Department of Homeland Security
Data Privacy and Integrity Advisory Committee

OFFICIAL MEETING TRANSCRIPT

Wednesday, April 6, 2005
Mayflower Hotel
1127 Connecticut Avenue, N.W.
Washington, DC 20036

MORNING SESSION:

MS. RICHARDS: Good morning, and welcome to the inaugural meeting of the Department of Homeland Security, Data Privacy and Integrity Advisory Committee.

My name is Becky Richards and I'm the Executive Director of the DHS Privacy Advisory Committee. I hereby call this inaugural meeting of the DHS Data Privacy and Integrity Committee to order, and would like to introduce Nuala O'Connor Kelly.

MS. O'CONNOR KELLY: Good morning, and thank you all for being with us today. We are most honored to have two members of Congress with us who have urgent need to be back on Capitol Hill by 9:00 a.m., so we will dispense with our introductions for the moment. And I am pleased to introduce the Honorable Bennie Thompson, who is the ranking member of the House Homeland Security Committee. Mr. Thompson has over three decades in politics and has been in the House of Representatives since 1993. He's an active member of the Congressional Black Caucus and has dedicated his career to civil rights issues and other concerns on the Congressional agenda, including those of the Privacy Office. He and his staff have been great friends of the Privacy Office, and we are grateful for his interest and his leadership, and we are thankful that he's here with us today. Congressman Thompson.

THE HON. MR. THOMPSON: Thank you very much. I look forward to working with the Committee, I look forward to working with Ms. O'Connor and her staff as you develop what is a very important mission for this country. Privacy matters are important to a lot of us, it crosses the entire spectrum of ideology from liberal to conservative, and the one good thing about being an American is many of those issues associated with your past that you're charged with is why we are such a great country, and we have to maintain that. I have some prepared remarks I'd like to read for you, and along the way I will kind of give you a little Gospel according to Bennie Thompson, if you don't mind. First of all, as I indicated, you have an awesome responsibility for you as a Committee. As you undertake your efforts I request that you keep one thing in mind, privacy and security should not be a balancing act. We don't need to sacrifice one for another. Our Homeland Security efforts we must remember are designed to reinforce the constitutional life and privileges that Americans enjoy. That includes privacy. At the same time technology is an important tool

in our war on terror. Information held in databases and networks increase the likelihood that we can identify potential terrorists. To best use technology and protect our citizens rights the government must make sure that the information is, number one, accurate; number two, remains confidential, and that the access is limited to appropriate personnel to protect civil liberties and privacy. Given the sensitivity of the information about individuals it is imperative that this data be protected during its creation, transmission, and storage.

This is where you come in. Your Committee and the Privacy Office have a responsibility to ensure that current and future programs have adequate measures in place to protect personal information and individual privacy. At the same time you need to make sure that the best technologies for data integration with privacy protections are being utilized by the government in its war on terror.

There are some issues associated with privacy I want to specifically challenge you to look into. The Choice Point and similar database breaches that have come to light in the past few months absolutely are real concerns. The issue with Choice Point exposes a serious gap in our Homeland Security.

The threat is twofold, terrorists can steal identities and credit information to finance terrorist attacks. The situation in Bali is an example where credit cards were used to finance operations. In terms Al Qaeda they have used similar methods of stealing identities and credit card financing for their terrorist activities. Now also they can use these identities to enter the United States illegally. So you need to look at that.

One of the issues associated with Choice Point and all of that is there's no real difference in the minds of Congress whether or not Choice Point and other data gathering entities didn't use best practices, or they were just dumb. The danger of them not doing the best practices possible, or not being as smart as they need to be, is something we can't as a country expose ourselves to. So I really want you to look at the Choice Point. Bank of America situation was another issue in terms of information being somehow stolen and having access.

Notification, such as a California law is important. It was only after several months did the public really find out that there had been some breaches at Choice Point. So those things are really important to the Committee, and I want to charge you with looking at those database breaches.

From a Committee and Congressional standpoint we've asked the Department of Homeland Security, Ms. O'Connor's office, to investigate this Choice Point matter and determine how to best protect private information. But we need your help. Contrary to what some members of Congress think we don't know it all. And that's why as ask citizens like you to help us fashion the model that we need to adopt to secure databases and other things. I've also introduced legislation in March with Congressmen Edward Markey, and Senator Bill Nelson. This legislation requires information brokers to safeguard and protect the confidentiality of personal identifiable information appropriate to the nature and type of information.

The other thing I want to share with you is that we buy information from some of these same companies as the government, so it's important that some of that information is private and privileged so that we can protect the people we're gathering the information on. But again it is important to the extent that we've also asked the Government Accountability Office to identify anything DHS may be doing to ensure that commercial databases containing private information are secure. So we're kind of looking at it. But the best thing is to have people like you to help us look at the whole issue of privacy.

I expect this Committee to work closely with the Department and it's Privacy Office to make certain our government is doing all it can do to protect our citizens. I also hope that you will help the Department to better understand the intersection of privacy, Homeland Security, and technology. By doing so you can help strengthen the Department, its programs, and our nation. So I thank you for letting me come in. I know you have a lot of work ahead of you.

Privacy is important, but we still need to protect the homeland, and I know you look forward to your work. Ms. O'Connor as I indicated is as you know very capable of assisting this Committee, and her staff also. So we all look forward to working with you, the Homeland Security staff.

Just as a sidebar, we've already gone on a retreat as a Committee. Very few committees can actually last two days by themselves out in the woods, but we were able to do it, and we came back pretty much committed that the whole notion of Homeland Security is a bipartisan issue. And so we look at it this way, and look forward to working with this Committee and others in securing the homeland. Thank you very much.

MS. O'CONNOR KELLY: We are most grateful that Congressman Thompson was able to be with us today, and Congressman Cannon is on his way, he's been detained on the Hill, so I'm going to take care of a little bit of housekeeping for the room for the day. The first request is that you would either turn off or put your cell phones on mute so as not to disturb the speakers. I just did that myself, so I would ask that you do the same.

We have comment cards in the back of the room. At any time during the day if you want to pose questions to a panelist, ask a process question, or make a comment, please see Lane Raffray, who is in the back corner, he just waved, and he will give you a comment card and if you will pass it to the podium to make sure it's shared with the group.

We have also reserved 45 minutes at the end of the day, as was in the Federal Register notice, for the Committee to receive comments from the public. Depending on the number of comments, or commenters, we have we would ask that you limit your comments to two minutes. You may have a little more time depending on how many people wish to comment. A number of people have already signed up, but again if you would see Lane and the staff in the back of the room they can sign you up, give you a number so that we have people go in order, and that comment period is scheduled for I believe 3:45 this afternoon, so we hope you stay with us and share your thoughts with us. We want to see an open discussion and inclusive of all view points. We do think there will be time for people who have not signed up yet to make comments at that time. We will try to keep the

meeting as close to schedule as possible given the needs and timing of our speakers, but regardless of what time we stop we will devote the entire 45 minutes to public comments should there be any at that time.

We also allow written comments in the Federal Register as we mentioned in the Federal Register, and information on how to submit those comments can be found at the DHS Privacy Office website at wwwdhs.gov\privacy.

I think we have a little more time waiting for Congressman Cannon so I have indicated to the Committee that I think it would be worthwhile for each of you to say a few words and introduce yourselves to the public, and talk about why you are interested in being on the Committee, and what you hope to get out of it, or whether there are items you might like to see for your work in the coming year. And I'm going to start in alphabetical order if that's okay with you. And I think we've got a little time so take your time. We may interrupt if the Congressman arrives in the middle. Thank you very much.

MR. ALHADEFF: Thank you, my name is Joseph Alhadeff, I'm the -- my day job so to speak is I work at Oracle as the Chief Privacy Officer, and Vice President for Global Public Policy. And I guess one of the reasons I think participating is important is I guess I'll take a line out of the Gospel According to Congressman Thompson, which is that privacy and security don't have to be a balancing act. They can in fact be mutually reinforcing and technology plays a role in that, and that's one of the things I do in my day job, and I think it's one of the things that we can do better as a country, so that's one of the topics I'd like to be addressing, and one of the things I'd like to be getting out of it. Thank you.

MR. BARQUIN: I'm Ramon Barquin. I am a technologist, mathematician, electrical engineer. Many years with IBM, and have been. Over the last few years my day job, as Joe says, is building data warehouses and business intelligence systems. I have been also extremely, extremely interested and involved since graduate school days with what was then referred to as the social impact of computer technology. And on that note I have founded and still head the Computer Ethics Institute whose claim to fame is having issued the ten commandments of computer ethics. Not that anyone pays attention to them, but in any case -- In any case I look forward to serving with the other members of the Committee, and helping out in what is a really, really important set of issues here.

MR. BEALES: My name is Howard Beales. I teach in a business school at George Washington University in Strategic Management and Public Policy. I developed -- I first got interested in privacy issues during my tenure at the Federal Trade Commission as the head of Consumer Protection. I think -- and I think it's a very important and continuing and timely set of issues for us to be addressing. I guess I'm particularly interested in a lot of the security issues about information. It's something we made a priority in the time that I was at the Commission, and something the Commission continues to do, and I think where there's a really important role to play in trying to make sure that information is secure so that it can't be used inappropriately, and in a way that causes harm to consumers.

MR. FREEMAN: My name is Reed Freeman. I'm Chief Privacy Officer for Claria Corporation and an adjunct Professor of Law at George Mason University School of Law. I've been a privacy law practitioner for most of my career, and I'm delighted to serve because the opportunity to engage in public service within my practice area is a real honor, and particularly to be associated with such a distinguished group of experts is a thrill for me.

MR. HARPER: I'm Jim Harper, a Director of Information Policy Studies at the Cato Institute here in Washington, D.C., and editor of Privacilla.Org. The Cato Institute is known to many Washington, D.C. locals as a think tank devoted to free markets, limited government and peace. Privacilla is a web based think tank that covers privacy from top to bottom, including privacy from government, privacy in the private sector, financial and medical and on line. I suppose I am doing this because privacy issues are very knotty in themselves, and squaring privacy and security is perhaps an especially knotty problem that I'm very interested in working on. I suppose we could take it as our charge to see that privacy and security can both be had, but rather than an article of faith I think it's important that we make it actually happen.

MS. O'CONNOR KELLY: We are going to interrupt the introductions because Congressman Cannon has joined us. We are most honored to have Congressman Chris Cannon from Utah join us this morning. Congressman Cannon serves on the House Judiciary Committee and chairs the subcommittee on Administrative and Commercial Law. He is serving his fifth term in the House of Representatives, and he has a well known recitation for getting folks on both sides of the aisles to work on a number of thorny issues, including some affecting the Department of Homeland Security such as immigration, high technology issues, and anti- terrorism and legislation. He is also one of the key champions of the Privacy Office at the Department of Homeland Security and we are so grateful for his oversight and thoughtful leadership on our office's behalf. We have testified in front of his Committee a number of times and we are grateful for that honor, and we are grateful for his staff's work as well. And we are grateful that he is here with us today. Thank you, Congressman Cannon.

THE HON. MR. CANNON: I hate to have this distinguished Committee have to turn to this podium, but I guess we also have an audience, so I'll try and do both. It is a great pleasure to be here. You know, I was struck this morning by my first experience with a bureaucrat, and I thought it might be relevant here. I was in the Interior Department as a minor political appointee, had about a hundred lawyers reporting to me in the area of surface coal mining, which was a hot potato in 1984. And I got a piece of mail that was very important, and it had been in the House system, that is the Interior Department's offices, for three days before it got delivered.

And so the very first thing that happened the very first day I was there was this terrible frustration how could you have a letter in its system for three days. And as I was fuming a very wise senior bureaucrat named Ed Bonicam (phonetic) came in and sat down in my office and said, you know, the first thing political appointees also do is try and make the mail system better. And then we had this very pleasant talk about what made you an effective political appointee, or bureaucrat. And the answer is often just the recognition

that government doesn't do things very well very often. But that over a very long period of time we in America have decided that in some areas we will spend the overhead, and often compared to private industry that's a dramatic overhead, in doing things so that over time we do them better and make improvements. I suspect actually the mail in the Interior Department has improved in efficiency largely because of Federal Express has shown how you can handle mail, and then now UPS has its overnight service, and so I suspect that government tends to catch up, but that leaves you all in a very difficult position.

You're in the position of trying to figure out how we take a monster that has grown dramatically in size, overlaid with technology that is in some ways very frightening and in some ways sort of helpful. I mean, you know, who would have guessed 20 or 30 years ago that we'd be in a position today where a person on death row could be saved by face recognition technology of the fans at a football game. So this is not all bad.

I was thinking in the context of what my bone fides are, have to do what I do. Well I chair the Committee that has oversight. Cool, right? But my bona fides are probably, to a much lesser extent, a little bit like yours as I look around this group. Some of the very first PCs were made in my neighborhood, in fact some of my neighbors were the engineers who did some of those first PCs. In fact one of them actually achieved national status and ended going away when the Apple computer came out.

I mean I suspect that many people in this room actually remember the first Apple. I was astonished when I saw it. You know, what did it have -- like a 50 -- it was in the kilobyte range for that first drive. And I remember in Utah a few of my friends put together six PCs -- this was like major cutting edge stuff. I mean Novell was the company that actually networked PCs was a small client of the law firm that I left when I came to Washington, D.C. I actually didn't even know them at the time, but some of these guys who were the engineers I remember they actually put six PCs together and they were strung together back in the early '80s, and they were able to control a gigabyte of data. That was a major technological break through. And now today we have these iPods that have what -- I think 120 gigabytes, tiny hard drives. So we've come a tremendous way.

We have also in Provo, Utah where Novell sort of grew up, we had traffic problems and some fathers of the city who were wise enough to realize that if you could have cameras at every intersection you could deal with traffic much more efficiently. It's a long north/south city and so if you can time traffic lights you can actually move traffic better. And so virtually every traffic light in Provo, Utah, which is a hundred or hundreds, has a little camera on it. And that makes traffic move better, and that's really a nice thing. I mean it makes our lives better, right? And truly I would say that Provo has one of the best -- is one of the best cities for traffic. But it takes a picture of every single car that goes through those intersections every minute of every day. And so maybe if you are charged with a crime and can have access to that data, and it's not that difficult a thing I suppose, to figure out what license plates went through those intersections at what given time.

On the other hand if you are leaving your mistress's house, or in the case of women your friend's house, that could actually be an embarrassment, and it could be a significant embarrassment. And we find ourselves today in a situation where we have massively

accumulated bodies of data that can be used for many different purposes, and very few controls on those people. And I think it would be a little bit difficult to get that data for the intersections, and you've have to do some programming to get an algorithm that would identify the license plate but that's not very hard to do, most people here have had a little bit of experience with the technology that could probably do that. So what are we to do?

