DEPARTMENT OF HOMELAND SECURITY

DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE

FULL COMMITTEE MEETING

WEDNESDAY, December 6, 2006

Eden Roc Hotel

Mona Lisa Ballroom

4525 Collins Avenue

Miami Beach, FL 33140

AFTERNOON SESSION

CHAIRMAN BEALES: Welcome back. Our first speaker this afternoon will be Catherine Papoi who is the deputy chief FOIA officer at DHS. She was recently appointed to that position in the Privacy Office where she's responsible for assisting the director of the Department of Disclosure in Program Administration.

Before joining the Privacy Office Catherine was a FOIA specialist with NIH where she worked on agency FOIA matters since 2003. Prior to her career with the federal government, she devoted three years to the Michigan Public Health Institute working on a grant funded project analyzing and cataloguing all available tobacco litigation documents into a single large database, so I'm sure that database is now obsolete!

Catherine, welcome, we look forward to hearing from you.

MS. PAPOI: I have one small correction. I served not only as Hugo's deputy chief FOIA officer, but also as the Director of Disclosure in FOIA. So a double hat.

I'm honored to have the opportunity to address the committee on a statute and on a program that is near and dear to my heart, really and truly, because many of us can look back at our administrative law classes in law school and remember hearing about FOIA, and thinking, "Oh, my goodness, why, why would anybody be interested in this?"

It is an interesting field and I am very much enjoying it.

Within DHS it is very challenging and today let me give you a brief overview of FOIA at DHS with respect to obstacles that we're facing and those ways that we're hoping to overcome those obstacles.

I don't know how many of you are intimately involved within FOIA, but in the private sector, generally, if you are on the other side where they're trying to capture information that's submitted to an agency and they have an agency record as well as in the educational environment where they face that same situation.

I don't know that it is really worth our time to go into too much of a description about the statute itself, but the statute was enacted in 1966 and has been amended several times to accommodate technological advances such as EO amendments, but essentially, it allows the public to request existing agency records and we provide those records assuming there are not any exceptions that apply to any of the information that is in those records.

The whole role of FOIA is to ensure processing, transparency and accountability of the government. Within DHS the statistics are a bit mind boggling. Coming from NIH, things work a little different. At DHS we came in behind the eight ball in the sense of when we stood up we had 22 different agencies all with existing FOIA officers with FOIA offices doing their own thing and along with that came the backlog associated with those offices.

In addition to setting up one FOIA program we also had to deal with all of the various offices bringing together what we're still trying to form a cohesive FOIA program at DHS.

To give you an idea in fiscal year 2005 the federal government received 2.6 million FOIA requests. DHS received and processed about 290,000. The federal government annually in FY 05 spent $300 million on FOIA and DHS spent $29 million.

There is a section in the package that goes through all of the exemptions that apply to the statute and many of you are familiar with some of the various exceptions.

Within DHS, I would say that we deal with probably a good majority except of A and 9, and quite honestly I'm not sure what agencies work with A and 9, but we deal much of the exemption as far as it relates to grants and contracts, Exemption 1, Exemption 2, and Exemption 3, but look through those if you're not familiar with some of the exemptions.

We are required to provide segregable portions of documents after we have redacted any information falling within those exemptions.

In January 2003, DHS became a department incorporating 22 different agencies and we still remain decentralized in terms of FOIA processing.

Each FOIA officer within that component is responsible for that FOIA and they have denial and release authority. They all report to DHS on an annual basis and we're required in February of every year to report to DOJ as a department on our FOIA statistics.

To give you an idea at DHS what we have experienced in terms of the influx of FOIA requests, in 2003 when DHS stood up, we received 161,000 requests.

Those are large numbers and many agencies do not see a quarter of those and the vast majority of those requests are sent to CIS. Immigration Services processes all other requests for the A Files, so, really, the vast majority, 90 percent of our requests are CIS.

