want to be able to access information in one that's in Los Angeles. The interconnected nature of the Fusion Center development and rollout makes this a national surveillance project. Now, how private -- and this is the other component that's really making this raised to the level of what we're talking about when we say domestic surveillance -- bringing in private- sector entities -- hotels, financial service providers, telecommunication providers, every description of an educational entity, from kindergarten all the up to trade schools and professional education programs, hotel/motel accommodation service providers, gaming industry, licensing -- whether it's driver's license to professional permits -- every aspect of our lives you can possibly imagine is outlined in the Fusion Center development process. I think it's hard to argue for it not to be a domestic surveillance program.

MR. BEALES: Can I just jump in here for a minute? Because I was going -- was going to ask this question at a later point. But, I mean, it seems to me like there's a -- there's a -- there's a labeling issue here, because I can -- I can see the sense in which you think of Total Information Awareness as a Fusion Center. But it is a radically different kind of program, or usage of the term, than what we heard about this morning.

MS. CONEY: What I think is --

MR. BEALES: Now, is --

MS. CONEY: -- interesting –

MR. BEALES: Are -- do you think -- do you think what we heard about this morning is not typical of Fusion Centers as they actually are operating, or are you worried about a potential that -- you know, for a different kind of a use that's more expansive?

MS. CONEY: What I -- what I've done -- if you look -- EPIC.org/privacy/fusion -- it lays out the progression of events and activities leading up to the discussion we're having today. This is not just a policy discussion. Total Information Awareness was initially talked about in a broad scheme. How do we actually make this work, pulling in information from all these sources into one grand database, or something like that, to be able to search and look for information? In the development of Fusion Centers, we're not only talking about policy wish-list kind of things, we're talking about develop -- they've already laid out the architecture, the software of choice, whether you -- and laid out two different models. You can either have a centralized database similar to the discussion of Total Information Awareness, or you can have a decentralized process, where the information is pooled -- all the databases are not pooled into one centralized source for searching, you actually send queries out from one point to several different points of systems that are participating in the Fusion Center process. Whether you pull it into one grand database or you're able to search multiple databases simultaneously, whether they're restricted to your jurisdiction or all the jurisdictions that are connected -- interconnected because they're using the same software programming language to facilitate searching of their databases, the effect is still the same.

MR. GERMAN: Can I address that, too? Again, just to make sure that we realize that this is not the rantings of paranoid civil libertarians, let me quote Secretary Chertoff. This comes from the CRS report that I talk about in my report. Fusion Center supporters argue that the Federal Government can use 800,000-plus law enforcement officers working across the country as their eyes and ears of an extended national security community. The CRS report quotes Homeland Security Director Michael Chertoff as saying, 'What we -- what we want to do is not create a single Fusion Center, but a network of centers across the country.' Yet the report makes clear that Chertoff was,

quote, 'cautious to stipulate that he views these centers as entities of the State and local governments that establish them, and not the -- and that the Federal Government had no intention of controlling them,' which is the -- it goes right to that point of who's in charge of these things.

Many of these Fusion Centers are in FBI or other Federal agency workspace. They're staffed by DHS and FBI personnel and analysts, and financed with FBI -- or Federal Government money. To say that they are State governments just so they can avoid the Freedom of Information Act is inappropriate, and it's -- and it's not the reality. The reality is, the Federal Government is what's creating these things. And if we don't put rules over what they're doing, they will be able to circumvent accountability.

You know, I -- there's been a lot of discussion today about establishing a trust relationship. The Constitution does not talk about a trust relationship. The whole purpose of the Constitution is that the founders realized they could not trust a government -- any government, not just this government. And that's why they built in the protections that force transparency. And the problem with this program, as with all intelligence programs, is that there is no transparency, and that's what needs to be resolved.

MR. BEALES: It -- I mean, I appreciate -- I appreciate that. But it seems like there's, sort of, two very different things, with different implications. And the control issues may be very much the same. But querying a database -- a bunch of databases -- requires that you be asking about something -- or someone, more often -- more commonly, as opposed to TIA that was, you know, "Let's merge all this data, let's mine all this data, let's use that data to pick targets," as opposed to, "Let's use that data to find somebody that we know we want."

MS. CONEY: But –

MR. BEALES: What we heard this morning was the "find somebody we know we want." And I recognize that one can slide into the other, and that's a danger that we certainly need to worry about appropriate safeguards for, but that -- are we on the same page with what's happening, or no?

MS. CONEY: Well, there are a couple of things. I think it's very unique that this particular information Fusion Center process will not only have law enforcement involved -- we're talking about law - local and State law enforcement account -- across the United States -- Federal law enforcement agencies, and national intelligence agencies querying the system in some means -- by some means of method. But you're also going to have private-sector partners. And there are discussions within the development guidelines talking about -- one, they recognize the money that's coming from the Federal Government is probably -- may be one shot, so you've got to figure out how to stay in

business. So, it has to have some functional purpose, a benefit for those participating in the process. Now, you may have law enforcement who -- specifically looking for information on an individual for a reason, but then, what about the private-sector partners? What information will they be seeking, and how will they like to use that information, where it would benefit them? It may be everyone who checks into the Hilton, you know, or everyone making a reservation to take a cruise on a particular cruise line, or it may be someone trying -- who might be potential customers for a particular product or service. So, when we say this is -- this is going to be a totally different process. And I was saying it's parallel to TIA, I'm saying this is a lot bigger and a lot farther down the road than the discussions that were initiated because of TIA and MATRIX. And the effort that's going into trying to figure out how to keep this thing going and how to make sure it's beneficial to participants, so that not only are we dealing with a trust issue, but the benefit issue, and the benefits and -- to private sector are going to be very different than those law enforcement or -- and very different, again, from those in -- amongst the other partners, which is national security, so that the use is -- if you don't have strict guidelines, if you're not creating oversight, it opens up the door to a lot of different things that we may not even anticipate, and definitely weren't discuss, because we've had no private-sector partners at the table to find out what benefits they're going to see coming from the process.

MR. GERMAN: And answering your question, as well, let me quote out of the DOJ guidelines, where they state the purpose of the Fusion Center is, quote, "to build professional relationships across every level and discipline of government and private sector by ensuring that intelligence and other information, including threat assessment, public safety, law enforcement, public health, social service, and public works, is shared throughout and among the relevant communities." That's the stated purpose. Not security, not antiterrorism, it's this wide-ranging share -- and if the Fusion Center personnel don't have a database themselves, like the analyst in North Texas was talking about, but has access to all of your databases at any time he chooses to turn the switch on, what's the real difference, as far as the privacy and civil liberties of the people whose data he's looking at?

MR. HARPER: If I could jump in on this, with the Chairman and Tom's agreement, I was interested by your question earlier and your question just now, for a reason that might be quite boring compared to the very good discussion that you've just created.

I think there are two senses of the term "surveillance." And you may be talking past each other. And certainly this morning when you asked the question of Director Riegle, I think, about surveillance, he took it to mean wire-tapping and snooping and secret stuff. And a lot of people think that surveillance means that. But I think -- and I think the sense in which -- in which EPIC and our panelists are talking about surveillance

is, you know, as a translation of the French, "watching over." And that's not necessarily secret. We -- surveillance happens a lot. We want surveillance to happen in some cases. I always come across a regulation from the Commodity Futures Trading Commission about surveillance of the futures markets. I'm not against that.

And so -- and so, in my estimation, I think -- I think EPIC's characterization of this as a surveillance system is accurate and provocative. It's okay to be accurately provocative. So, that's my opinion on the use of the phrase, which you, I think, rightly brought up.