And the answer is, as I came over here and looked through the very impressive people who are sitting on this Board, I have great comfort. Our responsibilities are enormous. Many of you people have spent much of your lives dealing with these issues, and that's a great comfort. Some of us – in this audience, many people remember the debate over how a social security number could be used. We had, a couple years ago or three years ago national ID card as part of the Judiciary Committee, and I was astonished that only two people in that group actually were aware of the limitation on the use of a social security card. If you recall, the debate was will you have to use this card? And the answer was it will not be mandatory ever. Now how many of you guys have tried to see a doctor and said look, I don't want to give you my social security number?

Now, for most medical purposes, you need an identifier that allows the doctor to know what records he's dealing with, and knows he's not making a mistake. The relatively incoherent debate from the early '50s and '60s on these issues was absolutely uninformed by the concept of 120 gigabytes on an iPod. They were absolutely uninformed by that. And here we are with 9/11 and the need to balance these information issues with security.

And I would just like to leave you with a quote from Alexander Hamilton, whether you liked him or hated him, and he was certainly liked or hated in his lifetime, he was prescient, he was a brilliant guy. I was recently at a town hall meeting in my district and I asked people for their priorities in life, and one of them raised his hand and said getting rid of the Fed. And I said, you know, that may be a very important thing but I just don't have a clue how to do it. And afterward he came up and he pointed out that we had gotten rid of the fed two or three times in the history of America. And every time -- by the time I think the last time was during Andrew Jackson's presidency and resulted in an eight-year recession or depression in the country.

But the issues back there were the same as they are today when we're dealing with how we deal with money, not untied to what we're doing here, and the ability for a guy, a brilliant guy like Alexander Hamilton, to come up with ideas that affect us even today, is remarkable. You see that in the Federal Reserve process that evolved from the ground work he laid to his ideas about liberty.

And so if you wouldn't mind I'd just like to read this quote. "Safety from external danger is the most powerful director of national conduct. Even the ardent lover of liberty will after a time give way to its dictates. The violent destruction of life and property, incidents of war, the continual effort and alarm attendant on a state of continual danger, will compel nations the most attached to liberty to resort for repose and security to institutions which have a tendency to destroy their civil and political rights. To be more safe they at length become willing to run the risk of being left free." Now that is not inexorable.

Every problem that technology poses to us today all have another side, and that is the opportunity for limitations, thoughtful, appropriate limitations. Those institutions are not imaginable by any individual today, but by a group like you are not only imaginable but they can actually be put in place, and if the work is thoughtful it can be a foundation for even greater personal liberty, and ultimate limitations on government.

My hope, to quote another founding father, Thomas Jefferson was obsessed with the idea of a local government. Everything he wrote -- well, he had actually two purposes in mind on everything he wrote. The first was to assure his place in history as the author of the Declaration of Independence, and the second was to remind people that government at the very lowest level was the best kind of government. He used the term ward, and for him he was obsessed by the northeastern concept of political wards, which meant about a hundred families, based upon the concept of Deuteronomy by the way, where you have captains of ten and captains of 50 and captains of 100, and that is the system that the northeast had at the time.

He was astonished by the blockade of the Boston Harbor and the response of that social structure to help people in Boston. He was astonished by it and it directed the whole rest of his life. He tried to tell the southerners how it worked in the north, the northerners saying that's how we do it, they couldn't really see how you need to; while the southerners said well we don't understand, and so he never got very far, but he was obsessed with this idea.

Today we -- I'm not sure we use that idea, but today computing power gives us the ability to govern ourselves at an ever closer level to the local. And to control traffic in Provo. That comes with national implications and you are the brain power of America with the responsibility to help us create a foundation for how we use information that 200 years from now can be looked upon by our descendants and say wow, what great founding fathers of the concepts of individual liberty in a context of huge amounts of data.

I commend you, I appreciate your being on this Committee, we look forward to working with you. I'm the biggest fan of Nuala that ever existed, she's done wonderful things, and not the least of which is gathered together luminaries such as yourselves. We wish you the best, we hope for the best and we pray for the best on your behalf. Thank you.

MS. O'CONNOR KELLY: We'll continue with the Board introductions at this time.

MR. HERATH: Thank you. I'm Kirk Herath, Chief Privacy Officer and Associate General Counsel of Nationwide Insurance Companies. I'm responsible at Nationwide for all things privacy. We have approximately 40,000 employees and agents spread across the country, and we have some international operations as well. What I would like to do is be able to lend the Department of Security and the United States government my five years experience building what has become a very successful privacy program at the corporate level. I think there are a lot of similarities and corollaries that I can provide as examples. I'd also like to say that despite all of the press surrounding this Committee I was not named in any article. So as a local government official, as the Congressman said, I can tell you I

know what it's like to be attacked in the press. So I was happy to see that I was absent from the press this time. Thank you very much.

MR. HOFFMAN: Hello, my name is David Hoffman. I'm Intel Corporation's Director of Privacy charged with the responsibility of providing reasonable privacy protection for all of those with whom we do business. I'd like to thank Chief Privacy Officer Kelly, former Secretary Ridge, and Secretary Chertoff for this incredible opportunity to serve the United States and to serve the United States people. It's a true honor to serve on this Committee with my distinguished colleagues, it's an incredible group of people that's been assembled and I feel confident that we as a Committee can also provide guidance so that the Department of Homeland Security can accomplish what it needs to do while providing reasonable privacy protection for the American people, and all of the people for whom it will collect data.

MR. HOFFMAN: Good morning. I'm Lance Hoffman, Distinguished Research Professor at the George Washington University in Washington, D.C. I'm a Professor of Computer Science. I also run GW's Cybercorps Program, a federally funded program that trains undergraduate and graduate students studying computer security from various fields, forensics, computer science, business and so forth. I taught one of the first computer security courses back in 1970 at the University of California Berkeley, I think it was the first computer security course in a regular four-year institution. I'm honored to serve on this Committee to hopefully strike the right balance between privacy and security, and hopefully we can have both. I was struck by the remarks of Congressman Cannon. You know, it will be very important to help set a course for DHS and hopefully other agencies where people can look back 200 years from now and say they got it right.

MS. LEMMEY: I am Tara Lemmey. I am the CEO of a firm called Lens Ventures. I work on the future. Our company works on innovation three to ten years out. Relevant to this Committee I started four technology companies starting in the early '90s and some of the first ones that I was working on really led me into dealing with the privacy issues around data which helped me be on the founding Board of TRUSTe, and then eventually become the President of the Electronic Frontier Foundation for a period of time. I currently co-chair the technology group of the Markle Task Force on National Security, and I think through both the work in the private sector space as well as the security work what I've learned is that as we lean into the technology to optimize the systems we're also going to have to lean into the privacy issues to deal with both of them. The good news about it is the same things that are going to allow for us to use technology for security better, such as audits and efficient use of data and protection are the same things that we're going the lean into on the privacy areas. I think it's going to be a very exciting time for all of us, and this Committee has a very good set of minds to work on this issue.

MR. LEO: Good morning, my name is Joe Leo. I'm a Vice President with Science Applications International Corporation. Prior to working with SAIC I was a Federal servant for over 30 years. My last position was the Chief Information Officer for the United States Department of Agriculture. By way of background for the old hands here I'm one of the founding fathers of Electronic Benefit Transfer for the Food Share Program, and helped the leadership to convert the entire paper based three billion pieces of paper into

today it's all done electronically. Of course the issues of privacy and security were prevalent then with regard to over ten million households at that time in the Food Share Program which had moving from paper to a card, and what were all the issues including the issues I had the debate on the forerunner of a national ID card, and whatever. So I hope to add a pragmatism to the discussions and look forward to joining my colleagues in this very, very important field. Thank you.

MR. MARSH: My name is Jack Marsh, and actually I'm a country lawyer from Virginia. We are very, very fortunate to have the leadership of Mrs. O'Connor. I've had an opportunity to observe what she's done and the enormous strides she's made in addressing this issue. I teach law at George Mason University. We are engaged in a sort of pioneer experimental effort to develop programs that relate to cyber security terrorism, national security law, individual rights. One of our key leaders is here, Lee Zeichner. I just saw Lee walk in. Served in the Congress for eight years, member of the Appropriations Committee, then went over to the Executive Branch of government and was the National Security Advisor to the Vice President, and then at Mr. Ford's request, with whom I served in Congress, who had chaired the reorganization and formed the American Intelligence Community in the 1970s, which gave me an insight to the different dimension of privacy, which is a very important one. I look forward to serving on the Committee. In observing privacy I point out to our students that without liberty there is no privacy. So really the balance is between security and liberty, and liberty gives us those rights of privacy which are so essential to our society. And I think the law is very evolutionary, information technology is very revolutionary, and there is tremendous technological lag on the side of the law, but this sort of organization here I believe can address some of those issues that are so vital to our society.

MS. MCNABB: My name is Joanne McNabb. I'm Chief of the California Office of Privacy Protection in the Department of Consumer Affairs. This is a four- year old office that was born as one of the many pieces of legislation on privacy that have come out of California in the past few years. We've had a lot of experience in California in addressing the privacy issues that this Committee will be addressing, such as ID theft, information security and breaches thereof, medical privacy, financial privacy, and I'm very pleased to have the opportunity to share whatever might be relevant of our experience with this organization, and I very much look forward to learning from this Committee things that I can take back to California to improve our work there.

MR. PURCELL: Good morning, my name is Richard Purcell. I'm the head of a small consultancy firm called Corporate Privacy Group. I'm also the chair of TRUSTe, the online web seal organization. Through our work, both in our consultancy, through TRUSTe, and my former work as the Chief Privacy Officer of Microsoft, we've tried to demonstrate an ongoing commitment to personal dignity through respect for, and protection of, personal information. I'm delighted and honored to join my colleagues here in promoting a national standard of care for continuing this unique experiment of the American culture in both promoting personal liberty in a context of national security.

MR. PALMER: Good morning. I'm Charles Palmer from IBM Research Division where I'm the Director of Security Networking and Privacy Research at that lab as well as some

of the other labs around the world. I'm both honored and awed to be on this Committee surrounded by people who've been working in the public eye, or at least in the public interest, for a very long time. I see my role here as less of a policy person and more of a technology policy person, and that is technology is often seen as the solution to many of our problems. Technology always has two sides, the good side and the dark side. And we hope to make sure we can balance the technology that we have today and talk about the technology that we may have tomorrow.

MR. ROSENZWEIG: Good morning. My name is Paul Rosenzweig. I'm a Senior Fellow with the Heritage Foundation, another one of the proliferation of think tanks here in Washington, D.C. I'm very honored to be a member of this Committee. I am here principally because I think that the issues facing this Committee are amongst the most important facing the country today. To be sure our Congress has many things on its plate, the reform of Social Security, raising the tax rate, and all that, but I think accommodating legitimate security needs while remaining respectful of, and cognizant of, the vital liberty and privacy interests that make America what it is, is perhaps the single most interesting and important question facing the country today. So I'm quite pleased to be able to participate in the discussion.

MR. TURNER: My name is Michael Turner. I'm the President of the Information Policy Institute, and that's think tank in New York City making us somewhat unique in this group. We are the only think tank that is dedicated exclusively to the study of information regulation, broadly defined. Our organization engages in thorough empirical studies and therefore we don't have an inordinate amount of through put on the topic because the studies we do by definition necessarily take quite a bit of time. Nonetheless I've been engaged in really studying the relationship between technological change and regulation and institutional reform for the past 15 years, the bulk of the time in the telecommunications arena, coming to privacy really in the late '90s when, again, technological change thrust the issue of privacy back into the fore with the advances in computer and communications technologies. I think there are an enormous number of issues that this Advisory Committee needs to focus upon, notably the exchange of data between the private and public sector, and the thorny issues associated with that data exchange. The international dimensions of this issue because, you know, much like Diogenes this group can't operate in a barrel, the consequences of the work that the DHS Privacy Division undertakes are going to be felt worldwide, and also finally the three components that this Committee has to focus on, not only is data privacy and data security, but also data integrity that hasn't been mentioned yet, indeed accuracy, and those are very fundamental for this group. So I'm honored to again be affiliated with Nuala, with whom I've had the privilege to work in various capacities over the years, and have always admired her ability to bring focus on issues that others can't identify, and to work with the group to generate very positive results.

MS. SOTTO: Good morning. I'm Lisa Sotto. I'm a partner in the New York City office of Hunton and Williams, and also head the Regulatory Privacy and Information Management Practice with the firm. Unlike Professor Marsh I am a city lawyer, and I assist companies in building best privacy practices into their programs from the start, and I hope to be able

to transfer some of those skills to this Committee, and I am both honored and humbled to serve with such a distinguished panel. Thank you.

MR. SHEEHAN: Good morning. My name is Jim Sheehan. I'm a Vice President and General Counsel of a residential school in Hershey, Pennsylvania called the Milton Hershey School which serves the needs of economically and impoverished -- economically needy and socially needy children from K to 12. I truly am a small time, small town, lawyer. I bring to this Committee hopefully some modest analytical skills and open mind, and a profound interest in the subject. I am honored and humbled to be a part of this Committee which I think is going to be addressing one of the country's most significant issues for the next decade. Thank you.

MR. SABO: I'm John Sabo, a Director of Security and Privacy Initiatives with Computer Associates International. Internally, I do a lot of work working with our corporate compliance managers and legal people, as well as our brand and development teams who build software products which help support security and privacy controls. My background that I guess partly brings me to the Committee, I worked for 23 years at the Social Security Administration and the last decade created the Social Security Administrations online services program, bringing, you know, the web to the 40 to 50 million beneficiaries of the agency but also getting into controversial issues as we began moving into online services and addressing the challenges of identity management. And that created some very public attention to that whole issue of identity and privacy back in the late '90s. I moved on to the private sector with Computer Associates five years and what I do in addition to the internal work is I represent the company in organizations that focus on security and privacy. I do a lot of work now on critical structure protection, but also with an organization International Security Trust and Privacy Online that is focusing on how IT architects can help implement privacy controls. A couple of things also, I've been a member of the Information Security Privacy Advisory Board, which is a NIST sponsored Board and my term is ending, and we've done a good amount of work on privacy the last several years, but that Committee does not have the attention that this Committee does just because of the nature of DHS, and yet some valuable work has been done there.

My particular interests, and there are many, is peeling the onion on privacy is a complex thing, but the use of private data mingled with, and in conjunction with, public data along with algorithms to make decisions affecting citizens and visitors to the U.S. is an important area because of what was mentioned earlier, data integrity and the validity of the algorithms. The other thing is the whole range for information practices that are embodied in the Privacy Act of 1974, and other statutes, most of those practices do not get attention by government systems, and I think that's an area that DHS can look at. And that leads a little bit into an examination of the adequacy of the Privacy Act and perhaps the need for, as someone said earlier, a sort of code of conduct for privacy that may go beyond what the Privacy Act requires.