In 2004, it went up to 168,000 received and in 2005 it dropped to 163,000. Preliminary numbers, this is as we speak, we're putting together our report for FY 06, approximately 140,000 received in FY 06.

The numbers are decreasing and it is interesting and in a bit I will go over some of the different components and the numbers that are going up in some components and they are going down in others so some of the trends are interesting to track.

Some of the challenges that we face at DHS, as I said, CIS receives the largest portion of requests and actually CIS receives the fourth highest number of requests in the federal government.

The majority of these requests are documents in the A file. I don't know how many of you are aware, but within the immigration proceedings there is not a discovery process as we are familiar with when instead they must seek records for their clients via FOIA.

It's a problem. CIS acknowledges that and shortly I will go into that as well.

In addition, CIS and ICE both process records within the A file. The A file is a shared file, an actual paper file, and right now CIS and ICE are working out there differences in terms of how to most efficiently process those records.

It's challenging, but we're making some progress. Hugo and I have both traveled down to the National Records Center which is the hub of CIS. This is where they process all FOIA requests for A files.

MR. TEUFEL: You should mention that there are millions and millions of A Files in these underground limestone cabinets that have been dug out.

MS. PAPOI: They call it "The Cave" and we really just thought it would be a warehouse.

MR. TEUFEL: Just a dark and dreary building, but no, it's all underground.

MS. PAPOI: Yes, a limestone walled is this cave. CIS and ICE are working together and Hugo and I are becoming very involved in fixing the process.

The CIS backlog as of right now is over 90,000. That's mind boggling. It is to a point at which people have become paralyzed at CIS as to how to fix the problem.

Of course many people feel that more money should be the answer, but Hugo and I are firm believers that the process needs to be changed to prevent further uproar once the money runs out.

DHS backlog. We inherited some once we came to fruition in 2003, but we started with only 29,000 in our backlog, then in 2004 it escalated to 46,000. Then it escalated to 83,000, and as I said in 2006, we are anticipating it will be much higher.

The federal government's total FY 05 backlog was about 220,000. DHS has the majority of about 40 percent of that.

Above and beyond the internal DHS workings that we're still trying to hammer out, on December 14, I do remember that day well, Executive Order 13392 came down from the President titled Improving Agency Disclosure of Information.

The goal was a citizen centered and a results oriented approach that would improve service and performance thereby strengthening compliance with the FOIA.

Within this executive order, it's a double-edge sword coming with a bit of panic on my end, but on the other side some very very good changes are afoot with requirements that will enforce and make the agencies accountable for their FOIA processes.

For example the order requires the appointment of a departmental chief FOIA officer, hence, Hugo's position.

As Hugo mentioned he felt that it was important to add a deputy's position to that chief FOIA officer just to bolster DHS's commitment to FOIA acknowledging the fact that we do have some issues within DHS that we need to deal with as that relates to FOIA.

We have to establish customer service centers, FOIA public liaisons, and we have done so in all of our components and all of the information is available on line. We are to increase our reliance on web-based dissemination of records and the use of electronic resources.

DHS, because we are so new this is going to be one avenue that we need to pursue very heavily. Proactive disclosure is something that not only does it state fair requests, but it is of enormous assistance to the public to be able to go on-line and just automatically access the record that they're seeking without having to send in a FOIA request and then wait several months to receive the document and proactive disclosure is something that we very much an advocate for.

We have been asked to review all FOIA operations, developments of departmental improvement plans and report results. We submitted an initial report and our initial

report actually revealed that we needed to do a very in-depth study of all of the DHS FOIA processes in all of their components.

I keep saying CIS, but there are other components and issues as well.

What we did is we went in and we really evaluated every single component to decide what it was we could do to tweak their systems and what else we could do to possibly develop policy that would apply across the board.

It's large department especially when you have many agencies that have had their own policies for a number of years. So that is a battle, but it's one that we are taking head on.