MR. BOYD: Let me briefly respond. I don't disagree with your point. But perception is reality. And if we're in the process of discussing the merits and demerits of a Fusion -- fusion systems throughout the country, we all recognize the need to have some sort of sharing environment, because we failed to have that, 9/11. And it -- and suffered dramatically as a result of it. But if the common perception and the characterization here of operational domestic surveillance program differs, I think -- I would suggest, from what you've just described, Jim. And I think that certainly would be the public perception of that phrase. And if we use it, we had -- ought to be accurate about it. Certainly, there are many opportunities and threats that you generally raised that we need to be sensitive to, but one does not beget the other.

MS. CONEY: Well, I think this is very important, because when you raise something to the level of public discussion, it allows for the fleshing out of these particular points. From a national security perspective, there's probably a very different definition of what surveillance is. There's a different perspective and definition for someone who is a law enforcement officer. And then, of course, those who do privacy and civil liberties work, surveillance, to us -- we have a totally different idea about what that is. But having a discussion, where we're exchanging those views and those understandings, allow us to scope out where our differences are, where our conflict points are, and working towards a process where the issues are being addressed, like if -- Are we going to have oversight? Are we going to have transparency? Are we going to have auditing? Are we going to have accountability? Who's in charge? Why and how are those components going to be enforced? Do we have to have statutory laws? Do we have to have guidance from agency -- from agencies on this? Is it something that needs to be codified or oversight provided through -- you know, all of those steps and processes happen in the public discourse on particular issues. This is a very important one, and we're very grateful for the opportunity to have the -- this committee look at this issue. And you've asked excellent questions, very interesting ones, especially from our perspective, that, from the civil liberty and privacy perspective, we see the world through the different-shade glasses, I guess you could say, and it's important for us to have these conversations. Because I know we're talking about two different things -- or three

different things, depending on who you're talking about. If you're law enforcement or surveillance, sitting outside, watching someone, or tapping a phone. If you're national security, what's surveillance? Their definition is different. But with civil liberty and privacy advocates, when we say surveillance, we're talking about the things you see outlined in the testimony that I've given you.

Thank you.

MS. FRANKLIN: May I just briefly add one more point? I don't think any of us sitting here -- and they'll correct me if I'm overstating their views -- would say the government shouldn't be in the business of doing surveillance. We're just saying we need the appropriate oversight mechanisms and transparency and rules laying out when it's appropriate and who is appropriate to surveil. No one is saying, Don't do surveillance.

MR. GERMAN: And I would just add one thing that I always try to add whenever this is brought up. You mentioned the 9/11 findings that information sharing contributed to the problem. It wasn't information sharing. They identified ten operational failings. Every single one was caused, not by culture, not by a lack of imagination, but by classification rules and the bureaucratic rules that developed around those classification rules. The classification rules are what the problem is, not anything else. And that's the problem that is trying to be solved by this. But that's really where we need to push for reform, is in the classification rules, not in creating new mechanisms that are only impacting our liberties and privacy, and not contributing to our security.

MR. BEALES: David Hoffman?

MR. DAVID HOFFMAN: I just want to clarify something. This committee has adopted two papers, already, on additional controls that we recommend when the Department of Homeland Security is using commercial data for different purposes. And so, I'm particularly interested in the concept of the Fusion Centers having data feeds from private sources. I may have misunderstood, this morning, but I thought it was very clearly said this morning that those private-sector feeds would not exist, and the data feeds were all coming from local and State and Federal law enforcement authorities. So, I'm just wondering -- and I'm looking through this, and I see a couple of different distinctions, and I want to get them straight. One is, yes, there might be private-sector organizations participating, but they might be participating to get access, not to submit data. And then, I also see a distinction that the scope might include the possibility that private-sector data could be used, but it may not be happening yet. And so, I wanted to say - all of that to say, if there is evidence that private-sector data is being used now, I think that would be something this committee would be particularly interested in, if you could supply us with it.

MS. CONEY: That's the real -- one of the reasons, when we talk about transparency, that presents a real challenge in this. You have nondisclosure agreements. You do know that -- we do know that there are private-sector participation, at what level, and in what context. We don't have that information. But we know that there are private-sector entities participating, because, in the guidelines themselves, they mention private-sector companies, they also direct local fusion and State fusion developers to do outreach to private-sector -- in order to pull in information. And it could be tactical or it could be strategic. Like, you may want to know if there are -- certain thing about a product that's being made that may indicate a vulnerability, if someone wanted to try to execute some kind of terrorist attack, maybe something out, and you -- you see this on the -- that this is a potential threat. You could go to the industry person, because you have that contact information, and say, "Is this plausible? Is this possible? Can that really happen?" And they can tell you, yes or no, and, sort of, help you figure out whether it's a real threat or not.

Then there's another aspect of that, where they may be looking for a particular person. Now, there was a situation recounted where someone was accused -- this morning -- someone was accused of killing their wife, and the person -- the only thing they had was a telephone number. So, with the phone number, they were able to locate the -- it was a pay- phone booth outside of a hotel in Kentucky. Now, with the Fusion Center possibility of action, could they have called their contact at that hotel chain and say, "Could you check to see if this person is registered at the hotel?" In this particular instance, they contacted the local Fusion Center person, and they facilitated and arrested the person within 45 minutes. But the option would have been -- because there is no –

MR. DAVID HOFFMAN: I just –

MS. CONEY: -- definition of –

MR. DAVID HOFFMAN: I just want to be –

MS. CONEY: -- how information is used.

MR. DAVID HOFFMAN: I just want to be real clear with my question. Do you have any evidence that private-sector data is being used as a data source for the Fusion Centers, currently?

MR. GERMAN: Yes. Richard Hovel, the senior aviation and homeland security advisor to the Boeing Company, a private company which has an analyst assigned to the Seattle Washington Fusion Center, testified, in May of 2007 before the House Homeland Security Committee, quote, The private -- the private sector, quote, has the ability to effectively acquire, interpret, analyze, and disseminate intelligence information which may originate in the private sector.

In the wake of the influx of evacuees from Hurricane Katrina, the Texas Department of Homeland Security contracted with Northrop Grumman Corporation for a $1.4-million database project that, according to a newspaper article, quote, "would group traffic law enforcement information, Department of Public Safety, criminal law enforcement reporting, the Texas Ranger database, consumer records amassed by ChoicePoint," together.

So, this is what's being reported. That's -- unfortunately, I can't walk into the Fusion Centers and tell you what they have access to. And that's a problem.

MR. DAVID HOFFMAN: Thank you.

MR. BEALES: Lance Hoffman?

MR. LANCE HOFFMAN: I want to thank all the panelists. This has been a very informative discussion. I'm getting more concerned about these Fusion Centers, the more I hear about them, especially because I'm concerned that we may be unwittingly creating or enabling an unregulated system of marketing in data, especially when the magic -- certain magic words come up, like "ChoicePoint" and things like that.

In a Web 2.0 world, suppose that some non-DHS private entity -- let's say it's an investigative agency or a reporting agency or some unregulated person, or even some guy in a dorm room with the next MySpace -- okay? -- sets up his or her own private Fusion Center, the MySpace of Fusion Centers. Okay?

I have the same problem with this, that Chairman Beales was alluding to, the semantic question. Do we need something like a -- an accredited Fusion Center -- if we even have defined what a Fusion Center is -- because, otherwise, what if this goes private? You don't need any DHS money. Or DHS money runs out, as somebody testified, then what happens? Any -- you've- all have testified to this, so you may need -- may not want to respond any further. If you do, fine. I see my light on. If not, I just wanted to say, I'm horrified by that thought.