MR. WRIGHT: Good morning. My name is Sam Wright, I'm a Senior Vice President of Cendant Corporation. It's truly an honor to serve on such a distinguished panel with such an important issue to wrestle with. And one that we need to get right the first time. This is not -- I don't think we have the opportunity to have several bites at this apple.

My purpose in wanting to serve on the Committee was to be able to do whatever I could to make certain that the acts of terrorism both here in our country and abroad did not result in a change in the way Americans go about their daily lives, and go about the way that our forefathers have conducted their lives. I think that if we develop into a system where people are afraid to travel, the terrorists have won. I don't think that's right. If we result in a system that significantly impinges upon peoples' privacy and other rights, the terrorists have won as well. So my purpose in serving on the Committee is to try to avoid either of those two results. Thank you.

MS. O'CONNOR KELLY: I want to thank all the Board members, and let me also say thank you to the members of the public who are here today. We are honored by your interest and your time with us today, and we are very grateful for that. Let me also thank the members of the Board. We had an overwhelming response from a wonderful applicant pool, so much to choose. We respect that you are taking time out of your busy schedules and your professional lives to be with us and to devote your energies on behalf of your fellow citizens to the Department of Homeland Security, and for that we thank you as well.

Just a moment of a process, the reason I am moderating today is not because I am on the Committee, but because the Committee has not yet selected a Chair and a Vice Chair, so because my office put together this first days program and we are most familiar with who is speaking at what point I will serve as the moderator for today only. In the future the Chair and Vice Chair will run the meetings, which will be, as you know, public. I also want to note again that comment cards are available and they can be handed to Toby Levin from you office who's here in the front row, and Tony Kendrick who is behind me, at any point during day and we'd be grateful for your comments, and also for your participation in the afternoon public comment session.

At this point I'm switching roles to actually report to the Committee on behalf of the Privacy Office, and I am reminded of something that Secretary Ridge said to me early on in our tenure at the Department, which is just because we have a serious mission does not mean we always have to be serious, in fact we had many laughs in the first year or two of the Department, we had to laugh, if any of you have seen our office space you would laugh as well. But we have had a tremendously good time and done some very, very hard work.

And so I wanted to share with you a very embarrassing story about myself, and I'm sure Maureen Cooney is rolling her eyes right now thinking where is this woman going with this story. But this morning at about 5:30 I cut myself shaving, and for those of you who are wondering what I was shaving, it was my knee. And here am I running around my bathroom with blood pouring out of my knee, and a little tissue stuck to my knee going where are the bandaids in the dark. But just so you should all know that we all seek humility in this office even though we have great champions on the Hill and elsewhere in the press and in the country, we are all fallible and that is why we have created such a stellar Board of experts to bring us great thinking, and to formalize our relationships with the public to bring your thoughts and your concerns about the Department, but also the best learning and the best practices from the private sector. And the little shaving story also reflects the fact that I was a little nervous myself because I am here to report to you about my office and you are, as we say in the private sector, the shareholders, the stakeholders,

you are our bosses and so I hope you are pleased with, and find satisfactory, our report on the state of the office, which is strong.

I am incredibly proud of the work that we have done at the Department of Homeland Security Privacy Office in the first two years of its existence. The Department's office was opened on April 16th, and that's because that's the first day I started work by myself in a empty office building with a bunch of other senior leadership, some of whom you will meet today, and we have grown our office to I believe a tremendously strong and almost a model office for other federal agencies as well. We've modeled this office on the structure of privacy offices in the private sector, including one that I started at a high tech company a number of years ago, and we have technologists and lawyers and business people and program analysts, and people who delve into the work of the Department and help the Department run. We oversee privacy impact assessments and Privacy Act compliance as well as the Freedom of Information Act, which was re-delegated to this office in the summer of 2003.

We are incredibly proud of the work we've done to help the mission of the Department, but also to question that mission when we think it delves too much into the personal information of the individual. At this time I'd like to introduce a few of our senior staff members. Maureen Cooney is over here to my left, our Chief of Staff and our Senior Advisor for International Privacy Policy. Maureen was one of the first people to join our team from the Federal Trade Commission, and those of you who work on international privacy issues know her well from her work there.

Elizabeth Withnell is our Chief Counsel. I think she is behind me. Liz joined us from the Department of Justice and I think she is actually the second member on the staff early in 2003, and she's served as our lead lawyer for the Office, and with all due respect to the Office of General Counsel, and my dear friend Joe Whitley, to whom she reports, we think of Liz as one of our own. She oversees Privacy Act compliance as well, and a number of other incredibly important privacy issues.

I am also very pleased to announce that Toby Levin as joined us as our Senior Advisor. Toby Levin is another wonderful and senior leader from the Federal Trade Commission, with due apologies to Commissioner Swindle, who has just joined us, we are most proud that Toby has joined us to help us in particular work on our investigations and reviews of Departmental programs, and I hope we'll be seeing some great written work and reports on the status of Department in the coming months.

Tony Kendrick, again behind me, is our Director of Departmental Disclosure. Tony oversees our FOIA program for the Department. As you all know the Department combined 22 former separate agencies and created a handful of new ones, each of which has their FOIA program and he oversees the work of over 430 Privacy Act and FOIA compliance people. Catherine Papoi is our FOIA Specialist and she will be joining us in just a few days working under Tony.

Peter Sand is our Director of Privacy Technology. Peter is behind me as well, and he joined us from a state agency where he was Chief Information Officer and Chief Privacy

Officer. And again he brings the technology as well as a legal focus to the Department, working particularly with our Science and Technology Director as well as our Chief Information Officer.

I cannot begin to thank enough Becky Richards. She is behind me, please stand up. Becky is our Director of Privacy Compliance. She also serves as the Executive Director of this Committee and is the reason why this is as well organized and well run a program as I think I've ever seen, and we are most grateful for her work. Becky came to us from TRUSTe, the online privacy seal program. I have a lot of people to apologize for stealing their staff I have to confess, but we again have put together a terrific operational team.

John Kropf, who is directly across from me is our new Director of International Privacy Programs. John has joined us from the State Department, and is a very senior lawyer -- was a very senior lawyer there, and we are so grateful that he has just joined our team within the last few days.

Lane Raffray, in the back of the room I believe, has just joined us as a Policy Analyst and he will be helping out on a number of programs including our investigation and report writing with Toby, and we are delighted he has joined us as well.

Sandra Hawkins, I stole her from my time at the Department of Commerce, is our Administrative Officer -- yeah, I just did that, sorry. We are delighted that Sandy is part of our team. She keeps the trains running on time and she is an incredible addition to this office. I also need to -- there are a number of other people I'm sure I'm forgetting, but I need to thank Robyn Kaplan and Nathan Coleman from SRA who are on Dan Chenok and Jill Rhodes' team there, and the support from the SRA team for making this meeting possible.

We also have a number of DHS Privacy officers in the components. This was part of our vision when we created the office was that it would not be only headquarters driven, it would have Privacy Officers in each of the operational units who sat with this program staff day to day to really impact their decision making at the very earliest stages of technology, its development, of procurement, and some of our stellar folks on that team include Steve Yonkers, who's behind me, the Privacy Officer for the U.S. VISIT Program. Steve has built a tremendous team and has done education and training and compliance audits across that agency, across that program, that has made it really a model for the rest of the Department to follow.

Lisa Dean, who I'm not sure is with us today, is the Chief Privacy Officer at the Transportation Security Administration. Again a courageous woman who like myself as some others in this room went into agencies or organizations that had some challenges to try to help change the face of that agency, and she has done so with tremendous success.

Andy Purdy, our Privacy Officer and Acting Director of the National Cyber Security Division has an incredibly important job, he's over here to my left, working on our cyber security and privacy issues which of course many of you are well familiar with. And

Elizabeth Gaffin, the newly named Privacy Officer at Citizen and Immigration Service, who I do not believe is here today, but we are delighted to have her on the team.

As I said the office is nearing its two-year anniversary, you'll see our first annual report came out much earlier this year and it's in the back of the room. I've told you a little bit about the structure.

Now the mission as we envision it is one that is not antithetical to the Department's mission of securing our homeland, but one actually that is core, that is central to that mission. As both Secretary Chertoff and Secretary Ridge before him articulated his vision for this Department it is one that protects families and freedom, one that protects both lives and liberties, so we are core and central to a protective mission which is that of the Homeland Security Department. We do not perceive ourselves as getting in the way in the slightest, but rather as facilitating that mission by making sure that the programs get this issue right from the beginning.

I think we've demonstrated some business success in that area with programs again like U.S. VISIT and some others that have considered privacy at the earliest stages. And programs that also have considered privacy in their procurement, in their requests for proposals, in the very process of money, as one of our law professors said follow the money, and that is a great way to attach privacy as a value to the very structure of this Department by attaching that value to the procurement of large contracts from the private sector, and we are proud to have done that with U.S. VISIT.

A few of the hot issues that we are dealing with in the Department and in our office in particular, obviously international privacy is a key focus for the Department. We have -- we collect and we use and we retain data from citizens of other countries, and the legal structure in this country is one that does and does not consider those issues in varying strengths. We have again -- Maureen started out as our International Director and now John is taking over part of those duties, and we will continue to have important conversations with the European Union and other parts of the world on the dissonance and the concordance of our lives and theirs.

In addition obviously technology development is a key component of our analysis by the Department. The use of biometric technology and in particular data collection technology is the key reason I think this Department -- at least the office exists in this Department, and it is part of our statutory mission to review the use of any new technology by the Department before it is employed.

And lastly, as I think Michael mentioned, data integrity, and the sources of data I think is probably the most compelling public policy issue that continues to face our Department and our office, and that is how we find data, how we use data, and particularly how we import or do not import private sector data into the government's base for the use in credentialing and analysis in terrorism prevention.

We want to harness the best language, the best thinking, the best resources in the private sector, but we want to place constraints on that information, on that technology, that are

thoughtful, that are useful, and that both facilitate the Department's mission but also constrain its impact on the individual. I'm proud of the work that we've done so far and I'm grateful for this Boards' efforts towards overseeing my office, and the Department.

At this time I would like to turn to the issue of appointing a Chair and a Vice Chair for the Committee. I have spoken with a number of members of the public, and a number of members of the Board about the need for a Chair, and two names seem to resonate again and again. I would like to put forward the names of Paul Rosenzweig and Lisa Sotto who are members of the Board. Paul, as he mentioned is affiliated with the Heritage Foundation and he is also an adjunct professor of law at George Mason University. He has written extensively on the Department, on the issues facing the Department, and he has both offered supportive and also critical thoughts on the Department. Lisa Sotto, again a partner at Hunton and Williams, and also a member of the Center for Information Law Policy Leadership, has written again on privacy law in the United States, and has spoken both thoughtfully and positively and negatively about the Department and its mission.

I would like to say, hopefully without divulging too much personal information about Paul and Lisa, that we have in the team a Democrat and a Republican, a liberal and a conservative, a male and a female, a representative of Washington and New York, two cities very much affected by 9/11. And I think they would bring viewpoints that are both divergent but also thoughtful, critical and respectful of the work of the Board and the work of the Department.

I'd like to ask first Paul and then Lisa to make a few remarks about their thoughts on undertaking this assignment, and then open it up to the Board for discussion.

MR. ROSENZWEIG: Well first off, I am as honored as I was to be named to this Commission. I am even more honored, Nuala, that you would think me capable of chairing it. I am somewhat skeptical of your judgment in that regard but I do thank you for thinking of me, and if my fellow Committee members are interested I would be pleased to serve in that capacity. The reason we are here we've already alluded to in a number of instances. There are a series of challenges facing the Department of Homeland Security and more broadly the country in trying to both assess new technologies as they come on line, and their effect on essential liberties that Americans cherish deeply.

That challenge provides us I think with a very great opportunity which is to say that as I survey the policy development area now with the possible exception of the Markle Task Force, which has done some extremely excellent work, there is no group convened in a regular manner to consider thoughtfully and extensively the issues that face the country in balancing liberty and security. I promised myself I wouldn't say "balancing" but it seemed to fit in there, because I share Congressman Thompson's vision that our objective should be to maximize both values to the extent possible and make trade offs only when we realize that they cannot be both achieved.

More importantly I think that the most significant function that this Committee can serve is to open up those trade offs to public discussion and consideration. The single most significant criticism I think I would have of the Department in the past few years is that to

a large degree the necessary trade off questions have been made implicitly; that has improved a great deal in the last year or so. But at least initially there was a sense that those decisions were being considered but not in ways that exposed the reasoning and decision making to public consideration.

I think our great opportunity here is to serve as a public forum for the discussion of these important issues. I would hope that the Committee would continue in the practice that Nuala has set up for today of being inclusive in opening up our thinking and our processes to members of the public, to others who are concerned about the issue, to others who have thought deeply and long and hard about the issue.

I think our greatest challenge as a Committee would be to focus those discussions, which is to say that we've already heard -- I had a list about eight or nine separate instances in which the privacy technology, or liberty technology, comes together, whether that's a question of biometric face recognition alluded to by Congressman Cannon, or the data integration issues and data management issues and data integrity issues that we've talked about. So I think the biggest challenge, especially for today and for the very beginning of our work, is to focus our agenda and then determine how it is we're going to take what we learn and present it in ways that actually advance the ball.

A lot of brilliant discussion without any set of concrete recommendations would to my mind be a missed opportunity. I don't know yet how we're going to synthesize the product of our deliberations, the charter that we've been given seems to me to leave it pretty much carte blanche for us to figure out how we want to proceed. And I hope that in learning about DHS today, and hearing from members of the public about what their vision is for us, we can, following this meeting, make our own plans in a more systematic way determining whether we're going to address questions by technology or by program for example.

Whether we're going to be broad based and cross cutting or narrowly focused. I confess I don't know the answers to those yet, but I think that it is an important first step in what we will do. People who -- I'll conclude by saying people who talk about the privacy policy issue here in Washington are often given to quoting Ben Franklin, you know, “they that give up an essential liberty in return for temporary security to serve neither liberty nor security.” And that's a great aphorism, and we've all heard it, but the hard question is figuring out which liberties are essential and whether or not the security gains are temporary or permanent. And that's a deeply intractable question that requires case-by-case analysis, and a lot of hard work.

And I'm really pleased to be offered the opportunity to Chair the Committee that will I hope dig in to the elbows and engage in that hard work on a really detailed and thoughtful level, and thus communicate sound concrete advice to the Department as well as contributing to the education of the public on the difficulties and necessary problems -- necessary systems for addressing problems that the Department is going to develop.