The last piece is the requirements which is to eliminate FOIA request backlogs. The DHS deputy secretary, and you can view this report on-line at the FOIA web site right off the DHS web site, and in his initial introduction to the report, it indicates that he wants the entire DHS backlog eliminated by the end of calendar year 2007.

That is a very heady goal, but I think we're making progress. We just need to make changes and implement them agency wide, component wide, and leave that support and I think is probably one of the best things to have happened to FOIA within DHS is actually Hugo because he is committed to making the changes necessary and enforcing those changes.

The recent accomplishments within the executive order, as I said, we have appointed our officers, we have established our liaisons, and we have eliminated the DHS headquarter's backlog which is within my office.

My office process is for the Office of the Secretary, DOP staff, the executive staff, all of the higher-level executive offices, and quite honestly, I had a hard time, the component to get rid of their backlog when we maintain a backlog, so that was my first order of business.

In addition we developed the operational improvement plan for DHS and we are currently working on drafting a FOIA policy.

As Hugo mentioned earlier the final FOIA regulations we are still currently working under the interim regulations. They are lacking in some respects, so I think the improvements that we make will make a significant difference.

Basically our targeted improvement areas for FOIA, as I said, it is backlog reduction. The components of the highest backlogs, and I can tell you those are CIS, ICE, FEMA, and I think the Coast Guard also has a relatively high backlog, but quite honestly given the Coast Guard's mission and how spread out they are it's not nearly as bad as it could be. Currently for 2006, they have received 6,000 requests, so that is a very doable situation.

The CIS situation, Hugo and I visited The Cave and in addition we spoke with Dr. Gonzalez and his deputy several times pertaining to our concerns with FOIA at CIS and we're continuing with those conversations.

The CIS Ombudsman's Office is very intimately involved in this process as well and has great concerns. The CIS Ombudsman issued a report back in December, I think it was, available on-line indicating several different areas that he felt could be addressed within CIS to remedy some of the FOIA problems within CIS.

The FOIA backlog, and I apologize for this copying, you cannot read it really, but at the bottom of page 7 it indicates the backlogs, the six of the nineteen DHS components that have backlogs of over 100 cases.

CIS, ICE, Coast Guard, the Secret Service, CBP, and FEMA.

Then it goes on in the next column to talk about the number received in 2004 and received in 2005. That gives you some idea of the numbers we are dealing with at DHS.

Some of the other DHS improvement areas, right now, I guess I would equate FOIA to keeping our head above water, and until this point I was the only FTE at FOIA at headquarters level supported by minimal contract staffing.

We recently hired two FTEs to come on board at FOIA. One will be an associate director of operations taking over for the actual processing of FOIAs at the headquarters level.

The other position is more of a policy position and will be focusing on the lack of policy and developing policy that needs to be implemented throughout the Department.

This person is reaching out to all of the components to get a feel for their willingness to cooperate and hopefully come up with some means by which we can develop policy that we all agree with.

Education and training is something that DHS is lacking. Many departments have some very comprehensive training programs within FOIA. This is something that each and every component goes through because the day you put your foot in the door at the agency you're aware of agency records and your responsibilities under the statute in terms of records retention and in terms of searching when you receive FOIA requests, et cetera, so those types of programs need to be set up at DHS.

Technology Improvement. Right now we are working with a very elementary system. It tracks requests in terms of we know what is coming into our door. We are not pushing it. We track what is coming in the door and we track what is going out the door. Really, that's about it.

If you have any experience in the FOIA field, then you know that there are some very advanced systems that are available that not only redact documents, but transmit documents, and of course that's going to speed up the FOIA processing.

Those are some pieces that we are looking at to hopefully implement that at DHS, and at DHS, meaning, within their component levels as well.

At this point, what I can say is, and I have said it before, Hugo is the greatest supporter of FOIA at DHS and I thank every day that I have him on board. He is more than willing to step up to the plate and tell the leaders what we need to make changes and have a successful FOIA program.