MS. CONEY: There were some discussions -- it was very interesting, because, in the guidelines, they basically say there's no guarantee you're going to get any more money from the initial funds you get from DHS or other government agencies, so you have to figure out how to make your Fusion Center break even, I guess. I wouldn't way to say "become profitable." But the -- look for how to make it beneficial, so beneficial and attractive to participants that they will fund it, so the commercial and -- you know, aspect of having private-sector entities -- of companies engaged in this process does raise some questions about how this might all evolve.

MR. GERMAN: And one of the things I -- I think that's a very good thing to be worried about, because there already has been this mission creep, where the justification for creating these things was antiterrorism, and it's moved to all-crimes, and then all-

hazards, and some people even say to prevent disorder. But, speaking of why that happens, the Congressional Research Service reported that leadership in some Fusion Centers have admitted that they switched to the all-hazards approach because, quote -- this is quoting the unnamed Fusion Center leadership -- "It was impossible to create buy-in amongst local law enforcement agencies and other public sectors if Fusion Centers were solely focused on counterterrorism, as the Centers' partners didn't feel threatened by terrorism, nor did they think their community would produce would- be terrorists." So, when there's a lack of mission, and the Federal Government is throwing all this money at 'em, they're going to create something. And what that something might end up, we don't know, unless there are very strong guidelines.

MR. BEALES: John Sabo?

MR. SABO: Thank you. You know, in looking through The Constitution Project report, I was really struck by its constructiveness. In other words, the report didn't really bash anything; it talked about -- this is the report on watch lists, because we had done some work on screening systems and watch lists and so on, and -- but what you talk about, when -- your views about when watch lists are appropriate, so you set that baseline, and then you talked about areas where you felt watch lists may not be appropriate, and then recommended reforms to watch lists. So, it was a -- it was a constructive document. And I think -- in picking up what Tom started; and Howard, a little bit -- I think that's missing, a lot, in the dialogue. It is great -- I think it is important for people to wave the banner and look into the future and see the potential perils that come from unchecked, unregulated, uncontrolled, and unmanaged interconnected systems. There's no doubt about that. You -- but, on the other hand, there are valid reasons for Fusion Centers. They've been documented, they're very clear, 9/11 recommendations, et cetera. So, the question I guess I have for you is, yeah, I mean, it's fine to look forward and see the perils to our liberties and so on, which could very well be real, but, as a matter of reality, the Fusion Centers are being funded, the networks are being established, actually are in place. Public/private sector, State, local, and tribal communities are now plugging in.

So, I guess I'd ask each of you, from your organizational perspective -- and we haven't seen the ACLU report -- how would you view a more constructive- or a constructive to this issue? Would you categorize the types of activities that Fusion Centers do, and which different sets of policies and controls would apply? Would you expect the government, which is funding the Fusion Centers, to establish policies that would be applicable across them? Would you look for some audit capability? I guess it's an open-ended question to see -- what would you suggest we do about it -- that's very constructive, something this panel could take a look at as we look at Fusion Centers -- this committee and our subcommittee work -- that would move us to reality. And reality

is, they're being -- they're now operational. And my understanding, from other sources -- DHS sources -- was that the plan -- this is to fund up to 70 of these, not 43. And that's a huge number of Fusion Centers. In some States, there are multiple Fusion Centers, because you have a large population, or, like New York City, and then you have the State of New York.

One other thing I'd throw -- so, I'll -- that's my question. What -- do you have constructive approaches that, in addition to showing us the long- term peril, you would advise can be done to help us mitigate some of these concerns, tactically?

MS. FRANKLIN: Thanks. I'm going to go first, since you referenced The Constitution Project's watch list report. And thank you for your kind words about that report.

That is The Constitution Project's, hopefully, general approach. We do try and reach consensus with working groups of leaders from across the political spectrum. And -- so that hopefully our recommendations will have resonance and be practical and, hopefully, capable of implementation.

And I would agree with you that these are a reality, and that the productive way to move forward is to try and set up systems of checks and balances, and transparency procedures, to try and make sure that we are protecting our civil liberties and privacy simultaneously, and not losing track of that.

And we don't have -- I think my colleagues here probably have more specific guidance on Fusion Center, per se, but the principles that we reference here, in terms of not allowing sidestepping by just obtaining private data and doing an end run -- once that data comes into the government's possession, it should be subject to the same safeguards of having audits, of having proper training on procedures, that those can apply across the board, and that it is very important to -- now is when you're setting up the Fusion Centers -- to act now to get these systems in place, because it's much harder to rein them in after the fact.

MR. GERMAN: One of the things that I was very heartened by in starting this -- we actually reached out to every Fusion Center. Some were more cooperative than others. But many that we talked to were very happy to discuss this, and actually felt that the Federal Government -- in particular, the DOJ guidelines -- were sort of being forced down their throats, and they felt that they did not want to go down the roads that we caution against, that they did not want private-sector participation, because they felt that their law enforcement information would be susceptible to misuse, that they did not want unregulated collection of information by these different entities. And what I kept hearing over and over again is the rules that they think are very effective, which is 28 C.F.R., Part 23. And if we pay attention to that -- you know, the structure's already in place. Law

enforcement should only collect information, and retain information, when there is a reasonable indication of criminality. It's that simple. Some of the law enforcement officers we spoke with talked about concerns about sharing information with DHS, because DHS hires so many contractors that they felt if they're not sworn officers, "Are we really secure and really following the law by sharing information with private contractors?" So, I'm heartened that the State and local law enforcement officers have a better grasp of what the rules should be than a lot of the material -- particularly the DOJ guidelines, but other material that's coming out of this.

So, you know, I think that the rules are in place. We just have to figure out a mechanism to making sure that they're being followed.

MS. CONEY: The recommendations that I have made -- or that EPIC is making at the -- are at the end of the report. But most of them focus on transparency and assuring privacy protections. One, Department of Homeland Security should disclose all the Fusion Center entities they've funded and where those Fusion Centers are located. Federal reporting requirements should direct Fusion Centers to make public the names of participants in each of the Fusion Centers. Annual reports by Fusion Centers -- basically, talking about the numbers of arrests, prosections, convictions by category of offense, which directly relate to the information -- the work of the -- of Fusion Centers. All information collected, analyzed, or shared must comply, at a minimum, with Federal Privacy Act protections. And, where State laws offer better protections, those should apply. And that we shouldn't preempt any State laws that of -- strong State laws that provide strong privacy protections. We should not meddle with those laws by trying to set a lower Federal ceiling. And transparency. For instance, actionable items that come to local, State, or Federal jurisdictions on requests by other Fusion Centers should be followed up. The individual who was arrested in Kentucky, did anyone follow up to find out if he was actually charged? Was he prosecuted? Was he convicted? What was the disposition of the request that came in from the Fusion Center, regardless of the entity? And then, of course, looking at the wall between national intelligence requests and their engagement with Fusion Centers. I mean, how are we going -- how is oversight going to be implemented in that environment? Because the Fusion Centers and the local law enforcement entities or the private-sector entities will find it very difficult to go to a national security entity and say, Okay, what did you do with the -- you know, the information we gave you? That kind of thing.

Those are the recommendations that we're making. And we think that's the best approach, to put some structure and guidance and oversight, checks and balances, in the processes.

Thank you.

MR. BEALES: Larry Ponemon?

MR. PONEMON: First, I want to apologize for having missed what appears to be a very fruitful and productive presentation by our panelists. So, please accept my apology.