If we do that, if we do that open to the public, and if we do that in an independent minded way that both praises the Department when it deserves praise, and critiques the Department

with constructive criticism when it deserves that as well, then I think we will be a success and that would be my goal for this Commission.

MS. SOTTO: As a less skilled impromptu speaker than Paul I have prepared remarks that I'd like to share with you, but first let me clarify, I am the woman.

This Committee is charged with advising the Secretary and the Chief Privacy Officer on how the Department of Homeland Security can establish a proper balance between privacy and security. This is a vital task, but for me it's more than abstract or theoretical. I come to this Committee with a personal history that gives real meaning to these words, and that inevitably directs my vision as to the responsibility of this Committee.

I lost my brother in the World Trade Center, my brother-in-law, sorry. As a result I understand in a more intimate way than many that America's physical safety is essential. The afternoon and evening of 9/11, and the days that followed were beyond imagination to those who lived those moments as my family did. For me our national security will never be a political issue. How can it be when real lives, real people are at stake. I understand first hand the effects of terrorism and so I also understand that it is incumbent upon our government to make every reasonable effort to ensure our safety. We cannot allow our security to be compromised, we cannot fall short. But we also must not over reach.

As the daughter of a Holocaust survivor I understand that there must be rational limits on how information about individuals may be used in the name of national security. There should be a direct demonstrable correlation between the collection and use of personal data and the prevention of terrorism. My father's horrific experiences during the Holocaust, and the ultimate price paid by most of his family, imbued me with a deep understanding of how information that may be gathered for seemingly neutral, or even beneficial, purposes may also be used to quash the very freedoms that we seek to protect.

Our national security must not come at the ultimate cost of a loss of the freedoms that we as Americans so cherish. I firmly believe that we must not, and that we do not, need to choose between our safety and our constitutional rights. We can have security without surrendering our privacy. This requires carefully tailoring information collection and analysis methods. It requires building in privacy from the start. It requires careful and responsible oversight, and it requires strong measures to protect against mission creep, and to enhance public confidence.

To put it bluntly we must protect security so that no one else has to endure what my family suffered on 9/11. But we must do so only in ways that are consistent with the American values that my father and so many others like him sought in their journey to this country.

I look forward to working with the members of this Committee, the staff of the Department of Homeland Security, and the public to pursue this vital objective. As someone intimately familiar with the dangers of failing to guarantee either national security or privacy I can think of no more important undertaking. Thank you.

MS. O'CONNOR KELLY: Thank you so much Paul and Lisa. Is there any discussion about this?

MR. HARPER: I wanted to ask the both of you that sort of vision question which you both referred to I think somewhat. Our system of government uses contests of power very often to try to reach the right decision or the best possible decision, federalism pits levels of government against one another, separation of power pits branches of government against one another, and the litigation system, for example, pits parties against one another. And in that crucible comes the truth or the best approximation of it, best policies possible, so I'm curious about your vision for this Committee.

Would it be to act as a privacy advocate and sometimes push back against the Department of Homeland Security's other branches, or is our role more to find a synthesis or balance in a neutral way?

MR. ROSENZWEIG: I guess my answer to you, Jim, would be neither -- or both if you prefer. As a - - no, no, I mean I know that that's funny, but as an Advisory Committee, you know, our role is statutorily charged under the Federal Advisory Committee Act, which is to provide advice to Nuala, and through her to the Secretary. I fully anticipate that in many instances that advice would include you really have missed something here, include this. That would be privacy protective level -- that would enhance privacy protections within the programs that they are considering.

I particularly think that constructive criticism from the bully pulpit to which we've been advanced here can serve a really positive tool, serve as a really positive tool for the Department by assisting them in advancing the missions that they perceive in ways that do not infringe upon cherished liberties. I imagine that in some instances we would actually wind up commending them for having adequately or appropriately taken into account privacy.

To characterize us as a pure privacy advocate strikes me as assuming that privacy is always the trumping value. In many instances I think it will be, in other instances I can imagine that our analysis of the program would suggest that privacy is being well taken into account.

So I think that the fact that there are kind of a hundred and twenty people in the room listening to us suggests that our thoughtful recommendations will have a great deal of sway if only because we've been given the opportunity to give voice to them, and I think in that regard the Department is to be commended for creating this Committee because in many ways having created us they lose a little bit of control over us.

Our mission I take it would be to take that and bring together the very, very brilliant minds around the table who understand these problems, you know, probably a lot more deeply than I do, and work to be constructive where we can, and to be condemnatory where we need to be. I don't know if that answers your question.

MS. SOTTO: To add to Paul's remarks, I would hope too that we would not serve as a rubber stamp to the Privacy Office at Homeland. Now having said that I don't view the Privacy Office as a place that rubber stamps the security programs of Homeland Security. I think there are enormously thoughtful minds at work in that office, and certainly around

this table such that to the extent that we find that there is a program that needs deep questioning with respect to its privacy values, and whether the program has built-in privacy protections from the beginning, consideration of a program, I would hope that we would in fact strongly challenge and if necessary condemn actions that we don't view as appropriate.

MR. SABO: Just a comment. Having served on ISTAP perhaps Joe Leo would have similar views, I think it's tremendous to have good leadership and I think the candidates are superb for this role, I think some of the most important things are being able to get the right set of facts on the table, the focus where necessary to have good staff support to help the Committee bring -- synthesize and bring focus to its work.

And I think one of the most important factors given the visibility of this Committee is the ability of the Chair and the Co-Chair to help the Committee reach consensus on issues, and to move beyond what could be widely divergent views, and to bring us together so we can actually move the ball forward. And I think one of the worst things would be to not bring that focus, and not really marshal the efforts and the thoughts of the Committee to move forward collectively.

So I think those -- the consensus building and the ability of the Chair and the Co-Chair to move the agenda forward and to schedule meetings as necessary to form the right sub committees would be really critical.

MS. O'CONNOR KELLY: Additional comments?

MS. RICHARDS: As Executive Director of the Committee I move to ratify the Chief Privacy Officer's appointment of Paul Rosenzweig as Committee Chairperson, and Lisa Sotto as Committee Vice Chairperson for one year term. VOICE: Second.

MS. RICHARDS: All in favor say "Aye."

COMMITTEE MEMBERS: "Aye."

MS. RICHARDS: All not in favor say "Nay."

COMMITTEE MEMBERS: (No response)

MS. RICHARDS: Hearing no objection I announce --

MR. ROSENZWEIG: Can I be registered as abstaining?

MS. RICHARDS: Paul Rosenzweig has abstained. Hearing no objections I announce Paul Rosenzweig as Committee Chairperson, and Lisa Sotto as Committee Vice Chairperson. Congratulations Paul and Lisa. (Applause)

MS. O'CONNOR KELLY: We are running almost on schedule so I'd like to ask everyone to just take a ten-minute break and get back to the room as close to 10:00 as possible. Thank you.

(Whereupon, there was a brief break.)

MR. ROSENZWEIG: Before we begin, Kirk, I'm pleased to tell you that I've taken care of the first problem that you had, which is there is coffee in the Delaware room.

MR. ROSENZWEIG: So my first act as Chairman was a success.

MS. O'CONNOR KELLY: It's my great pleasure to introduce one of my new bosses. Deputy Secretary Michael P. Jackson was confirmed as the third Deputy Secretary of the Department of Homeland Security on March 10th, of 2005. As Deputy Secretary Mr. Jackson serves as essentially our Chief Operating Officer with responsibility for managing the day-to-day operations of a Department that is over 180,000 employees strong.

Most recently prior to the Department of Homeland Security Mr. Jackson served as Senior Vice President of ACOM Technology Corporation. He was responsible for ACOM's government relations globally and served as Chief Operating Officer of the Government Services Group. Previously Mr. Jackson has had quite a career in government serving as Deputy Secretary of the U.S. Department of Transportation from May 2001 to August 2003 where he focused on DOT's response to the terrorist attacks of September 11th, including establishing the Transportation Security Administration, which is now part of the Department of Homeland Security.

We are most grateful that Deputy Secretary Jackson will make remarks to the Committee today and answer questions from the Committee. Thank you.

MR. JACKSON: Thanks, Nuala, and thanks for what you're doing here, and thank you for the work in organizing this important Committee. I have a very simple message, I've already said the words and I'll repeat it a number times as I go through here. It's thanks.

This is such an important area for us to understand well and to nail right in the work that we do at DHS. And this group gives us a tremendously strong tool to draw upon from a broad base of people with the diversity that each of you brings to this topic, this conversation. So I just really want to say on behalf of the Secretary and myself how important we think your work with us will be, and how grateful we are for you coming to do it.

I especially want to say to Paul and Lisa that I'm grateful for your roles in helping to herd this parade, and for the work in advance that we're going to extract from you in this role, so thank you very much. I know you are going to hear from my colleagues, a number of whom are arrayed before you in the front row and who will come and talk in a lot more detail than I intend to do about our Department, because I think the first step along this process is we want you to understand our Department as we understand it ourselves to be deeply imbued with our sense of mission in the importance, in the fervor, that DHS brings to the job that we have before us. And to understand the complexity of what we're trying to accomplish, what we're trying to do.

I will tell you I just think I have the greatest job in government to work with the colleagues at DHS that I'm now allowed to work with, both the guy above me and the tremendous

number of committed people at DHS, the men and women who do our job. It's one of the tremendous challenges to take on a complex mission, but it's made so much more enjoyable and pleasant and possible because this is really a Department where people don't consider the work that we do every day as some sort of government business as usual. This is not about showing up and punching a time card, it is about doing these critical tasks that are so important to the nation's security.

And I was one of those folks holding a government badge at DOT, as Nuala told you, after 9/11, and my life and commitment to public service was unalterably changed by those days, weeks, months and years after 9/11 and the work that we did in the government. So security is this tremendously motivating principle that animates, I think, this entire great DHS team.

But I will tell you it's not enough to be single threaded, the very nature of our mission is so complex. Just take the Coast Guard for example, the Coast Guard's mission on the national security is indispensable part, an indispensable part of what we have to do on the counter-terrorism front. But they also have tremendously important roles in search and rescue, saving lives. If you've ever had any interaction with the Coast Guard and you see these young men and women who jump out of an airplane and pull, as a rescue swimmer, somebody in from a sinking boat, and I've had the grace to meet a number of them, they just sort of, you know, get up from one of those exercises and brush themselves off and say gosh, that was a lot of fun, can I do this again tomorrow. And that's really the spirit and the complexity of our mission as this diverse portfolio of things that have been merged together from 22 different agencies. So in the Coast Guard's case search and rescue, environmental work, work they have on fisheries, and the counter-terrorism mission, work in support of national defense, they're there standing watch in the Gulf today as part of the Iraq effort.

So if you just unpack our agencies they all relate back to this core mission, but they each bring a sort of diversity and complexity of mission. So where do you come in this? This is our Department's mission in the counter-terrorism world and particularly is about finding a balance, a reasonable balance. It is about finding a balance between security and freedom, or security and mobility, and balancing the principles and the convictions of this nation that are supposed to be worked together to reconcile what is the right approach to take on these security and counter-terrorism missions.

So that's where the work of you will come into play in a decisive way, because we have to fuse a culture around finding the right balance, making prudential judgments, and these are almost always, you know, not black and white, not simple things, yes, do this this way, or that that way. They often find in some of the core programs that we'll be bringing to the table to ask your counsel about you have to take your life experience and throw them against the problem and see how to shape and form what we're up to. This means that this counsel that you can give us will be valuable and will be very much sought out by us across the diversity of our missions.

We do have a need for, and a reliance upon, using data and information about the threat and about individuals in a way that is mission focused and allows us to thread our assets

against the risk in an efficient and effective and valuable way. But at the same time we are committed to preserving the privacy and constitutional liberties and obeying the laws that are written to protect people who may have data in such a database.

So let me just give you one example, we've had a lot of conversation about the iterative versions of what's now called Secure Flight, which is our program that is under development to try to define for us a tool that will allow us to sort through the risk in two pools. Pool one, how do we know that we are finding people that we believe to have a nexus to terrorism is they present themselves to fly in the commercial system. Question two, how do we get a handle around trying to understand better if someone who's name we don't know presents themselves to fly in the network, how do we get a handle around that second question as well. So we're obviously trying to take intelligence data and other common sense tools and make a process out of this that can help us crack that problem in some sensible way.

At the same time we have the Secretary and the team is going to bring a very, very strong commitment to having enough transparency, enough clarity of process, enough commitment to the privacy, that we can manage to run a system like this to earn the public's confidence that we are doing it in the right way and provide a valuable tool to the country. So I don't think this is honestly rocket science.

I have worked for corporations that do rocket science and this ain't that hard. So, you know, it's about a lot of common sense and then putting in place tools and mechanisms that can trust, but verify. It's about giving transparency in programs so that individuals who may think they have incorrect information somehow in a visa application process, or a CAPPS II list, to find a mechanism that is practical and that works and allows them to delve into that in a way that can correct obvious errors.

I think that there are proven tools in the commercial sector, I think that there are experience from some of the firms that are represented around this table who have grappled with these same types of problems that can be flooded into the work that we're doing across this multiple complex terrain of our mission, and that we can actually do this well, and do it consistently, and do it transparently, and do it successfully.

So I think I'm going to stop with the soap box, I think the bubbles are probably leaking out from below the table here at this point at one level. But I really just come with a message from the boss, and a message from our team. This is not window dressing, we are not asking you to show up here to check some box. We want to know what you know, we want to make this stuff work in the right way, and we think that you're going to be a valuable tool in helping us do the right thing and meet our mission objectives in a way that we will all feel proud about. So, I thought that maybe it would be helpful. I'm skeptical, but maybe you might have some question that I could answer, and so I'm happy for the Committee members to ask any questions that you may have for me.

MS. LEMMEY: Well I have some comments rather than questions. But I think it's important for the Committee at large to think about as we go into this process. One, is the term balance keeps coming up, and I think it's important for us to address that. That in the

Markle Task Force work we found that if we held them as balance we didn't get to the right place, but when we held the privacy or liberty questions together with security, and we honored both it was very important to do that and to say how do we solve the problem by honoring them both together.

And I think that's going to be an important piece for us to keep bringing up in this Committee discussion because it's easy to try to see them as opposite ends of a teeter-totter as opposed to bringing them as part of the fulcrum of society that we're trying to get to. So I bring that up because I know that you're probably not as close to the conversation as some of us here, I think we're going to be watching our own language a lot as we go with that.

And then the second thing I want to bring up for the Committee as a whole, and what we've been finding, is that the space that we're moving into with technology and security and privacy we're in an age of innovation around it. This is a new time for us. And I think -- thinking that there is one right way is going to be very difficult, and it's a period of experimentation. So one of the best things that we're going to be able to do as a Committee is to hold up some of the options that we're experimenting with, and say a little to the left, you know, or a little to the right, or umm, not quite right we need to go up on this one.