The executive order that was issued on December 14th strengthens our cause because it does require the Secretary to report up, but at DHS we reaffirmed our commitment to improve operations within FOIA and we are more than willing to acknowledge the shortcomings. We will eliminate our FOIA backlog and that goal is the end of calendar year 2007 and DHS leadership is conveying emphasis on the importance of FOIA across the Department.

Many of the different components, for example, FLETC, CBP, US Visit, all of their leadership initiate memos to the various offices indicating that this is the priority and is not something that can be pushed aside.

We at DHS continue to embrace technology, and as I said, we are really encouraging some sort of a department wide software implementation and we have been looking at some different systems and hopefully we will be able to come to some resolution shortly.

That about sums it up for our FOIA program at DHS. We do have a colored chart that is available in the back and I must offer this disclaimer that these are initial numbers. +This is for fiscal year 2006 reporting and it is due to DOJ on February 1st, and as I said, my staff is currently working on assembling these numbers and this is what we have thus far, but it does give you an idea of what we are looking at.

It's interesting that ICE went from 4,000 requests received last year to 9,000 this year. FEMA went from 400 last year to 700 this year and a part of that was Katrina and that was a huge hurdle.

Quite honestly, I have to say that I think it was a good test for FOIA at DHS and I do think our office working in tandem with OGC we were able to pull together and effectively process the Katrina FOIA requests.

CIS, interestingly has gone down. They received 138,000 in 2005, and now they are down to 109,000 in 2006. Yes, it is interesting or at least I find these trends to be interesting and time will tell what happens, but we will have our final report out by

February 1st to DOJ and then DOJ posts it on their web site and we also post it on our web site.

Thank you.

CHAIRMAN BEALES: Thank you very much, Catherine. John Sabo.

COMMITTEE MEMBER SABO: Thank you, Catherine. I have a question on distinguishing for aliens, the Privacy Office and the Department at one point determined that they would treat aliens with the same sets of policies as the Privacy Act provides to citizens.

For purposes of these FOIA requests when you say alien file are these all pure FOIA, that is, they are not individuals whose information records are being maintained about them or are these primarily from third parties?

Could you just provide some characterization because it is a little bit confusing. As to the Privacy Act, I can make a Privacy Act request for my records and that is not a FOIA request in other agencies, so could you clarify that.

MS. PAPOI: Well, actually, interestingly at most agencies, including DHS, if you make a Privacy Act request it is also processed as a FOIA request.

As it relates to CIS, and the A File, the requests generally come from the attorneys who are representing the subject and it's treated as a FOIA and a Privacy Act request and processed as such.

MR. TEUFEL: To the extent that the Privacy Act is going to apply because obviously if the person is a non-U.S. citizen or it's done by proxy is not going to apply, but generally speaking in this context as Catherine indicated it is counsel for the individuals who are making the requests under FOIA to get the information in the A Files to use them to represent their clients with before administrative tribunals.

COMMITTEE MEMBER SABO: Just a follow up. Some portion of them, this work with the Privacy Act requests from individuals who are seeking information from their own records, that's what I am trying to see if they are all lumped together or are separated because that is a distinguishing characteristic the right of access under the Privacy Act unless you have one of the exemptions.

MS. PAPOI: Absolutely.

COMMITTEE MEMBER SABO: That is important because we talk on the committee about redress and accountability, so do you break that out statistically?

MS. PAPOI: At CIS I don't believe they do break that out.

MR. TEUFEL: I don't think they do.

MS. PAPOI: Yes, and I should point out that CIS has a system called FIPS, I cannot right now recall what that stands for, maybe it's FOIA Information Processing System.

MR. TEUFEL: Very slow and it is expensive.

MS. PAPOI: Yes, and does not necessarily kick out the information that we need, so possibly some of the information that you're looking towards is just not captured within that system and they would not be able to provide those numbers.