But, just in hearing this conversation, I really would like your input, because I -- as my colleague, Lance, mentioned, we're -- over the course of the last few days, I'm -- we're starting to get more and more concerned. We were concerned about some of these issues, but, even more concerned. What I'd really like to understand from your perspective, Is the concept of a Fusion Center, given everything that's going on, an impossible concept -- because -- all the bureaucratic issues, all of the cost issues, the lack of accountability that could emerge -- or is there a net benefit to the public? Because ultimately what we're talking about is what's in the public's interest, right? Not what's in the Department of Homeland Security's interest or your interest, but what's in the public's interest. I mean, we are part of the public, so the -- at the end of the day, how would we know -- is there some -- in your mind, some calculus whereby we can say that the value to the public out -- is more valuable, because it creates greater safety and security than the potential diminishment of our civil liberties? I'd really -- I mean, if you could each respond to that, that would be very helpful.

MS. CONEY: That's the proportionality discussion. Proportionality is really the analysis of the cost-benefit of taking a particular action, of following a particular -- to reach for a particular outcome. Proportionality is part of the Organization of Economic Cooperation and Development's privacy guidelines. It's not a part of the Federal Privacy Act guidelines, but it's a very important rule for determining whether the benefits from taking a particular action outweigh the problems that would have been -- could have been avoided if you take another route. The proportionality discussion is part of what should take place, because right now the centers are being rolled out, but you're not having the proportionality discussion, and it may be that society determines that, no, the benefits accrued by allowing private-sector involvement may not be great enough, that maybe that role should be limited to analysis or being able to answer questions about vulnerabilities or potential threats, how plausible are they, that kind of thing, but not actually getting into customer databases and things of that nature.

So, yes, it's a very important thing, and we should be in the process of doing that.

MS. FRANKLIN: This may not have been part of the intended premise of your question, but, to the extent it was, I just want to disagree that it's necessary to sacrifice privacy in order to have a Fusion Center. You can institute the protections that will simultaneously do both. And, in many situations, they are consistent goals: to serve the privacy interests and civil liberties interests and the security interests. For example, in our watch list report, one of the recommendations that we make is, if you get an anonymous tip, uncorroborated -- somebody just makes a call, you don't know who it is, you don't know how reliable they are; could be somebody just, you know, against their next-door

neighbor they have a grudge against, you don't know -- that so-and-so is a terrorist. Okay. Well, you don't want to throw that out, because maybe it's reliable. But, in the interim, while you -- all you have is that call, the agents should not be able to take any action against that individual, based on that uncorroborated tip. So, when you implement these privacy and civil liberties protections, you say, "That's not enough. It has to rise to the level upon which it should be actionable." It's serving both interests, because that would be bad law enforcement, to act on it, and it would be violating someone's privacy and civil liberties to act on such an uncorroborated and anonymous tip. So, I don't -- I don't think that they are inconsistent. I think you can institute the privacy protections and still move forward with whatever security goals you may be able to serve by the fusion concept.

MR. GERMAN: This is where I think it's very important to state what the mission of the Fusion Center is. If the mission of the Fusion Center -- which is what we found some of the Fusion Centers consider their mission -- is to be a central call-in location so that everybody in the State knows that if there's any kind of threat, that call -- that comes to one place, and that -- any law enforcement agency that feels there is some information they need to know, they know who to call, so that there's one place. As long as 28 C.F.R., Part 23, is being followed, and law enforcement is only collecting law enforcement information, that's perfectly -- that's great. You know. And if that -- and if they can be networked so that they can share that amongst law enforcement agencies across the country so that every Fusion Center knows that if I'm talking about a problem in Kansas, I'll call the Kansas Fusion Center, that's great, as well. You know. And if that's what our purpose is, let's move forward to do that. But let's make sure that we're not doing these other things that are contemplated in the guidelines, about collecting information that has nothing to do with threats or criminal activity. And so, if that's what the mission is, then it can be accomplished. If the mission is to create what I read the DOJ guidelines say about having one source where all information from the public and private sector is available, I'm not sure that's a model that can work.

MR. PONEMON: Would you mind if I just have two follow-up questions? So, from your point of view, it -- it's basically a scope-creep or a mission-creep problem, that, with a real narrow mission, (a), and (b) great consistency across the -- across centers, so that you basically have a model that you could understand. And it seems like, today, my understanding, from the Lieutenant -- I forget his last name -- the -- from Maryland -- very nicely stated -- but someone mentioned – maybe it was Mr. Riegle – he mentioned that is you're applying the Massachusetts to Arizona, because you have different geographies and different issues, it's hard to create the one model. But I don't think it's hard to create one -- a process. You know, engineering it so it has the flexibility, but there's not a lot of deviation, and there's not as great a potential for the mission creep,

which isn't necessarily bad people doing bad things, but it's good people probably making mistakes because they don't understand the process well enough.

So, is that the point that you're making, that it can actually work, but it could only work under the condition of a very well-defined mission?

MR. GERMAN: Absolutely. And that mission goes beyond the Fusion Centers, as well, because -- in fact, speaking to the Lieutenant, at a previous meeting that we had, they were one of the Fusion Centers that was very interested in talking to us and cooperative in answering our inquiries. He made a very good point, because one of my concerns, as a civil libertarian -- ad this is something that came up in most discussions where we asked Fusion Center personnel what they do -- they say, "Well, you know, there are the calls that come in, Muslims taking pictures and Muslims acting suspicious," and, you know, I have a concern with that, because, of course, where -- you know, where there's smoke, people think there's fire, but in many of these cases, there's no fire at all, and -- but, pretty soon, if there's enough smoke, people will assume there's a fire. And he made a very good point. He said, those calls are going to come in to law enforcement anyway. So, wouldn't you rather them calling in to one center that's used to receiving those types of calls and can -- and knows how to handle them? And that's great. And I commend him for that. But he admitted, during our talk, anything that implicates a terrorist threat must be reported to the FBI JTTF. So, even though the Fusion Center analyst recognizes this as a nonimportant, not valid complaint, he still has to report that to the FBI, which then does create a record. So, while the Fusion Center isn't creating a record, the FBI is creating a record.

So, that mission also has to be carried over where there is that leap, so that everybody's playing by the same rule.

MS. CONEY: But that –

MR. GERMAN: But –

MS. CONEY: EPIC really wants to see that step go one step back and say that you look at proportionality, you create the structure, you answer the question, we want to prevent what? And then, what are the -- which are -- what are the best means for stopping this bad thing? And then, what is the least privacy-intrusive method to accomplish that? But then, you also create reporting requirements, so the system tells on itself. You know, if we're putting all of these resources and efforts into Fusion Centers, then what we are actually getting out of the process? Are we getting prosecutions, investigations? Are we getting deterrent? Are we getting preventative measures that are taking place, that are getting us this particular outcome for this particular effort? That's very important for the oversight mechanism from Congress, for the media, from the public, in order to evaluate the contribution of taxpayer dollars and human resources and

capital, and on and on and on. So, you -- we have to get information out of the process in order to make judgments about whether it's a good process or not.

MR. PONEMON: And just one other point about them -- thank you very much -- on the -- the issue of – you mentioned, privacy and for civil liberties -- the problem with that argument -- I agree, it can be engineered that way, but it's actually an information economics problem. And, at the end of the day, you're never going to have enough time to decide whether information is correct. It's the inherent inaccuracy of these tips -- sometimes they're good, sometimes they're not --and the inability of the agent, the person receiving the information, that creates the possibility of marginalization of someone. So, the idea is -- you might have to accept some degree -- it may be very small; hopefully, really small -- but, otherwise, the system -- you can't construct a system, that we're talking about here, that is perfect, because of the time dimensionality.

MS. FRANKLIN: I would just say, on that, I agree. No one is -- we're human, we're not perfect.

MR. PONEMON: No, I --

MS. FRANKLIN: But to have clear rules, particularly in the watch-list context, which is the one I was, you know, speaking of, and clear standards that are uniformly applied and understood -- What does that mean? -- that it's enough to actually put somebody on a watch list, as opposed to maybe having not quite that threshold level, where you put them on some, maybe, preoperational list --

MR. PONEMON: Right.