And I think it's going to be very important in our dialogue together with the Department to really respect that we're in this innovation space and that we have to be careful to not say right, because we know right -- for those of us who's been entrepreneurs we know there is no one right. We fail a bunch of times before we get close, and so I think we need to give ourselves the space and grace to do that.

MR. JACKSON: I think those are both excellent points. One of the things on just your latter observation that is just indispensable is we are not about the normal government job of, you know, building a system and putting it on the shelf and watching it run, we have a fundamentally different set of DNA that we have to deal with here because we have to innovate one step ahead of the ones that President Bush called the evil ones.

And so when we figure out how to do something we have to ask ourselves the very next day how do we do it different, better, and stay ahead. So I very much agree that one of the reasons that we are eager to have some outside counsel like this is precisely two stay on the top of best practices, innovations, cycles that are short, and collapsed, and so I think that's really important.

I'm happy to learn a new language, I'm a lapsed college professor so I can be taught, and I'll take that down. I'll tell you where I come on the balance issue. Maybe it's skewed somewhat by my experience at the Department of Transportation. On the night of 9/11 after Secretary Mineta and I had each been dispersed to our different spots and we had met with everybody, talked to the airline CEOs about what we were trying to do, it was about 1:00 o'clock in the morning and we sort of shut the door and sat down by ourselves, and there was still the glow of the Pentagon on fire that was visible out our windows. And we said, you know, we talked about something at the time, it was an attack in Israel of a

bomber who went in and blew up a pizza parlor and killed up everybody -- killed everybody in the pizza parlor. So we said to ourselves you know, how do we behave going forward after this night which changed our world? And it was illuminated by that glow of the fire, and we said, you know, we will have to find a balance between security and mobility.

It will constantly mean that you have to try to figure out how do you provide for both, it's not either/or, it's for both in the right way. You could close all pizza parlors in a country, or you could strip search everyone coming into the room and these would be tools that would help you address your security objective. But in doing so you'd violate all these things that we hold dear about mobility and about freedom and about privacy.

And so what I think of when I talk about that balance is that we want both, it's not an either/or proposition, but oftentimes it involves trying to calibrate the best tools that you can use in the tool kit to do both at the same time, and you don't want security at any cost, or you know -- I don't want to say privacy at any cost, but you don't want to go either way too much. That's unpacking the Deputy's thinking anyway. But I take your language lesson as a welcome education. Yes, sir?

MR. SHEEHAN: I'd like to make a comment also about the balance, and semantics as I've heard them this morning. And I think we might be cutting it a little too nicely to worry about that term. As you said the teeter-totter analogy I think actually works in favor of the word balance because you do honor both when that see-saw or teeter-totter has reached equipoise. So I wouldn't be too concerned about your use of the word balance because I think true balance does honor both.

MR. ROSENZWEIG: I just want to ask you a quick question, perhaps one that you can't answer right now. But as I surveyed the Department and the relatively limited space on the agenda of this Committee going forward I think one of the most significant problems we're going to be facing is picking and choosing what the objects of our scrutiny are. And, you know, I'm sure that members of the Committee have issues that they think are very important and we'll be discussing those. But I would be interested in hearing from you or from someone suitable who knew which issues you think are the most significant from the Department's perspective that we should -- where you think our attention would be most valuable?

I don't necessary promise that we'll listen, we may wind up focusing on things that are of interest or we perceive as otherwise important, but I certainly would like our consideration of the agenda setting to be informed by you, and I think you're the right person to ask because I'm sure if I ask the Coast Guard they have their own particular set of issues that are, you know, unique to them, and border security, et cetera, and I already know that the components are -- they're not totally stove piped, but they have their natural inclination. So I would really -- I think the Committee would be very much appreciative of hearing from a higher level from the policy perspective of your shop, or the new Under Secretary of Policy if you ever have one, about what you think our focus should be.

MR. JACKSON: Well, Paul, I'm happy to make sure that we provide that in the right way. I do think that it's important for us to do the first stage of hearing what's on your mind because that's why we're getting you together here at one important level.

Second, we're undertaking a -- internally we're calling it the second stage review, which is an attempt to look across the Department and identify transformational activities to map our structure to the mission, and to just take a little bit of a pause as we continue to do our mission, to step back and look at the whole. So already I can tell you one where I think that Nuala will ask your counsel on, which is our screening coordination office.

We've proposed in the President's budget to create an office that will look at some of these new programs that do risk screening. We have programs which you'll hear about from my colleagues in the freight world, in the immigration and border protection world, in TSA on the passenger screening with secure flight that I've already talked about. But some of these involve common electronic platforms and approaches that we think will -- at least I personally believe would be very valuable to have you alls view about.

We're trying to bring a specific proposal to the Secretary about how to craft this office, and part of that Nuala has been invited to be one of three people from the Department joining me on a oversight board that we're going to use to begin to work those set of issues, probably will be expanded inside the Department. But we want to try to make sure that we're trying to introduce common best practices on these privacy issues across a range of these types of programs. So I think that would be an early nomination from my side for where you all can be helpful, Paul.

MS. O'CONNOR KELLY: I don't mean to quash debate but we are well over our time and out of respect for the future speakers I need to ask that we perhaps have this conversation with the Deputy either in writing or at a later time if I can so ask the members to hold their questions. Thank you very much for understanding. We have a number of senior officials who have other engagements they need to get to. So with that thank you so much to the Deputy Secretary, we are honored by your time today, sir.

MR. JACKSON: Thanks, Nuala, that was a charming hook, and I'll take it and -- (Laughter)

MR. JACKSON: -- defer to my colleagues. (Applause)

MS. O'CONNOR KELLY: Next on the agenda we have Assistant Secretary Parney Albright. Parney, like myself, was one of the original cast of thousands in the Department, and a little known fact about Parney is that he parks next to me in the parking lot, and so I know these very long hours that he puts in because his car is usually there when I arrive and there when I leave. Parney has been working on these issues really from the very beginning. He served as Assistant Director for Homeland and National Security in the White House Office of Science and Technology Policy, and has been involved in the National Security arena since 1986, including work at DARPA, and at the Institute for Defense Analyses. Thank you, Dr. Albright.

DR. ALBRIGHT: Thank you very much, and it's a pleasure to be here. I'm very grateful for having the opportunity to address this Committee. As Nuala pointed out I'm with the Science and Technology Directorate. The Science and Technology Directorate not surprisingly is that part of the Department that does research development tests and evaluation activities for the Department of Homeland Security. What I thought I would do in the ten minutes that I have is to try to give you some examples of some of the activities that we are engaged with in the Science and Technology Directorate for which privacy issues tend to be a very, very important factor in our considerations.

One of the things you need to understand a little bit about the Science and Technology Directorate, and I'll just take a second to point this out, is our history. Our history -- in the President's original proposal it really wasn't called the Science and Technology Directorate, it was called the Chem Bio Rad Nuke Directorate. Something that doesn't really roll off the tongue particularly well. But never the less what that means is that we have a legacy and a history of being the resident expertise within the Department, not just in research development testing and evaluation activities, but also in the qualitative, the more technical, activities associated with dealing with truly cataclysmic threats like Chem, Bio, Rad, Nuke.

And the reason I bring this up is that as I said despite being called the S&T Directorate we do have that history behind us and therefore we tend to be the "go to" organization, in particular when dealing with issues surrounding bio-terrorism. And therefore we end up not just developing the programs associated with dealing with the bio- terrorism threat, in fact we often own and operate those kinds of activities.

And a specific example, and a specific issue that's relevant to this Committee I think is, is that means that we come into contact fairly quickly with some of the issues, privacy issues, associated with medical surveillance type of programs. And the reason we have to do that of course - all over the country that are sampling the air for aerosolized attacks, things like someone trying to spray anthrax from the top of the building. We do that, but if you're interested in detecting a deliberate introduction of an infectious disease either into the human population, or importantly into the animal population, that requires some sort of surveillance, some sort of medical surveillance activity. So we have a couple of programs that we're working in that area.

One example is something called a biological warning and incident characterization program. And what it's designed to do is to integrate public health and environmental monitoring data with a variety of other data that we collect as well, plume modeling and epidemiological hazard models.

We're also dealing with the architecture, and this is in conjunction with our colleagues in the Information Analysis and First Structure Protection Directorate, with a Presidential Initiative that's called the National Bio-Surveillance Initiative, and that was actually first rolled out in the FY '05 budget, and the idea here is to integrate medical surveillance data with a wide variety of other data, including threat data. But also, for example, reports from Poison Control Centers, and that sort of thing. So as you can imagine when you start to

think about these kinds of programs you run very quickly up against the issues surrounding HIPAA, for example.

And so this is something that we have to deal with from the very beginning. We have to think through carefully what information in fact we do need to get as part of these medical surveillance programs, and we work obviously very closely with Nuala's -- this office here, the Office of Privacy here in the Department, but also very closely with CDC to make sure that what we're doing is first of all consistent with the law, but also consistent with cultural values as well.

Another activity that we do that I think is somewhat different is we also conduct within the Science and Technology Directorate the research development tests and evaluation activities in support of our Cyber Security group over in the Information Analysis and Infrastructure Protection Directorate.

Now for those of you who are familiar with cyber security issues the biggest threat by far is the insider threat, as I'm sure most of you know, and in order to deal with that what is common practice today is essentially to monitor the networks for anomalous behavior. What you're doing is, is you're looking for people who are authorized users on a system and you're looking for people attempting to get into databases for which they have no authority to get into.

For example trying to access information that would be anomalous for them to attempt to access. That is a common practice within the industry, but clearly what it requires you to do, and it's not just the insider threat but in general if you're monitoring networks for cyber attacks you have all kinds of information that's flowing across these networks, social security numbers, financial information, peoples' names, that sort of thing. And so clearly if you're going to have this kind of monitoring activity you're going to have to design in from the very beginning capabilities that address the privacy issues, so we're doing that, because after all you're monitoring people traffic. And people don't like that.

But having said that there really is no other way to detect that kind of anomalous -- that kind of illicit behavior. So there are tools available that permit, you know, sanitization and anonymonization of data, and again this is another area where we work very closely with the Office of Privacy here in the Department to make this work, and to make sure that people understand that the tools that we're developing that address these privacy concerns in fact are acceptable and meet the standards that need to be met.

A third example, and this is one you'll probably hear a bit more about later on from Randy Beardsworth and the border folks, but one of the key other issues that we have to deal with that is relevant clearly to privacy is with the international flow of information. And you have very different privacy regulations and laws in other countries, and you frankly have very different privacy cultures in other countries. And as we've talked over the years since 9/11 about sharing of biometric information and collecting biometric information you don't have to -- you can pick up almost any casual, you know, any casual reading of a newspaper, particularly an international newspaper, will generally have some sort of article where people are very concerned about the sharing of that particular information.

One program that we've initiated working cooperatively with the Borders and Transportation Security Directorate is something called The International Travel Security Program, EITS. And it's an example of how technology can serve to mitigate a lot of the privacy issues of concern. What you have here is an IT infrastructure that allows countries in fact to interrogate data that is held by another country in a manner that is consistent with the privacy laws.

So for example, I mean the simplest example you could think of, is suppose someone presents themselves at the boarder with a passport. What I would like to be able to do is simply verify whether that passport is a valid passport or not. That does not mean that I need to have a, you know, some sort of uber database sitting in the United States that has everybody's valid passport in there. But in fact that would be not a very smart architecture because the validity of the passport number is something that may change on a daily or even hourly basis. It is far better off to create an IT infrastructure that allows me to go back to the country that issued the passport and just simply ask them, is this a valid passport number. Okay? And that's exactly the genesis of the EITS program.

Now once of course you've developed those kinds of pipes, okay, you then have the opportunity to, for example, interrogate biometric data, rather than me in the United States holding a large database of foreign biometric information all I may need to do is take that biometric at my border and pass it back to the host country and ask them to interrogate their database and say is this the person who they claim to be? So the idea here is it's sort of an ATM kind of infrastructure and the idea is, is to develop an international means for enhancing security while at the same time being completely consonant with the privacy rules and regulations and cultures of these other countries.

And this is a program we're actually piloting with the UK and Canada, Australia wants to climb on board and we're starting to talk through the OECD with the larger international community on this. Let me just give you some examples of some of the relevant science and technology programs.

We have lots of other activities that are relevant to privacy, we have interoperable data sharing programs, we developed software tools for example to help the threat screening guys do their job. And what I would just offer up is we'll be happy to work with you at any level of depth you want to work at to help you better understand what our activities are.

MS. O'CONNOR KELLY: Thank you Dr. Albright. In the interest of time I am going to encourage the Committee to think about written questions for the leadership, and this is really a taste of what our leadership does. I think we can invite them back for further interrogation, to use Parney's term, later on at another time. I welcome Acting Under Secretary Randy Beardsworth. Again, another senior leader who has been with the Department from the very beginning, served as a key member of the transition team charged with the creation of DHS beginning in December of 2002.

Mr. Beardsworth particularly worked on the integration of the four agencies that make up the Border Transportation Directorate, ICE, CBP, FLETC and TSA. As the BTS Director

of Operations under then Under Secretary Asa Hutchinson he focused on coordinating enforcement activities among these component agencies. It's been my great pleasure to work with Randy over these past two years, particularly on the use of information about our international visitors, and I thank him for joining us today.

MR. BEARDSWORTH: Thank you, Nuala. First of all let echo Michael, thanks to you all for being here and taking your time. We do view this as a partnership, we do see this as being productive not only for the Department but for the country, so thank you. And I'd also be remiss if I didn't thank Nuala for her close partnership with us as we work through a lot of issues that have some visibility within government and within the public, and I think you'll see that in the next nine minutes and 45 seconds that I have.

We are the largest of the Directorates in the Department. Of the five Directorates we have over 110,000 people of the 180,000 people in the Department. We have three large operating agencies, TSA, ICE, which is Immigration and Customs Enforcement, and Customs and Border Protection, as well as the Federal Law Enforcement Training Center and the U.S. VISIT program among others.

I always like to begin my talks with referring back to the law, and indulge me for about a minute here if you will. And in section 402 of title four of the Homeland Security Act it outlines the Under Secretary for BTS responsibilities, and very quickly, preventing the entry of terrorists and instruments of terrorism into the United States, that's one; securing the borders, territorial waters, ports, terminals, waterways and air, land and sea transportation systems; carrying out the immigration enforcement functions; establishing and administering the rules governing the granting of visas; establishing national immigration enforcement policies and priorities; administering customs laws for the United States; conducting agricultural inspections. And then the final one, which sometimes we never get to, is in carrying out the foregoing responsibilities, ensuring the speedy, orderly and efficient level of lawful traffic and commerce. So I think if you all look through, and do your work, that we may run into each other -- or at least some of our people will be talking with you on some of the issues.