Within CIS, the CIS ombudsman has conducted a report. We had sent down a team for a week out of our office to get a feel for the Records Center and for processing within the Records Center, and hopefully we will soon be able to issue some recommendations and FIPS is one of those areas of concern for that very reason. People want to know exactly how these requests are being treated.

MR. TEUFEL: Did you mention the CIS ombudsman report as well?

MS. PAPOI: I did.

CHAIRMAN BEALES: Joanne McNabb.

COMMITTEE MEMBER MCNABB: Thank you. I see on your longer slides on page 8 you mentioned that one of the things that you're looking at on technology is an electronic redaction solution and that also you are interested in increasing the practice of proactive document posting, there are definitely privacy concerns about public documents being posted on-line because of the personal information in them, so are you looking at having automated redaction of the documents you post on-line?

MS. PAPOI: Really, we're talking two separate situations. For instance, we have many competitors that will send in FOIA requests for contracts that have been issued recently and we will receive 30 requests for that contract, so clearly there are some exemption FOIA concerns and we have to comply with Executive Order 2600, so that that contract goes through the FOIA process, but once it has been cleared through the FOIA process we make that proactive posting available so everyone can access that document on-line.

When you're talking about something where there are Exemptions 6 concerns, and that is personal privacy, absolutely, something of that nature would be taken into consideration before we post any sort of a document.

A proactive document posting generally refers to contracts, any sort of an agency final decision, something about broader range of interest not necessarily relating to one particular individual.

MR. TEUFEL: I am just concerned with your question when you said automatic redaction which would suggest the lack of human interaction or involvement in redaction and that is not what I believe we are looking at doing.

So there would be a human being who would be looking at what is being redacted making sure that the right things are being redacted and that the wrong things are not being released to the public and not being put on the Internet.

COMMITTEE MEMBER MCNABB: If the two items are separate which I can kind of understand, so one item on the improvement area is electronic redaction.

MR. TEUFEL: As opposed to taking a highlighter and sitting down with a piece of paper and then take that to a photocopier.

COMMITTEE MEMBER MCNABB: Yes, so it's not exactly automatic, but as you said, you set up the system so that when it prints it out, it automatically covers it or it deletes it.

MS. PAPOI: Exactly, and there are so many advanced systems now where you can go in and redact electronically.

COMMITTEE MEMBER MCNABB: You have had some implemented?

MS. PAPOI: We do not within DHS headquarters. Some of our components do and have had great success. TSA uses the redaction and some of the problems that we are facing as it relates to identifying an electronic solution is just because of so many of the various components that have already an implemented system and they are not willing to explore other options or what we're looking at doesn't meet the needs of their mission because they are such different missions across DHS.

For my purposes, I am old school and I like Post-It tape because you cannot see through it, so my office is still using that until we come up with an electronic redaction system that's fully safeguarded.

Some of you may be aware of the Russ Kick incident where he was able to uncover some electronic redactions and were made via Adobe Acrobat and then not taken to the next level, so we certainly don't want that.

MR. TEUFEL: There are some systems where if there is consolidation in the Department they are not likely to go away, and with CIS and FIPS, because of the amount of time and money they invested in that system doubt that that will go away. I anticipate that there will probably be a consolidation down to maybe two or three systems.

Again, I do apologize because of the other aspect, the privacy side of the office has been working with today, so that if I am duplicating what was said, I do apologize, but some of the components are very innovative and come up with some low-cost solutions.

The Executive Secretariat has a solution that we have looked at and we are looking to see if we have got the funding for and then we will be talking to the component to see if they want to join on board.

Obviously it is easier if we are all on the same system we can better coordinate whenever there are FOIA requests that are cross cutting, but at this time I don't see there being any plans on having everyone use the same system across the board.

MS. PAPOI: Maybe in 30 years.

MR. TEUFEL: Yes, and often I have talked with a number of folks on the committee individually about the emerging culture of the Department and the subcultures of the various components.

Yesterday was a great example of a subculture that is very supportive of the larger entity.