MS. FRANKLIN: -- where you would still have agents investigating further, you would see what you would come up with, but that person shouldn't be on a list where they suffer consequences, subject -- such as the people legitimately already on a watch list.

MR. PONEMON: Thank you.

MR. BEALES: I want to thank all three of you very much for your time today. This has been a fascinating discussion, and a very helpful one. And we look forward to many more.

Our next speaker is Robert Mocny, who's the director of the US-VISIT program in Department of Homeland Security. We've heard about US-VISIT before. It's the largest biometric-based immigration and border-management system in the world. Mr. Mocny is responsible for day-to-day operations, including the development -- managing the development and deployment of the system. He has served in several senior Federal positions related to immigration policy and operations, including as acting assistant commissioner and assistant chief inspector with the former Immigration and Naturalization Service. He led the establishment of the dedicated computer lane

program, Secure Electronic Network for travelers, rapid inspection, that we visited in Bellingham and that exists in other places.

And, Mr. Mocny, welcome, and we look forward to your update.

MR. MOCNY: Thank you, and good afternoon. I do want to express my gratitude for having the chance to come and speak to you today.

Let me just state, from the very beginning, that working with groups such as yours is integral to what we do at US-VISIT. I think you know that privacy is contained in one of our four goals, which we will go over as part of this update.

And I think it's also fair to say that we have matured as a program, and we have certainly realized, as a global leader within the biometrics realm, the extreme importance of protecting the privacy of the individuals as we mature and as we go into other areas, of which we'll talk about a few today. And even when we reach out to our international partners, we make sure that we talk about the need for protecting the information that we're collecting.

So, we're going to talk to you today about a couple of issues. The two biggest ones right now are biometric exit at our air- and seaports, and then the transition from two prints to ten prints.

Before I get into those specifics, let me very briefly -- because I do believe you are aware of our program, and we're running late into your afternoon -- so, let me just tell you how US-VISIT works, very briefly, perhaps for the public, as well.

It is, as you mentioned, the largest biometrics-based identity management system in the world. It does contain some 94 million records of individuals that we have obtained since we began operation in January of 2004. We have a watch list of about 3.2 million individuals. That watch list is used anytime we encounter an individual at a visa issuing post overseas run by the Department of State, so the Department of State uses our fingerprint system as part of their verification process and their vetting process. So, that person is then checked against the 3.2 million in the watch list, and then the 94 million, to see if we've seen that person before in a different name. And, lo and behold, we have, in many cases, where people will visa-shop and try to get a visa in a different name because they're either trying to hide something in their past or they have failed to meet the test that the Department of State has stood up, you know, in the previous encountering.

The other way a person, of course, will encounter US-VISIT primarily with the visa waiver countries is at the ports of entry. So, the first time people who come to the ports of entry, they do not have to go through the vetting process at the Department of State, and they merely get in a plane and show up at the ports of entry. We will then encounter them -- again, taking two finger scans, the left and right index finger. It's -- at the port of entry, it's run against the 3.2 million, and then, post-primary, the 94 million records are

checked. And, of course, that changes every single day. We're running at about -- or increasing our fingerprint database at about 20 million per year. So, you can imagine where that database will be in 10 years' time. It's something that we're certainly aware of, and we have to make sure that we take -- took great pains to protect that information.

The four goals that we've talked about in the past -- very briefly talked about those -- the first goal is to enhance the security of our citizens and our visitors. We believe it is a fundamental obligation of the Federal Government to protect the people who live within its boundaries. And so, we make sure that we can protect those individuals by keeping the bad people out.

The second goal is to facilitate legitimate travel and trade. We recognize that one of the hallmarks of the United States is its openness. We want to maintain that openness. We want to make sure that we have economic security, as well as national security, protected. And tourism is a -- is a great supplier of that economic security, and so, we have to make it as easy as we can for the good people to come into the country, and as difficult as we can for the bad people.

People often ask us, How can you have -- how can you enhance security and facilitate legitimate travel and trade? And what I often say is, you do the first by doing the second; you enhance security by being smarter, you facilitate the vast majority of people coming into the country who aren't coming to do harm, and you find ways to make it easier for them to come into the country, making sure you're doing due- diligent checking, and that way you can spend your meager resources on those individuals who are trying to do harm to the country.

The third goal, then, is to ensure the integrity of the immigration system. We have to make sure that people come to the U.S. We also have to make sure that they leave on time, and that they respect our laws while they're here.

And then, the fourth is, of course, to protect the privacy of our visitors. We're going to talk about -- a little bit about that today.

But let me just basically tell you than, when we first started the program, there were a lot of skeptics out there. How can you have a large-scale biometric fingerprint system and still protect privacy, still have efficient borders? I have to say that there were many of us who were questioning it along the way, as well, and were quite remarked -- it was remarkable to see the development of the information systems. In fact, the airlines came to us the weekend before we were supposed to launch this thing -- congressional mandate said we had to have this in place by December 31st, 2003; and we did -- but they came to us, and they said, "That's New Year's weekend. What if the system doesn't work and we have all these people coming back after that weekend, and we have major interrupts at the airports?" But we listened to the airlines and the airports, and we said,

"Okay, we'll wait until that following Monday." Well, we did. And nothing really happened. The system's been running efficiently 24/7, 365 days, servicing not only the State Department, but all of our borders. In that time, we have denied entry to hundreds of individuals at our ports of entry, and the State Department has denied thousands of individuals visas that might otherwise have gotten those visas.

If we're going to measure the program by the goals, let me briefly, you know, go back to them and say, how have we done that?

Enhancing security of the -- of our citizens and visitors. As I just said, we've stopped a hundred -- hundreds of people coming into the United States based on the biometrics alone. And these are people who showed up at a port of entry with a passport under a -- with a different name, with a different date of birth, trying to beat the system, as it were; and, when they put their fingerprints on the platen, they turned -- they were found out to be wanted for murder, wanted for some aggravated felony, wanted for whatever crime, or having a crime in the past that would deny them the benefit of entering the country. And similarly with the State Department, in the thousands where people would masquerade as somebody else using different information to try and get the visa.

I can say, with a straight face, that we have effectively shut down visa fraud. You cannot go anywhere in any consular post in the world and get a visa, and then have that visa used by somebody else, whether you sell that visa to somebody, let your brother borrow it, or lose your visa; it cannot be used. That's significant, because that's an issue for immigration authorities that we've been wrestling with for years.

And the same would go with the passport fraud for the visa waiver countries, you cannot have a passport that has been logged in within US-VISIT, tied to the biometrics. That passport -- that visa waiver passport cannot be used by anybody else. And that's rather significant.

A bit about privacy. As I said, it's one of our four goals. We have -- we built everything into what we do with US-VISIT. We publish privacy impact assessments on a regular basis, anytime we have any major change with the program. We have a chief privacy officer, who's here with us today. We have a redress process. We have tried to embed privacy into the program itself. Every US-VISIT employee must go through privacy training every single year. When we have MOUs with anybody else that we might share information with, they have to go through privacy training before we give them that information. And so, we're very cognizant of the fact that, when people give up their fingerprints -- and we call them fingerscans, because that's what they are -- but people understand them to be their fingerprints, something about themselves, that that's something that we have to pledge to protect. It's something that we have done, and we have done very well.

I will have to say our redress numbers are very, very low, people calling in and saying, Can you please fix, X, Y, or Z. And usually it's an inadvertent error, where the husband and wife's fingerprints may have been swapped, and we go ahead and correct the record.