The Chair has asked the Deputy what is it that you all can do, or what we think would be a good thing to focus on? And I'll jump into that breach and make a comment. It is I think one of the most important things you can do for us is to help us figure out how to do facilitation in many of these programs that we do. The security piece is easy, but the facilitation piece of it can only be done if we can meet the privacy issues and do that in a way that the public understands and appreciates and accepts.

As I read through those eight things you'll see that there's a tension between security and facilitation in everything that we do, there's the security and facilitation tension. And privacy is right in there and is the tool about which we resolve a lot of that tension.

So your job is very important. I thought I'd take the next few minutes and just very quickly highlight some of the programs that come under the BTS purview, if you will. They expand into the other areas, they're interagency, there are policy issues, but these are some of the things that we're working on just to give you a flavor to sort of whet your appetite.

The U.S. VISIT Program is the first one. This of course is a biometric entry/exit system that's had a lot of visibility in the last year, or 15 months. We have had queried and registered over 20 million people over 2500 watch list hits and 500 refusals of entry based on those hits. These systems for U.S. VISIT are in 150 airports, 14 seaports and the 50 busiest land ports of entry. And that's an area where there are a number of issues revolving around biometric standards about how we use data, how we share data, and so forth.

I'll mention the ABC Initiative, which is the other within the Border Control Initiative. That's an effort to gain control of the southwest border and reduce illegal immigration, break up smuggling rings, and so forth. As you are probably aware from the press that over 50 percent of the illegal entries into the United States occur in the Arizona area. That's a whole area that's very operational where we're coming into contact with somewhere around a million people a year, or less than a million people a year.

A whole other area is cargo, and how do we handle cargo and facilitate the flow of cargo while ensuring security. We have a couple of programs that you'll become familiar with, the Container Security Initiative, and CT PATS. As you're aware there are over nine million containers that come in to U.S. ports each year, and again security and facilitation. And in order to get facilitation we have to use database, we have to do targeting, we have an automatic targeting system that is exercised through our National Targeting Center to try to figure out based on data submitted by shippers whether we're concerned about a particular container or not. And every container that's coming into the United States is screened in this manner.

Surface transportation is a whole other sort of area that we deal in. We've issued security directives in the rail and mass transit environment, but we've also screened over 2.5 million, 2.7 million, hazardous material drivers against various databases. We're developing a transportation worker identification credential, or the TWIC program, which will help us do checks on transportation workers.

The Deputy Secretary mentioned the Screening Coordination Office that the President's '06 budget discussed a little bit. This is a whole area that we'll be working to develop within the Department, as Michael mentioned.

And then the last two areas, the ones that you're probably very familiar with, and I'll tell a real short story before I get into those two areas, or highlight those. Often when I speak people will ask me what is it that keeps you awake at night, what makes you worry at night, what are you concerned about?

And one of the three things that I talk about is trying to understand who's getting onto airplanes before that airplane takes off, and being able to check and understand who these folks are. So one of the things that I would encourage you to do in your work as you look at the privacy issues is to understand the vulnerabilities and the threats that are driving us to worry about those things, about who's getting on an airplane. And some of the limitations that we have in being able to determine that while looking at the privacy issues.

These last two areas are -- generally are passenger screening, and Michael mentioned Secure Flight, which right now is the domestic portion of trying to answer that question. Michael described it as a couple of groups of people that we're trying to identify, known bad guys and unknown bad guys. But the practical problem here is that a lot of people have similar names, and we need to be able to figure out how to quickly eliminate and not bother the traveling public who happens to have the similar name to somebody that is a bad guy. Often you'll hear people say I'm on the watch list. They're not on the watch list. We need to be able to ascertain very quickly that they're not on the watch list, and data, and the use of data, and appropriate use of data, is how we're going to have to tackle that problem.

And then the last area I'll mention is one that we've been working is the No Fly List, which is a specific pre-adjudicated subset of the overall terrorist screening database, and we've made huge leaps forward in that world in terms of cleaning up the database, being able to -- having established government wide criteria that everybody understands about how you get on this pre-adjudicated subset of the terror screening database.

And then sort of the last issue, particularly with passengers who are dealing with people is we are working in every venue, if you will, to ensure that there are adequate redress procedures. And this is something of course that I think you'll be interested in looking at. That's ten minutes, I'd love to talk more about what we do, but I hope to have an opportunity to engage in some discussions in the future.

MS. O'CONNOR KELLY: Thank you, Mr. Secretary. I'd now like to introduce Under Secretary Michael Brown of the Emergency Preparedness and Response Directorate. In my shorthand that is the agency formerly know as FEMA. Mr. Brown was the Deputy Director of FEMA and the agency's general counsel prior to his service at the Department, and served on the President's consequent Management Principles Committee after September 11th. We are delighted to have him here. Mike is one of our TV stars, you've seen him on television during any number of national disasters and you can take one look at him and see why. He and Mike Garcia are our TV stars at the Department of Homeland Security. We are very grateful for his time here today. Thank you, Mike.

MR. BROWN: Thank you, Nuala, that was quite an introduction. I'd like to say congratulations to this group on your first meeting. I want to make a personal note, and my personal note is this: I think the work that you're doing, and the work that Nuala is doing, is incredibly important to the Department.

I mean September 11th changed everything in this country, and I think it's incredibly important that we maintain this balance between privacy concerns, security, and it's that age old question. And so the fact that you're meeting and doing this I think just as a private citizen to me is incredibly important, and I thank you for doing it. Now I've also served on groups like this, I know it can be a pain sometimes.

You know, you get stuck here and everything else -- hang in there, it's worthwhile to keep doing it. Before sharing a few key examples of how FEMA has specifically addressed privacy concerns and continues to do so I want to give you a quick overview of FEMA.

I hope none of you in this room have had an opportunity to meet FEMA. Frankly, you know, when the rest of the Department is unable to do what their job is for whatever reason we're kind of the mop up crew. We come in at the end and clean up messes that either the bad guys have done to us, or unfortunately that mother nature has done to us. And that's in essence what our goal is.

Last Friday FEMA celebrated it's 26th anniversary. It was formed in 1979 and in 26 years the mission and the focus of this portion of the Department, FEMA, has not changed. And we have responded to disasters in all 50 states, Puerto Rico, Guam, the Pacific Island Trust, the territories, the Virgin Islands. We have sent teams to India, we've sent teams to Bam, Iran when the earthquake hit a year ago. The first Americans in that country in 25 years. We have groups that go all over the world, Russia, throughout Europe, South America, that teach and train and exercise in how to do emergency management, how to respond, how to recover as quickly as possible because we certainly believe that the quicker we respond, and the quicker we recover, we tend to not only help people get their lives back in order but we help take the terror out of terrorism in doing so.

Through the efforts of the thousands of people that respond to disasters that we have brought this country through some amazing times. The Midwest floods of 1993 and 1997 which encompassed the entire Midwest. The North Ridge earthquake which we still have projects that we're working on out there. Obviously, the September 11th attacks, the April 19th attack on the Oklahoma City Murrah Building, the 2004 hurricanes, the Columbia space shuttle disaster. All of those things FEMA has been an integral part of coordinating the entire response of the Federal government to respond as quickly as possible. After joining DHS in March of 2003 FEMA continued that tradition of responding quickly and ably. We will come and help people wherever disaster strikes and regardless of what causes that disaster, and that is what we call our "all hazards approach." And that will continue to be the approach of not only FEMA but I hope the entire Department.

We do more though than just respond to disaster. We do things like mitigation activities. It's the belief of this President that things that we can do to mitigate the effects of disasters both before and after is good public policy, and we will continue to that on behalf of the President. We train first responders. Emmitsburg, Maryland alone we train literally tens of thousands of people who then go out and train others, so in essence we train millions of first responders in this country.

We work with the state and local emergency managers. We need to know who those people are because FEMA and the Department are only effective in the sense that we have good partnerships with state and local governments. We're not going to do it all from Washington, D.C. and FEMA is not going to do it all. We have to do it in partnership with state and local governments.

We manage the National Flood Insurance program, and we also have the U.S. Fire Administration. In addition to that we have inherited -- because of DHS we have inherited the National Disaster Medical team, we do work with the Strategic National Stockpile and Nuclear Instant Response Teams also.

But having said all of that another large part of our job, which I think you're probably even more interested in, is providing assistance to disaster victims. To give you an idea of the tremendous scope of this particular part of our program in FY '04 -- or actually in calendar year '04, FEMA obligated more than 4.9 billion dollars in disaster funds to individuals and state and local governments. That was for wild fire recoveries, flood recoveries, tornado recoveries, all the kinds of disasters you might have where FEMA responds. Last year alone was 4.9 billion dollars. Last year we responded to 65 major disasters and seven emergencies declared by President Bush.

That 4.9 billion dollars in disaster funds we provide to individuals and to communities comes through two types, two main types of disaster assistance. The first type I want to talk about very briefly is individual assistance. That's the money that we give to individuals, and I think this is important to underscore, at a time when they are most vulnerable and under circumstances in which they are probably the most vulnerable. This money goes to help individuals get their feet back on the ground and start the recovery process. It goes to things like temporary rental assistance, emergency needs to get some food, maybe some transportation so they can continue to work, to help them recover some household goods that may have been lost in the disaster. It's the type of seed money I would call it to help them get on the road to recovery. That's individual assistance.

The second type of assistance we provide is public assistance. And public assistance is money that we give to state and local governments to help them recover from the disaster, rebuilding the ITN bridge across Pensacola Bay for example from a Florida hurricane, rebuilding schools, rebuilding infrastructure, helping the state and local governments with those things that they would be responsible for, helping them in their financial recovery.

On the issue of privacy I want to focus for a minute on individual assistance, and the safeguards that we have in place to protect the information that those individuals give us. You see in order for us to give money to the individuals and to help them they must provide FEMA with some incredible information.

To determine that we must determine an individuals' identity, their disaster loses, they must submit to us certain personal and financial information so that we can understand who they are, who they really are, and what they may truly be entitled to. We use this information to make sure that we're not giving out duplicating benefits that they might be receiving from an insurance company, or from some other entity, and in some cases we actually transfer money directly into their bank accounts once we determine that they are eligible.

FEMA maintains all this information in a national emergency management information system, or NEMIS, which also operates under privacy standards and safeguards and is restricted to only authorized users. We work hard, very hard, to make certain that this information is protected and that we operate in accordance with the Privacy Act of 1974.

When you stop and think about disaster victims, and my point about we give them money when they're most vulnerable, under the most vulnerable circumstances, we must protect those privacy safeguards. It would not be prudent to provide an individual's name and how

much money they receive and what it was for because then people could nose in and find out what their neighbors got, scam artists who want to put a roof on or something could find out how much money they got, and suddenly that's the cost to put the roof on. So we take those kind of privacy concerns very, very seriously. We also make certain that the individuals who are applying for aid understand why we need the information and what we're doing to protect that information.

At the very beginning of the application process FEMA presents the applicant with an explanation of the Privacy Act and makes them aware that the information that they're going to give FEMA can be shared with the bank, the insurance companies, or other assistance providers. The same notice is the first page to appear when an individual applies for assistance to our website, fema.gov. On this page people actually have to check a box that says that they have seen the Privacy Act, they know it's available there, they can read it and understand it if they choose to do so.

One of the things that we did was by going through the website we wanted to make certain that individuals had the opportunity to use all types of methods to apply for assistance, not just in person at a disaster site, they could also do it over the telephone, but for those who maybe have gone somewhere else, you know, to get away from the disaster site we made available fema.gov so that we could help them speed up that process.

Before we used the web application process we went through a privacy impact assessment to make sure that we were still meeting our objective of protecting the information that people were giving us. But I'm very proud to say that through that assessment process we found that FEMA has very good strict adherence to the Privacy Act of 1974, and that we probably go the extra mile in protecting this privacy information because again, it's giving it to individuals at a time when they're most vulnerable in the most difficult circumstances. This is just one example of how we work to maintain privacy standards within the organization.

I'll just tell you, bottom line, FEMA is dedicated to protecting this information, and dedicated to ensure that those who provide us with that information believe and understand and have comfort that that is going to be safe once they give it to us. Again, congratulations on your first meeting, you're doing yeoman's work, keep it up. I as one lowly civil servant appreciate the work that you're doing.

MS. O'CONNOR KELLY: Thank you, Mr. Secretary. We are honored by your presence. I'd like to invite Deputy Chief of Staff Sue Armstrong from the Information Analysis Infrastructure Protection Directorate. Sue has been with the federal government since 1988 in the Office of Internal Audit at INS, and the Office of Inspector General at the Department of State, and the General Services Administration. We've worked closely with her office on the creation of the critical infrastructure information work at the IAIP Directorate and we thank her for being here today.

MS. ARMSTRONG: Thank you, Nuala, I'm happy to be here. General Matt Broderick, who is our Acting Under Secretary could not be here today because he's pretty fully engaged in the exercise TOP OFF 3, so I'm happy to be here. I thank you as do the rest of

the DHS participants for your work. I was trying to think of some things to highlight related to privacy that IAIP does, but I really can't pin it down to ten minutes. Really everything we do, and I'll talk to you a little bit -- I think what will be helpful is to tell you kind of a 50,000 foot view of our mission and our main components and what we're doing, and what we're trying to do. IAIP, as you may know, is a start up within a start up organization.

We were one of two new pieces of government that the Homeland Security Act of 2002 created, ourselves and the Science and Technology Directorate. And we are a conglomeration of five legacy organizations but I use the term organization loosely because we didn't really come to the table with any thing, or any people, or any buildings, or any way to comply with privacy frankly, and Nuala has been instrumental in helping us stand up at disclosure office and IAIP.

Anyway, our legacy components were from the Commerce Department, the Critical Infrastructure Assurance Office, from the Energy Department, the Office of Energy Assurance, from the General Services Administration, the Federal Computer Incident Reporting Center, or FEDCIRC, from the FBI, the National Infrastructure Protection Center, and from the Department of Defense, the National Communications System, which was our one legacy standing organization with the capability to do anything when we started, such as hire or buy something.

When we started we had about a 135 people, they were mostly at NCS. We had 499 vacant positions transferred to us. And that's where we started. Today we have 571 people, 491 of whom are on board, the others are pending security clearance, and we are hiring amazing people from throughout the government, from the private sector, and everyone at IAIP is working with a sense of urgency and purpose to safeguard this country, and it's been a real privilege in the almost two years that I've been there to just see the dedication and resolve of people in very challenging, frankly, circumstances for us.

Our mission is huge. We liken it to defining mission while you're executing it, that is you're in the airplane, it's taxiing down the runway, and oh, some of us are still putting on the wings, in our day to day. But our mission is to identify, assess, and analyze current and future threats to the United States, map them against the nation's interdependent complex critical infrastructure and to prescribe and implement preventive and protective measures.