If you will take time to do that, and there are so many things that we can accomplish, there are so many battles we can win, and frankly there are times when different systems may make sense.

For instance, with the Secret Service they have a very unique mission, so it is easy to see that they will be somewhat different, and CIS, because of the time and the money they have invested.

With a lot of the others, there are good reasons why they would want to jump on board with whatever we do or we may want to use what they are using and convince the other components that they should come on.

MS. PAPOI: In CIS when they first implemented FIPS back in the 1990s it was really cutting edge, but unfortunately there have not been many updates since that time so unfortunately we learned that it may be more of a hindrance at times than it is a good time-saving solution.

Those are some of the ideas that we are looking towards, as I said, that tweaks. When we met with Dr. Gonzalez the concern was, We just cannot get rid of the backlog overnight, but some times all it takes is maybe a list of small little changes that will add up to quite a large difference in the long run.

COMMITTEE MEMBER MCNABB: It sounds like the CIS has some operational problem rather than a processing of FOIA requests that somehow people are not getting the documents that they need in order to do what they're doing with CIS.

MS. PAPOI: That is one of the reasons Hugo and I sent a team of extremely qualified FOIA professionals down for a week to diagnose where the problems were occurring. Was it in intake or was it obtaining the records they need? Is it the processing?

Is it the approval? What are the hang-ups? That report is currently being drafted and should be very enlightening.

CHAIRMAN BEALES: Catherine, thank you very much and we wish you success in this effort. This is obviously an important thing for the Department to try to get on top of. We do appreciate your time and we look forward to hearing about your progress.

Our next speaker will be Dr. John Talburt from the University of Arkansas at Little Rock speaking to us about data integrity.

Dr. Talburt is professor of Information Science and sits on the chair of Information Quality at the University of Arkansas at Little Rock. He is the graduate coordinator for the Master of Science and Information Quality Program. He also holds appointments as director of the Laboratory for Advanced Research and Entity Resolution and Information Quality. He is associate director of the Acxiom Laboratory for Applied Research and the co-director of the MIT Information Quality Programs Working Group on Customer Sentry Information Quality Management. Dr. Talburt has published numerous articles related to Information Quality and Data Integration and is an associate editor for the newly created ACM Journal of Data and Information Quality.

Dr. Talburt, we heard great things about you at our last public meeting and we look forward to hearing from you directly at this one. Thank you very much for being with us.

DR. TALBURT: Thank you, I appreciate the invitation. It is certainly an honor to be here. I hope that my remarks might be helpful to this committee. I suppose I should blame Jennifer Barrett for the invitation.

I always enjoy the opportunity to talk about information quality. You asked me to come and talk about data integrity and data metrics.

The way I would like to approach that is from the framework of information quality because I would like to make a case that data integrity fits within that framework, and if you subscribe to that then it does provide a means where there is a very large emerging body of knowledge in the area of information quality that provides a lot of support in terms of processes and methods and techniques for managing quality of data and also for developing metrics, so I certainly do not come there today to tell you what metrics you should have, but simply to try to perhaps give you some guidance on how those could be developed and certainly I think they should be.

Any organization that depends on information such as DHS and the different units of it should have in place some kind of quality control related to data.

Data integrity I view it primarily as having two main aspects. One is sort of the protection of data both in the sense of not letting it be tampered with and preserving it. A

very big component of it is backup and recovery especially disaster recovery is very important.

There is another aspect of it also that's more the traditional computer science view of data integrity having to do with integrity rules and constraints or business rules around the data that should be enforced.

Certainly those of you who have dealt with databases you have integrity rules with referential and domain integrity, so in my view that is how I see data integrity and I will talk a little bit more in terms of having read your mission statement and how I think it relates to, again, the broader framework of information and data quality.

I keep saying information and data quality, but these terms are quite interchangeable but they are like many things. No one wants to let go of one or the other. I certainly prefer information quality as the term because it seems to have a broader connotation.