Once -- as you know, diplomats don't have to go through the process, but, after a long trip, sometimes even they just go ahead and put their fingerprint down. They back, later on, and say, I wasn't supposed to go through that. Can I have my fingerprints removed from the system? And, in fact, we have removed those fingerprints from the system. So, redress is a very big part of what we do as far as protecting the people's privacy.

Let me go into some of the things that they're working on. I can talk about some of our success stories. I just mentioned a couple of them. But they're out there every single day, people who try to get into the country based on false documents, and they're tripped up because of the fingerprints. Not a big surprise, but I just want you to know that it does occur. It occurs on a near-daily basis; certainly around the globe it does.

What we're going to be working on over the course of the next year is two very big events that I want to talk to you about today.

The first one is about air exit, air and sea exit. We are going to use the same type of biometrics for people exiting the country at our air- and seaports that we are at our ports of entry as they come into the country. We have been mandated by Congress to do this. We believe it's the right thing to do. It gives us a much better record of that individual's immigration history. We can say for certain that that person has left the country. And it obviously helps us on the negative side, where, if that person doesn't leave the country, we can then turn that information to the ICE officials and they can go and take the appropriate action for anybody who does overstay a visa.

It's a very remarkable event, in that I think people may have thought that immigration authorities had the ease by which to go and find someone who may have overstayed their visa after 6 months or after a year. And it just hasn't been the case in the past. Not until US-VISIT was stood up and we formed a group to look at that overstay information and cleaned it up, as it were, to make sure that the ICE agents had effective information to go after it were we able to do this. And right now we can, and we do, turn over, to our ICE colleagues, information that allows them to go and find an individual at a particular address who may have overstayed their visa by some egregious amount of time -- a year, 2 years, whatever that might be -- and then take the appropriate action. Again, something that wouldn't have happened, had we -- if we did not have the information in the way that we have it today.

The issue with air exit, we piloted this last -- the last 3 or 4 years -- 3 years, I suppose -- where we put kiosks out there at 12 airports, two seaports, and we made it mandatory for people to go through if, in fact, that machinery was there, and we had a very low compliance rate. People were not going through it, even though we had the kiosks, we had mobile devices, we had a, kind of, host of different technologies out there. And what we found was, the technology certainly worked. When we had a fingerprint upon exit and entry, we could match that with near-100-percent accuracy. The problem was, people weren't finding the kiosks. They were located in an area of the of the airport that was not easily accessible, they were late for their flight, they were intimidated, or they just didn't wan to do it. We had about a 20-percent-or-so compliance rate.

Well, the technology worked, but the process didn't. So, you have to think, well, how do you make it easy for the traveler to go through? Well, there's three basic points where people are going to, kind of, exit the country. They're going to exit from the -- at the gate when they get onboard the plane, they're going to go through TSA for the security checks, or they're going to go to the check-in counter. We looked at those three, and we've said, at the gate you've got fast turnaround times. We don't have the infrastructure that most countries have, where you have departure -- international departure lounges, or even passport control. And so, anybody can leave from any gate. You can leave from Gate 56 at LAX and go to Santa Barbara or -- and then Gate 57 to go to Sidney, Australia. It doesn't really make that much difference, the way they have their operations constructed. Plus, again, the turnaround time for flights that come in late, get the crew onboard, you've got to get people onboard, you've got a string people who haven't gone through the exit procedure, you're going to miss somebody. So, the gate's not the most effective place to do it, because of the fast turnaround times.

TSA, their mission really is to keep bad things off the plane. They've got to concentrate on looking at the screens and concentrate at looking at the luggage. Plus, the real estate in some locations, it's just not conducive to adding more and more equipment to that area. And so, the adage was, Well, if you can't put it at all TSA locations, you can't put it at any. What I mean by that is, if I'm at Orlando, I might be able to go through TSA, but if I'm at another location where the space is cramped, I have to go somewhere else. Again, it goes back to the kind of consistency aspect, where we want people to comply, so we have to help them comply.

So, where is that one location that most people who travel internationally with baggage and such will go through? And that's the check-in counter. At some point, you usually have to go and get that boarding pass, check in your luggage, and go through some kind of screening. We are going to publish an NPRM, this December, which will require the airlines to implement biometric collection at the check-in counters. We will then work with them, we will hear their response, which will be vociferous, and there will

be some back-and-forth. And I can only tell you that our Secretary committed to this, if you heard his testimony a couple of weeks ago, and where he basically reiterated the same thing. You're going to hear the airlines balk at this, is what he said. And we have to maintain that commitment.

We'll publish a final rule in June or so, and then we'll have the deployment begin in the December timeframe -- again, working with the airlines. I won't say it that this is not a challenge, that there aren't ancient reservations systems. I mean, there are jokes about how you check in, and they're, you know, trying to give you a window seat, and all the typing they have to do. They are antiquated system, no doubt about that. How do you plug in an AFIS, an Automated Fingerprint Identification System, into an old reservations system? How do you get that information, where they don't touch the information? We're not going to send them a signal back. We're not going to say whether this person is wanted or not. We're simply saying, "Be a collection point and send us the information." It might be batched, it might be immediate. We don't know all those details yet. But they will be collection points.

Can they use the kiosks that they're starting to use a lot more of? Sure. We've talked about that, and we can employ some kind of technology for that. We will work with the airlines. We will embed, if need be, our IT specialists with their IT specialists to make sure that we get this thing right. But we will have some form of biometric collection, with the airlines participating.

The cruise lines, in my estimation, will be a much easier lift. The process by which you get onboard a cruise ship to leave the country is much more controlled, a lot easier than it is in many airport locations.

So, the air edge will be a challenge. As I said, we'll be -- we'll be looking for that NPRM sometime in December.

The next big event I've alluded to, and you are aware of, is the transition from two-print to ten- print. This is a pretty good story, in the sense of -- we had always known we would have to go away from two prints to something more than two prints. NIST told us, when we first instituted this program, that, with the number of prints -- and this had never been done before -- with a 10-second response time, in some cases, 15 for the State Department -- 10 seconds for CDP at the ports of entry, and 15 for the State Department -- that, as your gallery size grows, the number of fingerprints in the system, and the time you need to execute that match, you're going to have to take more fingerprints. And I always akin it to, if you see a friend of yours, and they've got the veil over a face, it looks like the person, but you're not quite sure; and, as you take more and more of that veil away, you begin to recognize, obviously, who that person is. Well, that's kind of like the veil over the face. With just two fingers, the system -- the computer systems go, "I'm not quite so sure." And so, my fingerprints begin to look like his fingerprints, and I get sent

back to secondary, and I'm held up inadvertently, and I have to wait for, perhaps, a few minutes, or whatever, but I am being sent back too often, false matches. By having all ten, I am me, you are you. And so, we basically believe that will nearly eliminate, if not entirely, the false-match rate, where we can definitely tell, with the computer systems, that that is the same person.

Now, people -- there's always people out there with poor fingerprints, and we always will have fingerprint examiners to verify that, if, in fact, there is that match -- false match, rather. But we believe, by having the ten fingerscans, we'll be much better -- in much better shape.

Now, the State Department has already began deployment of the ten-print devices to their consular posts overseas. There are somewhere around 130-plus out of 211. They plan to finish the deployment by the end of this year. We're going to pilot the ten-print procedure at our ports of entry, starting the end of November. Let me list those airports for you, because they're not insignificant. They're going to be at Boston, Chicago, Detroit, Houston, Atlanta, Miami, New York's JFK, Orlando, San Francisco, and Dulles. In fact, I believe we open up Dulles -- November 26th is the current date right now.