That is to take what is coming out of the traditional intelligence community threat reporting, map it against what we know about our vulnerabilities, and put out to an audience that largely does not have a security clearance so this stuff has to be rendered unclassified, put out actionable, timely, good information to inform our Homeland Security partners what they can do to harden themselves as a target, to prevent the use of the nation's critical infrastructure as a weapon, as happened on 9/11, and to basically preserve our economy and the American way of life.

That in a nutshell is what we're trying to do at IAIP, and we are trying to tap into what I call, capital "I" Intelligence by virtue of membership in the intelligence community, so we're reaching into the intelligence community for information, but we also have the

incredibly vast universe of what I'll call small "i" information to help us better understand, better prioritize, learn more about terrorists tactics, intentions, techniques, and to get that information out to people who need it. So balance is a key word for us.

We have a universe of non-traditional sources of information that we're trying to tap into and use in our analysis of who's coming to the homeland, who's already here that would do us harm, what do they intend, what are they capable of, and what tactics are they employing. And when I say it's a vast universe of information I'm not kidding. DHS inspectors inspect primary inspections of over 500 million people a year. The border patrol apprehends over a million people every year. So when you start thinking about what DHS does and the information that we have just in DHS it gets mind boggling.

It gets even more so when you start thinking that part of our mission is to engage non-traditional sources of information that go into intelligence analysis. State and local law enforcement, state and local leadership, private sector owners and operators of critical infrastructure. 85 percent of the critical infrastructure in this nation is privately held. And as many of you well know the private sector is at best wary of forming an active partnership to share information with the federal government. So that's some of our talents.

We have three main component offices, the Office of Information Analysis, that's where our intel work is done. We do the intel work of the Department of Homeland Security on a daily basis, we brief the Secretary every morning with what's going on, and IA focuses both on current intel, what's happening right now, what's arriving right now, what surveillance or possibly suspicious activity is going on right now, and also we do intelligence analysis from the departmental perspective. What are groups inside the United States doing, what are they intending, what new techniques are they seeking to exploit. So it's both the right now, and the longer term intel analysis.

Our Office of Infrastructure Protection is how we make infrastructure protection not just a federal job, but a national job. It's how we get out there and partner with entities, with municipalities, with private sector owners and operators. We have a group of security specialists who will have completed more than 200 trips this year to visit facilities and conduct what we call site assistance visits. That is a comprehensive look at a facilities security planning, vulnerabilities and capabilities to protect itself.

We have the National Cyber Security Division, and I think Andy Purdy, the Director, is here today to listen and see what's going on. Obviously cyber is a high profile issue and we take it very seriously, and Andy has done a great job in taking the responsibilities that had to do with federal reporting of computer incidents to the national scale, that is to engage anybody who's got a system or a network to report what's going on so that we can take a holistic look at the internet and cyber space and protect it.

I mentioned the national communications system as part of IP, it's our one long-term organization at IAIP, it was set up after the Cuban missile crisis to ensure telephone continue activities throughout the federal government in an incident or crisis.

Again their mission is expanding because traditionally it was dial line, now the whole cellular question is something that they're tackling, and making sure there is cell phone con-activity in a crisis. And the last component of IP is our Infrastructure Coordination Division, and that is how we engage and talk to the private sector. You may have heard the term ISAC, Information Sharing and Analysis Center, that each critical infrastructure sector has or had, because they are actually now called Sector Coordinating Councils, but it's how we engage with, and talk to, and get information from, the private sector.

And then finally our other major component is the Homeland Security Operations Center. That came to IAIP in the mid 2003, and it is how the Department maintains situational awareness of what's going on in our country and at our borders. All DHS components are represented in the HSOC as are another dozen or so other federal agencies, and now some large metropolitan police departments such as MPD, the New York City Police Department, and LAPD. It's how we take a 24/7 365 look at what's going on in the country to inform senior decision making in the time of an event or an incident or crisis. It's how we monitor high profile events like the inauguration and other events that are not, as you'll hear from the Secret Service, NSFE, and it's how we get information to all of our partners.

We rolled out the Homeland Security Information Network this past year, and that is a real time collaborative information sharing tool. It's not just email, and it's not just a bulletin board that we post stuff on, it's literally how we can talk back and forth to the Oakland County Sheriff's Department, the Emergency Management Operations Center in New York City. We've rolled it out to all 56 states and territories and several major urban areas, and are planning for the next year is to roll it out to over 3000 counties in the United States, and it's a platform for sharing back and forth sensitive but unclassified information, but you can also post -- and this is where we'll certainly want to take your account, so you can post pictures, you can post other types of information, you can get into a dialogue with local police departments about suspicious incidents that they're seeing, and again all that information informs our intelligence analysis in the effort to partner and keep this country safe.

MS. O'CONNOR KELLY: Sue, thank you so much for being with us today. We appreciate it. We now call Steve Cooper, who's our Chief Information Officer. Many people have said that I have a hard job, I think Steve actually has a harder job in bringing together the legacy systems of 22 former separate agencies, and a handful of new ones. We are honored that Steve chose joined the public service from very senior positions in corporate America. I don't think he recalls but I recall meeting with him on Christmas Eve of 2002 when he was again one of probably five people working for the Department of Homeland Security at that time, and just beginning what has been a long and successful journey in the senior leadership. Thank you for being here today.

MR. COOPER: Nuala, it's my pleasure. Actually I am Janet Hale, the Under Secretary for Management and when I learned that I had to be at the White House and in front of this Committee at the same time I contacted our Science and Technology Directorate and asked if they could create a clone. Unfortunately the contractor awarded that capability of cloning was the low cost bidder. And this is the result.

As Steve Cooper I just want to thank you all for your service in being a part of this extremely important advisory group. The Department needs your insight, your expertise and most importantly I think your recommendations as we move forward. Partly because I'm not certain that we have together engaged in examination of the balance of privacy and security to the extent that it is now critical ever before in our history. So I thank you all for serving, look forward to kind of what develops.

What I'd like to do very quickly on behalf of Janet Hale, who could not make it today, is to give you a sense of the structure of the Management Directorate, which is actually the third directorate, Sue mentioned two, Information Analysis and Infrastructure Protection, and Science and Technology, that literally were brand new. They did not exist, there was no legacy inheritance. The third is actually the Management Directorate, which also did not exist. It's comprised of eight main offices inside the Department, each of what we all the Chiefs, the Chief Financial Officer's office, the Office of the Chief Information Officer, the Office of the Chief Procurement Officer, Human Capital Officer, Administrative Services Officer, the Office of Immigration Statistics, and the Business Transformation Office.

Very quickly, an overview of each one of those. The Chief Financial Officer's primary mission is to provide guidance and oversight of the money, the Department's budget, financial management investment and strategic planning functions to ensure that funds necessary to carry out the Department's mission are obtained, allocated and expended in accordance with the Department's priorities and all appropriate laws and policies.

The Human Capital Officer advises and assists the Secretary and other senior agency officials in carrying out our responsibilities for selecting, developing, training and managing a high quality productive work force. This mission actually includes a very extensive amount of change. I'm sure you've read and followed in the papers the fact that we are implementing a brand new performance management and human resources system, not necessarily the automation thereof when I talk about system, I'm talking the process and all of the accompanying policies and procedures. But in addition to that their mission includes aligning resource policies and programs with organizational mission, strategic goals and performance outcomes, assessing our work force characteristics and future needs, closing skill gaps, which at the moment do exist and we are working to close them, and ensuring continuity of effective leadership throughout the Department.

The Chief Procurement Officer supports the Department through the coordination and oversight of enterprise procurement and acquisition policies and procedures, all competitive sourcing initiatives and our small and disadvantaged business assistance program. They also have been given the responsibility for guiding the Grants Management Programs of the Department.

The Business Transformation Office, which is now housed within Janet Hale's office, serves as the change management agent for the Management Directorate directing supporting the transformational initiatives of the Department as identified in the Department's strategic plan, the President's management agenda, and ensuring the effective coordination of the enterprise wide support systems and initiatives of the Under Secretary for Management. This particular office reports directly to Janet and is the focal point for

functional integration coordination and oversight. This includes a dedicated focus review process over many of our enterprise initiatives, EMerge 2 which is our financial management massive program integration, our MAX HR program, which is the name given to the Human Resources initiative that I mentioned, and our Enterprise Information Technology Architecture initiative, Shared Services Integration, and the various review boards and councils established to focus Departmental decision making. This office is also going to take on process redesign opportunities and identify new or innovative solutions that cross organizational element lines, which hopefully will produce operational improvements and greater management efficiencies.

The Office of Immigration Statistics leads the development of statistical information useful to make decisions and to analyze the effects of immigration in the United States. By Congressional mandate its role is to develop robust statistical analyses that provide relevant immigration information needed by DHS managers and policy makers that is of high quality, relevant, timely, cost effective and customer oriented.

The Office of Administrative Services is responsible for all of our facilities, real property, equipment, material resources, also has leadership for our safety, health and environmental programs. Thankfully it has responsibility for our records management and forms management which normally is under the purview in other departments of the Chief Information Officer. It is a lot of work, not very -- a very thankless type of job, and for whatever reason I'm thankful that we put that under the Chief Administrative Office. And this office also has responsibility for all of the printing of the Department. It serves as an executive service center to support the Office of the Secretary and executive officers of the Department as well. Their challenge is very simply to consolidate an optimize all of the stuff, real stuff, that they have responsibility of overseeing.

And then last, the Office of the Chief Information Officer. I've had the privilege of working with Nuala literally since before the Department actually was created. Key to the role that you play my office has responsibility for ensuring that a privacy impact assessment is done for every application that the Department implements. At the moment that represents over 33,000 applications. I will admit to you up front that we do not have a privacy impact assessment in place for all 33,000 plus applications. Nuala's office and my office are working on that, we are moving as quickly as we can to correct that situation. Realistically it is going to take some time. We are approaching that by taking basically a prioritized approach, and that prioritization will be set jointly by Nuala's office along with the Secretary and Deputy Secretary and I would urge recommendations from all of you. And at that point I'm simply going to stop, give whatever remaining time back to Nuala and the Committee, and thank you very much, I look forward to working with you.

MS. O'CONNOR KELLY: Thank you, Steve, for being here today. Next on the agenda is Chief Counsel Robert Divine from the Citizen and Immigration Services. Mr. Divine has extensive experience in immigration practice, including all types of temporary visas, change status, permanent residents including asylum, consulate processing, naturalization and removal proceedings for businesses and individuals. Prior to joining CIS he was in private practice including immigration and business litigation. We are delighted to have him with us today. Thank you.

MR. DIVINE: Thank you, I'm here on behalf of Director Eduardo Aguirre, the Director of USCIS, U. S. Citizenship and Immigration Services. Director Aguirre sent me an email thanking me for covering for him on this and I want to quote what he wanted me to say, a brief thing he wanted me to say, and that is "that USCIS leadership is committed to supporting the form and the substance of privacy laws, we take our responsibility as the main keeper of many immigration records very seriously. We instruct our operations staff to monitor compliance to ensure that we practice what we preach, and we would welcome any input on perceived failures on our part and ways we can improve."

So I think we've got the right attitude anyway. I'm pleased to participate with people who know far more about privacy interests and issues than I do, and I personally am looking forward to receiving any insights that I can get from you in connection with our agency. Some of you are from institutions that have had challenging experiences with data privacy and related issues and I hope that you can help us avoid the kinds of experiences that some of us have had.

On a personal note I have served from a private position on a governmental committee similar to this in studying the expedited removal process as an expert for the U.S. Commission on Immigration and Religious Freedom, and I can only warn you to be careful that you now have exposed yourself to governmental workings and you may find yourself like me swooped up and placed in a government in a very unexpected way as I was less than a year ago.

My office is called the Office of Chief Counsel within USCIS and our office works closely with Nuala's and one of our attorneys, Elizabeth Gaffin, who is here today is solely devoted to privacy and the Freedom of Information Act issues. I want to give you a quick idea of what USCIS is and does and then move on to some more specifics about data type issues at CIS.

CIS -- I think it's helpful to think of USCIS as the fourth border. There's air, land and sea, and then there is the application process by which people obtain visa status, or extension of it within the United States, permanent residence and citizenship, and another type of significant application along similar paths is the asylum process. CIS manages those -- decides those applications, so it's primarily an adjudicative body of about 15,000 employees and contractors in that effort.

Headquarters are located on 20 Massachusetts Avenue very conveniently and curiously placed between the Dubliner and Capital City Brewing. Let me give you some details about -- well, and we also have a significant operation at 425 I Street, which is where I think most of the technology efforts are placed, and then obviously offices throughout the United States. Some service centers that are sort of immigration factories that have hundreds, or thousands, of people who decide these applications on paper, and then offices locally throughout the country that decide -- that interview people and make decisions.

USCIS manages countless files and databases on individuals who have applied for some kind of immigration status and they obviously contain very personal information. USCIS retains these alien files, we call them "A" files, for significant periods of time. I think, you

know, it may be 80 years or something, and at some point they become of interest to the National Archives for more historical and genealogical research. So I'm not sure there's an absolute end life for many of the records that we have.

These records are mainly on paper, but you know, obviously increasingly electronic, and there is a goal and an effort underfoot to -- or underway to digitize as many of these records as we can. That is a significant effort because it is a lot of paper that gets added onto piece by piece over time in ways that make it difficult to just make an electronic file and let it be. The plans to digitize the records I think will make it easier to access these records by various DHS stakeholders who decide immigration cases.

USCIS has also a set of application support centers, or ASCs, throughout the country. They're slightly different than our district offices, although sometimes co-located with them, that collects biometric information, and these days that's collected electronically. Someone comes in, does two prints, ten prints, photo, signature, these kinds of biometrics that are used for two primary purposes. One is for confirmation of identity and sometimes comparison with previous applications that have been made -- well maybe this is three purposes, for running through the FBI and fingerprint checks, and then for preparation of the documents that evidence the status that a person has been given. The goal is to create biometric documents that are more secure and are machine readable. The biometrics that are taken are increasingly -- I'm not sure exactly where this effort is right this second, but stored on the U.S. VISIT system that was mentioned by Randy Beardsworth. They are -- let's see, I mentioned what their uses are. And so now what do we do with other information, or what are we trying to do.

CIS gives status and documents to people that allows them freedom to work and travel in ways that the U.S. public expects us not to grant to dangerous people, therefore CIS conducts background searches concerning the applicants for status and has been carefully evaluating the sources and methods for checks, especially since September 11th, and it's an effort similar to the one that Randy Beardsworth mentioned for BTS, that includes us, and CBP.