Certainly at the level of data that you can make the distinction between data and information, and that's really the value change of intelligence and knowledge, but when you're talking about the quality of it those differences primarily somewhat go away. In terms of talking of quality you talk about all the same things that apply whether you talking about data or information.

Of course really it comes out of the total quality management movement of the last several decades and in some sense you can think of it as the application of TQM to information systems.

The working definition for information quality is the fitness of use the data for a particular application and that has some ramifications in terms of quality then must be measured in context of what you are using it for. The same set of data, the same database, in one of your departments, for one use may be a very high quality in certain aspects, but low in quality for other types of applications so you always have to view, the quality of the data or the information in terms of its ultimate application as far as the gerund principle of "the eyes of the beholder."

Getting back to data integrity. In looking at the broader view of information quality, or data quality, it is a multidimensional concept. I suppose you have the handout. If you will look on Slide 6, this is sort of the traditional, well, I should not say traditional as there is not too much of data quality that traditional involved as it only emerged in the last 15 to 20 years, but the sort of the breakthrough and the understanding about data information quality is that it is multidimensional.

Most people when they think about that think of accuracy, but this framework there are about 16 dimensions where different people have different ways of breaking it down, but this has sort of become a standard, if you will.

This was developed out of the MIT information quality research and they break it down into some 16 different kinds of dimensions of accuracy, believability, reputation, access, security, value added, et cetera, et cetera. So there are several of them.

CHAIRMAN BEALES: If I may interrupt for a moment. Becky, we do not seem to have in our notebooks this presentation.

DR. TALBURT: Forgive; being a professor I am used to speaking from notes and slides. I am not trying to lecture you, although it may sound that way.

CHAIRMAN BEALES: Even though we may need it. I think we're officially ready to roll again.

DR. TALBURT: In any case, on the first page in the corner, Dr. Wang who was at MIT one of the researchers who came up with this, there are some 16 dimensions that are typically now used as the standard dimension for information quality in four different categories.

What I thought I would do is to briefly, and again, I'm trying to establish that the data integrity fits within this framework and as a matter of fact if you will look at five of those dimensions they address several of the issues as I understand it of this committee related to data integrity.

For example on Slide 7 it is talking about the dimension of accessed information. Certainly that relates to privacy and confidentiality of information and security of information certainly in terms of use, limitations, and data protection, this idea of tampering, altering, and data preservation, backup, and disaster recovery.

Also there are some other things that I saw in your mission statement. Timeliness, certainly, that's a major dimension of information quality and the removal and destruction of obsolete information I think falls into that category and accuracy, of course, removal and destruction of erroneous information and then consistent representation gets into this broader issue of enforcement of rules and constraints and data inoperability.

Given then that those cover pretty much what you're thinking in terms of data integrity by the committee, then I think it fits very well into this broader framework of information quality.

From there what I would like to talk a little bit about is how you then produce the metrics or information quality and consequently what could be produced for data integrity as well.

I took those same dimensions briefly where there are some things that come out of the literature mostly out of the newspaper.

A good friend of mine, Dr. Tom Redman, who has done a lot of work in the area of data quality who has several books out scheduled a talk at our school and he said, If you really want to find out about the impact of data quality just read the newspaper everyday, and certainly the many many articles, and as you can see from some recent ones, the house that was actually evaluated at $400 million when it was a $121,000 house.

This is interesting and I gave this to my students because it illustrates a lot of things. First of all, obviously there were access and security issues where there was actually an abstractor who was in the assessor's office and just kind of stumbled on the right keystrokes that changed the valuation to $400 million and didn't know how to get out of it, or didn't think it would stay in there, but it went in.

The other interesting thing is that they used that, of course, then to run the tax assessments and project all the revenue and taxation and right after they did that they found the error so they went in and easily corrected the error that was in the database, but its impact remained because they did not, shall I say, redact or revise their projection even though they had corrected the initial error.