We couldn't have done this 2 and -- you know, maybe 2 years ago, 3 years ago. The technology was not there. When the Secretary came into Homeland Security, he made the bold statement and the bold, you know, charge to us, in June of '05, that we were going to move from two to ten. Well, even then, the technology wasn't available. So, we went out to industry and said, "You've got these big boxes that take too much time, there's not enough real estate at the CDP's desk -- CDP officer's desk. They're not very user-friendly. And so, we're challenging you to come up with something that's much smaller, user-friendly, lightweight, and faster." And so, in our offices, we had several members of several different IT companies -- and when I say "we," it wasn't just DHS, it was DOJ, Department of State, DOD, NIST. And we had a subsequent follow-up industry day in which we were joined by our partners from the U.K. and the EU responsible for developing their biometric immigration control processes. So, it was a united front to industry, to say, you know, "Build us something that really works." And I'm very happy to say that, within about 8 months' timeframe, industry came back with several prototypes that had a lot of promise. We did a down-select to a couple of 'em, and we have about 50 of them right now that we're testing in our offices. It looks good. I can't make a commitment that it's going to be faster or slower, at this point.

We'll see, when we get those plugged into the systems with CDP. We'll be testing a couple of different options. Right now, it's simply the left and then the right finger. We're going to have to go, now, through a multislap process. We're going to test a slap, slap, and two thumbs, and then a slap, right thumb, slap -- or left thumb, slap, right thumb. We're also going to move -- at this point, we're considering going from left to right, going

right to left. Sounds like a small issue, but what we're seeing is, more people are right-handed than left-handed, and they're starting to reach out with their right hand. The problem is, about 50 percent of the people we're seeing are repeat customers, and they're so used to going left-right that they may be confused with that change, too. So, again, a series of, kind of, operational testing to see what happens to the lines out there.

The obvious other reason that we're doing this is the latent print issue. And we would be remiss if we didn't even just think about the fact that, if we're collecting latent prints -- and I always use this as an example -- of bottles in caves in Afghanistan or wherever, I'm going to miss this guy, because I just -- I'm just taking his left and right index finger. But if I have his other fingerprints, and I get 'em off this bottle, I'm going to catch him. And I can tell you that, already, with the State Department having begun taking ten prints at many of their posts -- as I said, about 130, 140 -- we have already identified individuals from latent prints that we've been collecting around the world. So, a positive effect from the -- from the idea that, by taking more prints, you are not only enhancing your operational efficiencies, but you're also enhancing the security aspects of this.

Those are two big things I want to talk to you about today. There probably are more. I'll save some time for questions.

I just want to conclude by saying that we still, kind of, have constants, no matter what the project is. We've got projects with Coast Guard, we have projects with other entities within DHS. Two of the constants really are outreach and the dedication to privacy. I was just at a speaking engagement with the ITAA, the Information Technology Association of America, in which I repeated the same basic message. It's all about outreach. It's about talking to the public, "What are you doing with me, with my family? What are you doing to me? What is this about? Please inform me. Keep me informed. And, oh, by the way, make sure that you're protecting my information." And, I think, in all those areas, we're -- we will continue to do that. We will continue to do outreach. That's why I appreciate being here today. And we will continue to respect people's privacies as technology changes, as biometrics change over the course of time. So, we'll always have to be out there with a strong outreach component and a strong privacy advocacy.

With that, I want to thank you very much, and I'll be more than happy to answer any of your questions.

MR. BEALES: Well, thanks very much for being with us.

Now, I understand you have a schedule constraint and have to be out of here, so we will get as many questions in as we can. But, you know, just tell me when you have to go –

MR. MOCNY: Sure.

MR. BEALES: -- and we'll -- if we run out of time before we run out of questions, so be it.

David Hoffman?

MR. DAVID HOFFMAN: Well, first I'd like to thank you for coming, and also to commend you on the change to the exit program for US-VISIT. I think the last time we heard from folks, it became clear that that -- the former test likely was not -- was not likely to succeed. And glad to see that you guys are moving to something. Granted, it'll be difficult, but something that could really have great success.

I'm just wondering, the other thing that I think we had heard before was -- in our prior testimony – that the retention period for the fingerprints was what many of us consider to be very long. I think it was over 70 years, or something. I just wanted to ask you, again, if there's been any analysis of that, to see if that was absolutely necessary, and whether that's still the same figure.

MR. MOCNY: It's still the same; 75 years has been -- that was the original time period that -- when I -- that was first announced, back in the early 1990s. There's been, I would say, quote, analysis done about it. There certainly has been discussion about, Is that the right time to keep the information? Part of the reasoning behind it is the -- first of all, life spans are increasing over a period of time, and we want to make sure that we have, from the immigration continuance standpoint, the information about the individual across that immigration continuum. So, from the standpoint of, Will we see -- and, again, this is a bit incongruent with US-VISIT, in the sense that we fingerprint 14 and up, so you're not having that life span. However, the State Department does begin to fingerprint children at 7, because of child abduction cases across the southern border. We also know, through research, that fingerprints are pretty much stable by the age of 2. So, will we make a policy decision to change that 14 down to something like 7, or even younger, depending on the need for it? And will that individual then, over the course of a lifetime, be coming back and forth to the U.S. for that period of time, where 75 years may not be that far off the mark? As I said in my prepared statement, we're seeing people come back at about a 40-, almost 50-percent repeat rate. And keeping those fingerprints allows us to have the best image and then process that person in the most efficient fashion.

So, I think we will always look at, Is that the right retention period? It's not something we're -- we've dismissed as not having. And we will certainly, you know, do so, to keep that as long as it is practically -- and usable, and, of course, informing the public if that changes at all. But that's the rationale behind it.

MR. BEALES: Charles Palmer?

MR. PALMER: We've spent a lot of time talking to folks in Bellingham about RFID-based stuff. I believe, a few months ago Secretary Chertoff kind of called it all off, or redirected the program, or something to that effect, I don't remember the words exactly. Is TSA -- or is RFID playing a role with any part of US-VISIT? And can you tell us about it, if so?

MR. MOCNY: Sure. We did do some experimentation with RFID for land-border exit. I didn't touch on that in my -- on my prepared remarks here, only because if air exits can be challenging with the airports, land border would be -- would be challenging, just because there's no infrastructure out there. So, we looked at how we might use technologies to capture biographic information as the person who is driving out of the country at speed, sometimes 40, 50 miles an hour on a highway with Canada or so. And so, we did look at that. It is vicinity-RFID, I think, that you're aware of, so, you know, with -- we sometimes call it long-range -- so that we didn't have to have that person slow down and put their hand out the window and touch something. We've got it at speed, with a convenience factor.

We also did look at, and we had some experimentation with, biometric RFID, which was a device that captured a thumbprint. The thumbprint stored on the card matched the thumbprint on the card, and then send a signal, RFID, saying that a match was made. Didn't send a fingerprint, it sent a signal saying a fingerprint match was made or not made.

So, we, then, of course, shared that information. We shut down -- they were proofs of concept, and there were different levels of success. I think there's a GAO report that says it was, like, a 14-percent success rate. True on the -- kind of, the uninitiated users of it -- we had people trained to use it, it was a much higher rate. But, again, it was a proof of concept, and we said, Thank you very much, and, kind of, shut it down.

We then gave that information to CDP, who are now utilizing a lot of that information for the WHTI card and some of that process.

I will say -- and you mentioned, in the opening, about my involvement with SENTRI. We have been using vicinity-RFID since 1995. We implemented the SENTRI program on the southern border, at Otay Mesa in 1995, and have been using it successfully and safely ever since that timeframe. It was then changed to NEXUS, and there are other places in Washington where we have that same technology.

So, the technology has been out there for quite some time. It's been used very effectively. It's just a number that's transferred. We believe that that is the answer for the WHTI card, because of its -- both convenience and the security features.

MR. DAVID HOFFMAN: I just want to -- the programs that you just described, am I correct in remembering that those special application programs for people to be able to leave at -- quicker -- if they go through the application program?