Some of those are routine and other of those background checks are on a more limited basis, we use both names and biometric space checks, and the routine ones include the IBIS, or text name based system, that is itself a conglomeration of data contributed to by more than 20 agencies, and then also the FBI fingerprint and name check systems, or processes I guess I should say. Occasional sources can include some private databases.

Generally the effort is to find out if the person at hand is the person he or she claims to be, and if that person has been found before to be a person who committed acts that make that person inadmissible to the United States. CIS regulations require that adverse information from the sources be shared with the applicant with an opportunity to rebut before we rely on that information to reject a benefit. This effort to do background checks has resulted in much of the litigation that I am currently in charge of at CIS because it takes time and it slows our processes, and it's understandably frustrating to some. I can say that we are desperate to obtain more efficient means to accomplish this background checking

objective, and I think that your Committee should be alert to developments in that regard because I think they will have significant privacy implications.

Other law enforcement agencies have an interest in our sharing of our information. We have files about a lot of people and I think that's something you need to be aware of. There are increasing requests for that and Ms. Kelly's office is involved in dealing with those. We don't do any systematic data minings of public databases that I know of, but we are beginning to, and plan to increase, mining of our own records to find fraud and so forth.

We do have some computer matching programs, the SAVE system that's mentioned I think on our website where we verify with state and welfare agencies the immigration status that may be a pre-condition to eligibility for certain benefits. We have involvement with the employer verification systems that employers use to confirm that someone is eligible to work, and a few other small matching programs.

We do respond to a great number of Freedom of Information Act and Privacy Act requests where people are primarily requesting their own records. The Privacy Act only applies technically to U.S. Citizens and Permanent Residents, but we extend that in effect to aliens through an exemption of the FOIA Act, the Freedom of Information Act so that we basically don't give out private information to anyone except the person who is requesting -- about whom that record relates with very few exceptions.

There is a lot of information on our website at USCIS.gov about the agency in general and at the very top of the menu on the left is about us and FOIA, and you can get all kinds of information about our systems of records, you know, in that formal way that describes all kinds of things including technology protections and so forth. I think that's enough, and I'll be glad to work with you and look forward to hearing about your work. Thank you.

MS. O'CONNOR KELLY: Thank you so much for being with us. And thank you to our last two speakers who have been with us from the beginning of this session. Our next speaker is Deputy Assistant Director Steven Woodard from the U.S. Secret Service. We are delighted to have him with us. He has served with the Secret Service since 1987, and prior to his current position was the Special Agent in Charge of the Richmond Field Office, and worked in the Major Events Division as well as the Intelligence Division. Thank you for joining us.

MR. WOODARD: Thank you. And in the interest of time I will get right to my prepared remarks. The Admiral and I have done the math and we figure we each have about 45 seconds to do this.

On behalf of the Secret Service I am grateful for the opportunity to join you today as this Committee begins an open dialogue about the importance of safeguarding privacy and data integrity within the context of the significant work being done by not only our agency and our colleagues within the Department of Homeland Security each and every day. The Secret Service is built around the philosophy of prevention. Whether our goal is to prevent loss to our economy by suppressing counterfeit currency, investigating electronic crimes,

or preventing an attack on someone under Secret Service protection. Our philosophy is one that fits well with the commission of the Department of Homeland Security.

I believe that one of the Secret Service's most important successes has been forging partnerships. Partnerships between our federal law enforcement colleagues as well as with public and private sector partners on the state and local level. Now I don't want to bore you today with my standard Secret Service history speech, but I would like to take just a few minutes to tell you about our agency in hopes that this information will assist you in your work on this Committee.

Most of you probably associate the Secret Service with protection of the President, and that certainly is a critical national security mission we have been engaged in since 1901. But what people often forget is that the original purpose for the Secret Service was to investigate and suppress the production of counterfeit currency, which accounted for one-third to one-half of the currency in circulation at the end of the Civil War, a situation that was undermining the stability of the U.S. economy.

The law establishing the Secret Service was actually authorized by President Abraham Lincoln on April 14th, 1865, the last day of his life, he would be assassinated that evening at Fords Theater. Today the Secret Service remains a dual- mission agency charged with protecting our nation's leaders from Presidents and Vice Presidents to visiting heads of state and presidential candidates. We are also the lead agency for events, as you have heard earlier, of national significance called national special security events. Those events include the Olympics, Presidential inaugural, State funerals, political conventions and world economic summits.

The Secret Service's protective mission has become exceedingly more difficult in today's world. The variety and destructive magnitude of possible terrorist acts continues to increase and the nature of terrorist activity has become more technologically sophisticated. Likewise this country's banking and financial infrastructure must be protected from a growing list of criminal attacks. Although the protective mission may be what people think of when they hear about the Secret Service we are still charged today with the mission of protecting the integrity of our nation's financial infrastructure. In fact our investigative expertise continues to grow and evolve with the ever changing threats and electronic crimes such as credit card fraud, network intrusion, and identify theft just to name a few.

Because a large majority of economic crimes fall within the jurisdiction of the Secret Service we have taken an aggressive stance and will continue to be proactive in the education, investigation and prosecution of electronic crimes. For instance, in the aftermath of the September 11th attacks Congress enacted sweeping anti- terrorism legislation that significantly expanded the Secret Service's investigative authority in an effort to protect our nation's public and businesses from cyber, financial and identity-related crimes. As a result the Secret Service was mandated to establish a nationwide network of electronic crimes task forces. Already established and operational in 15 regions of the country these task forces along with our eight additional working groups provide a collaborative framework in which the resources of academia, the private sector, and local, state and

federal law enforcement can be combined effectively and efficiently to combat cyber threats.

As you know in today's world the financial sector is dependent on information technology and instantaneous telecommunications. So it makes sense that our investigative focus now concentrates on financial crimes with a nexus to computer sciences, information technology and telecommunications.

To say that our world has grown smaller and more dangerous sounds almost simplistic and trite. Today every investigation we undertake has a potential to be international in scope, and most of our investigations are technology intensive. Those of us in law enforcement have needed to re-orient ourselves to the fact that information is no longer just the instrument used to steal or manipulate something of value, rather information is now itself the target. Information is the world's new currency, it has value and it affords access, and likewise it must be protected, and compromises of information must be aggressively investigated.

Two years ago the Secret Service moved from its home of almost 140 years at the Department of the Treasury to the newly created Department of Homeland Security. And I can state for the men and women of the Secret Service when I say that we see our role in the Department as an opportunity, an opportunity for our organization to make an even more significant contribution to this country's national security and the defense of our homeland. At the same time we have long understood the importance of building trusted relationships and working closely with public and private sector entities. We do so for one important reason, necessity. Building an atmosphere of trust and cooperation whether it is with the leaders we protect, the general public, private businesses or our colleagues in law enforcement and the government, is central to the prevention oriented approach that drives both our protective and investigative nations. Thank you.

MS. O'CONNOR KELLY: Thank you so very much. And last, but certainly not least, Rear Admiral John Crowley, Judge Advocate General and Chief Counsel of the U.S. Coast Guard. Admiral Crowley also a long-time servant of the Department of Homeland Security having served as Special Assistant to the former Secretary Ridge, and is the Interim Director of the Homeland Security Operations Center. He serves as principal legal advisor to the Commandant, and oversees the administration of military justice in the Coast Guard. Thank you for joining us.

ADMIRAL CROWLEY: It's always a pleasure, Nuala. Thank you. And Admiral Tom Collins, our Commandant, wishes he were here. We want to thank you very much for your public service in this regard, confident that the rewards are great in public service, thank you. He also asked me to talk about three things, to tell you a little bit about our service, to let you know what his near term management priorities are, and thirdly how they relate to some of the initiatives that are entwined with data and privacy issues.

I'll report back that Deputy Secretary Jackson took care of the first and told you a little bit about our organization. In short he pointed out we're an operational organization made up of ships, planes, people on the ground doing boardings, doing rescues in this country and

overseas. Organizationally though it represents three main communities, a maritime safety environmental protection and security community that deals largely with the public sector, and has for many years. Our Operations Directorate is the community that runs the planes and the aircraft and the people at hand. And thirdly and somewhat recently, is the Intelligence Directorate as a member on our own standing of the intelligence community. That's our operational profile, that's who we are.

To move a little bit into the Commandant's priorities. These are what he has briefed to the Secretary Chertoff, the formulation of the National Maritime Security Strategy per the President's Security Directive number 13. The improvement of the maritime security regime. Establishing improving maritime domain awareness in concert with our partners at the Department of Defense. Establishing and maintaining a layered defense and an operational presence wherever needed in the maritime environment. To establish a sound foundation for our deep water acquisition program and maintain the capability in that operational presence and that layered defense that he would speak about. And finally internally optimizing our organization.

Before telling you a little bit more about some of those things and the initiatives that they involve let me describe briefly what I think the tensions are, the balance are, those terms that have repeatedly been offered to you today. One of the things that we observed after 9/11 that privacy interests, that information became more sensitive more quickly were appeals, processing, even litigation under my world of work were deliberate processes to get the right answer, to do the right thing, because that's what everybody wants to do in a deliberate fashion was the call of the day prior to 9/11.

Increasingly timely information is more and more critical, and we see that in terms of our employee information not only is information that may be subjected to FOIA requests, but it's also information now that establishes credentialing and ensures that someone has authority to investigate a facility that's subject to the law in a timely manner because that facility, that public structure, is also a target. It's not the government it's the nation. And so we must be able to in a timely way, and those identities now are more than information and credentialing, they can also be targets in terms of our personnel within the Department. So the scope of the tension between timeliness and deliberation, and as an operational organization we see things in leadership often as occurring within that 40 to 70 percent ratio of certainty. You can never wait until 100 percent, you don't go with zero percent, it's in that middle, how do you achieve that in increasingly timely manner. Some of the initiatives, HSPD13, the Maritime Securities Strategy.

And we look back at the success of a coherent operational and strategic employment in our counter-drug mission, an operation that specifically is known as Panama Express where we see the unfolding of intelligence and the combination of intelligence and law enforcement information to an operational asset, ships and airplanes at sea to take down to law enforcement measures on both U.S. and foreign citizens that are brought into our court system, convert it to new information and fold it back in to the intelligence and law information cycle again. So we see the success of a strategy that's coherent, that's well mapped out, and that takes data information both making sure that it's valid and making

sure that it's timely, and completing the cycle over again to be operationally effective, that's the model.

Now HSP13 repeatedly refers to the rule of law as being one of the governing principles that are attended to in developing the strategy, and I think that's important as we unfold and look at what that strategy will be. The laws of course include those of freedom and privacy that we value here in this nation.

Next, the Maritime Security regime, we have worked -- the Commandant has worked well with international partners as well as with inside our nation looking at up to 47 major ports, 3100 facilities, 9200 vessels, and somewhere between two and three hundred thousand merchant mariners, and that number varies from day to day and depending on who we look at. You know, immediately after 9/11 we went out and took a round turn on our merchant documentation program to ensure that we had valid licenses for those that were sailing our ships, that we could validate, having done the right background checks and verified that terrorists were not amongst them. You can imagine some of the challenges both in timeliness, in legal proceedings, and in ensuring the validity of information given all the information that's been shared with you so far today. That continues to unfold as we look into the future, and we look towards working with DTS, and TSA organizations on the transportation worker identification credentials. And how that unfolds, the partnering that will be necessary as well with our port partners both state and local in nature, and non-governmental private sector in nature, that they have workers also that need to be credentialed, that need to be verified, because they are part of the maritime transportation system, and also are both vulnerable as well as part of the credibility of the system.

Next, Maritime Domain Awareness, a concept really which provides all source information for the maritime environment whether it be intelligence, whether it be providing and accepting automatic identification signals from merchant vessels, now required at a certain level of tonnage, increasingly going to be mandated at lower levels of tonnage, smaller vessels, around the globe, further from our coasts, including both national and foreign members. We have part of that system, we have our field intelligence support teams working with local law enforcement, working with the port partners to develop the local scene.

We have concepts such as advanced notice of arrival where we have within 96 hours of approach to the U.S. coast requirements to inform us of vessels, of cruise cargo manifests working with our customs and port protection. We've made that electronic in partnership with CBP and in order to provide a more credible foundation, more timely, and also more user friendly for the merchant community. We'll look at layered defense and operational presence and we see it's basically an operational platform as we also leverage our state and local partners and their capabilities within our ports. And the importance of sharing information as it crosses sector and it crosses data platforms to ensure that the integrity and the privacy interests continue to be adhered to once it has left one sector into the other. And finally we have the direction of internal optimization, we are -- as the Department has we have taken their lead and worked at integrating our various communities that I described at the outset of my remarks in the port sector as well to get a better handle on the information going out as well as coming in, in an integrated fashion rather than having

three piece parts out there in our port communities. We have continued to participate in joint interagency task force.

Part of the Homeland Security Act of course was enabling us to continue to work in joint interagency task force and the sharing of information in that sense. And I think that's probably a pretty good summary. It's quite a challenge you have. Again, thank you for your service and we'll look forward to listening and contributing to your work as the days go on.

MS. O'CONNOR KELLY: Admiral, thank you and thank you for your patience this morning. We will resume the open session at 2:15, so please be back here promptly by 2:15. There will be closed administrative sessions, which for those of you who curious are truly administrative oversights, travel briefings, et cetera. So really not of great interest to the public and that's part of the reason they're closed. Thank you so much, and we'll see you at 2:15.

MR. ROSENZWEIG: Nuala, just before we break I just -- on behalf of me I'd ask you to thank all of the senior leaders who came here this morning. I know that we saw a lot of the senior management today and we're very grateful for their time, and I hope you'd express the thanks of the Committee for that.

MS. O'CONNOR KELLY: I will do, and Becky needs to actually close this session, don't you?

MS. RICHARDS: So I move that we close the DHS Data Privacy and Integrity Advisory Committee meeting for the purpose of administrative briefings for the members. We will reconvene and reopen the meeting at 2:15. The open session is now ended, please return and have your green bands on, the doors will open at 2:00.

****

CERTIFICATE OF NOTARY I, GEOFFREY L. HUNT, CVR-CM, the officer before whom the foregoing testimony was taken, do hereby certify that the testimony of said parties was taken by me by stenomask means and thereafter reduced to typewriting by me or under my direction; that said testimony is a true record of the testimony given by said parties; that I am neither counsel for, related to, nor employed by any of the parties to the action in which this testimony is taken; and, further, that I am not a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of the action. This certification is expressly withdrawn and denied upon the disassembly or photocopying of the foregoing transcript of the proceedings or any part thereof, including exhibits, unless said disassembly or photocopying is done by the undersigned court reporter and/or under the auspices of Hunt Reporting Company, and the signature and original seal is attached thereto.
_____ GEOFFREY L. HUNT, CVR-CM Notary Public in and for the State of Maryland

My Commission Expires: _____