MR. MOCNY: They are Registered Traveler programs, and --

MR. DAVID HOFFMAN: They're registered --

MR. MOCNY: -- they're voluntary programs, absolutely. Yes.

MR. DAVID HOFFMAN: Okay.

MR. BEALES: Jim Harper?

MR. HARPER: A follow-up to David Hoffman's question about the retention of fingerprint information. I'm delighted that he asked the question. But -- no, I think your -- I think your answer was a fair recitation of the -- of the reasons you're retaining the data. But, in your answer to his question, you moved from the function-based reasons for retention -- you talked about, you know, catching visa reapplicants and overstayers and murderers and even terrorists -- to a paperwork basis, which is, well, we want to -- we want to see the totality of people's immigration behavior. You could probably chart the number of years that a person will be an active -- actively attempting to reenter the United States under a false name or whatever, and, at some point -- 5 years, 10 years, 15 -- you can probably -- you can probably pretty well be sure that the person's not going to come in, and they're not going to be the same threat they were that many years before. And so, it's -- this is kind of like comparing the weight of a rock to the length of a line, but the security benefit of retaining the data after some period drops off quite dramatically compared to the privacy consequence to hundreds and millions of visitors to the country who are, many of them, feeling like they're being treated by criminals -- like criminals, and then knowing that their data is being kept as if they're criminals, are frustrated by the United States, don't want to come back to the United States, you know, harms our international reputation. I'll add, as an aside, that if you want more compliance with an exit program, you say, "Guess what? You do the -- you do the exit side of this thing, and we're going to -- we're going to expunge your records within a -- within a decent period of time." So, urge you to give more consideration to the privacy side of that difficult balancing act.

MR. MOCNY: And it's a fair question to ask, and to continue to ask. You know, I'm -- I don't want to say I'm forcing a solution into a 1995 decision. But, in some ways, I am. I mean, we -- IDENT was what we used to build US-VISIT. IDENT was created back in 1995, thereabouts. Its original purpose and its original design included the 75-year history. We inherited that. We didn't design US-VISIT. We didn't say, "Well, here's US-VISIT, let's pick a number: 75 years." So, I'm simply, kind of, giving you the historical -- which is the fair question to ask, Well, then fine, new use, let's look at that and see if, in

fact, for the purposes of US-VISIT, is it important to still have that in there? It may be, for some other purpose, but, for the purpose of US-VISIT --

So, it's something we've said that we'll look at. I know Nuala said this, so many years ago when she was here, that we would -- it's something we would look at. I will commit to you that we will continue to look at that, and just ask that question, is it still fair to keep for 75 years? The answer may be yes, but it may also be, in some cases, no. I just can't commit to that decision, but I can certainly commit to looking into it a little bit more stridently.

MR. BEALES: Neville Pattinson?

MR. PATTINSON: Thank you. I will not be asking any questions on RFID, just before anybody wants to know what I'm going to ask about. So, I have to recuse myself –

MR. MOCNY: You did. There's only one allowed, I think.

[Laughter.]

MR. PATTINSON: Yeah. So, I'm really interested about the biometric side of things. Clearly, two prints have worked for a few years, and now, clearly, the -- I guess, the false reject rate's rising because the database is getting so big, and the technology is finding it difficult to make a positive match. And, you know, we were invited to come and see the forensic examiners in Rosslyn, and how they're there to respond. So, their workload must be increasing as the system's getting more loaded. So, we're going to use ten prints, which I clearly understand the reason for that. But what's the projection of the use of that ten fingers, as far as years, before we have to add, maybe, toeprints, as well, to continue to keep ahead of that database that's -- growth -- as we have this 70-year, or whatever, retention?

The second part of the question is about -- what are you doing with the face? Everything here is to do the fingers, which you take the left and right. But I understand you also take a picture of the face. I'm -- I've heard reports of -- the quality of that is poor, and it's not designed to be computer-recognized, and so on. But you have a picture of a face, or at least the person, shall we say, shoulders-up. If you have that face, then obviously there's the use of the ability to do that for computer automation, but why are we collecting it today if we're not using it for that? And maybe one reason you could be using it, ultimately, is for the iris, which is another biometric, which is part of the face, which could give you another form of metric to test that person.

But, fundamentally, you know, what's the longevity of the fingerprint system, and why are we collecting the face, when we're not -- don't seem to be using it?

MR. MOCNY: All great questions. And I can see you know a lot about this, because a lot of what you're saying is what we're looking into, at this point. We -- the --

let me answer it, kind of, in progression, here. The fingerprints with ten, we believe, will be -- and I can't give you a year's projection, but we have a formula that says gallery size, number of fingerprints in there, and then time needed to execute that decision equals so many matchers. So, that has somewhat infinite number of possibilities. Obviously, over a period of time, you have room for only so many matchers. But, again, they're basically servers there, that are racked and stacked. So, there's no end in sight with ten fingerprints, just because of the permutations, that we believe.

The face -- and I'll, kind of, wrap it up at the end with the last piece you wrote -- or you mentioned -- the face, we take merely for a record. Who was this person that is attached to this particular face? It's just good for good old-fashioned, you know, kind of, you know, cop and investigative kind of investigations, you know, who belongs to this person, do you have a photograph of the individual? So, a little bit of that is, kind of, old-fashioned just -- you've got a -- you know, the mug shot of the individual.

We are going to be deploying enhanced cameras and software along with the ten-print devices to capture better photographs and look at some policies to not have these not-usable photographs, in some cases, and make them more usable. We'll also be testing some facial recognition algorithms, as well, which then gets to your third part about the iris. And, really, if you think about those three issues, I mean, that's the three-legged stool of identity, is the fingerprints, the iris, and the face. And having all those three will have us do a much better job of doing the match rate, such that, when you get into things like spoofing, and you have Registered Traveler programs, you can then select two or three or one or just change it however you want randomly. So, we're looking at iris, down the road. We still have the one company and the patent issue to deal with. But we certainly believe that the multimodal process by which we identify individuals is going to be the answer, in the long run.

So, it's certainly something that we're looking at. The unified IDENT program that we have, which is modifying the current IDENT process to be able to accept ten prints. We're also going to be having that adaptable to include other biometrics, as well.

Probably have time for maybe one or two more questions.

MR. BEALES: I think we've run out of questions. So, I want to thank you for extending your stay, and thank you -- thank you for joining us here today.

MR. MOCNY: Thank you very much.

MR. BEALES: I believe we do not have any requests for public comment. So, are there any comments or questions or closing remarks from the panel? John?

MR. SABO: Just a clarification for those still remaining in the member of the committee. There's been a lot of talk, in the earlier panels, about private-sector information-sharing with the Fusion Centers. I just wanted to clarify, like -- I do a lot of

work -- I'm involved with the IT ISAC, which is the information technology sector. I work with the other sectors. To my knowledge, our sectors do not want to provide, nor do we wish to receive, personal or personally identifiable information. There may be others -- commercial interests, or whatever -- who want to do that. But I just -- there was, sort of, a lot of discussion around, well -- private-sector data and so on. We generally need information so that we can made aware of threats or, as Lieutenant Wobbleton said, if there's a particular incident involving a chemical spill, they need to reach someone who can tell them how to deal with the spill or a particular hazard or something like that.

So, I just want to make it clear that, in the ISAC community, there is no desire -- in fact, there would clearly be, from a lot of us, resistance to providing information that wasn't relevant to critical infrastructure protection.

Thank you.

MR. BEALES: Thank you.

All right. With that, our quarterly meeting is adjourned. Thank you all.

[Whereupon, at 4:00 p.m., the hearing was adjourned.]