So there was a lot of grief later when all these different agencies of the town had to start letting people go because they didn't have the revenue they had anticipated. You can read those because I will not dwell on them.

Let me talk a little bit about information quality management starting with Slide 14.

A couple of important formulas and one of them is E=MC squared which is Einstein's formula for energy. In our business we often use in IQ's MCQ. This is very important because perhaps one of the most important principles in information quality management is you need to view information as being a product rather than a by-product.

So when you view it as a product you have to take into consideration all aspects of it from the collectors of the information, the sourcing of that information, the custodians of it, the people who are using it for operational purposes, building data warehouses and then ultimately the consumers of that information whether it be officers in the TSA or citizens.

Finally over all of that the management of those systems. This is a principle taken from TQM.

The other thing is that most organizations unfortunately have sort of a tactical approach to information quality management and that is more of a management perception where bad things will happen.

For example, there was discovery of some problem of a Palestinian bomber episode that happened a year or so ago with a bank offering credit card applications and

somehow in their files a person's name had been changed it was entered as this Palestinian bomber and they offered a credit card to that person.

Often these things are discovered by the consumer and then there is a great effort to go in and correct it try to fix it and what that lacks is any kind of anticipation or measurement.

Of course what we advocate is the taking of a more strategic approach to this information called management and again based on TQM principles where you actually assess the information quality periodically and monitor it so you can avoid some of these unpleasant surprises.

It also entails where you develop some kind of goals and requirements for that quality should be. You take measurements of those. So this is where the idea for metrics came in. Then obviously it is a good thing if you're not meeting your goals or there is room to improve that you take some analysis of what's going wrong and try to implement some kind of improvement.

This brings us then to the idea of metrics. Metrics are just functions, if you will, a mapping of the state of your information into numeric values as being just a way to measure it.

Of course, obviously, you assume there is some kind of relationship that as the number increases of your metric then that means your quality is better or it may have an inverse relation, for example, timeliness, if you are measuring time to deliver smaller numbers would be better, but there is some kind of a direct relationship.

Dave Lotion who is also another person who is very active in this field published some characteristics of good metrics. I will go through all of those, but certainly clarity of definition is very important and that they really relate to your business or your organization's goals is what you are trying to do and you also have the capability to drill down into them so you can analyze any potential failure.

Some of the key metric parameters are once you have requirements for a particular aspect of data quality for your metric you set up what is the maximum value you can obtain and the minimum value, but what you are really focused on and what are you trying to get to and at what point do you have failure, at what point do you say you cannot tolerate that, so that that may not necessarily be the lowest value.

One way to look at biometrics and probably two of these may be applicable to the situation here is you have controlled metrics and improvability metrics.

Controlled metrics are those where basically you don't have a span of values between the failure and the goal. You have to maintain a certain level at all times and

once you fall below that then you fail automatically, so you have to stop whatever the process is and that is a red flag immediately.

However there are many other aspects of information quality where you have improvability, that is, you know you are not at the goal, you want to make things better, or maybe it is getting into this backlog of FOIA requests, so you track and measure and use that as a way to determine where you are.

You also have composite and simple metrics where you can be tracking a single aspect of the quality, oftentimes you roll several of those together and you are looking at many things at once.

Another aspect is normalizing metric values. This is because since each metric is unique and it will have its own separate goal and failure point, when you look at them in their raw form you may not be able to determine the comparability of it.

For example, if I give a value of 77 percent and you're trying to get to 80 and your failure point is 60, is that any better or worse than a value of 88 percent where your goal is 95 percent and your failure is 80.

From that you can develop a number of what we call scoring algorithms that help you normalize or rationalize metrics so that they become comparable across systems.

This is very important when you are implementing across the various points and information flow or especially if you are implementing across various departments is to have a way to rationalize or to normalize so that everyone is working from the same page.

On top of scoring, oftentimes, and you are probably very familiar with this is, you can put Rubrics on top of the scoring to simplify it further with the idea of coating things with colors.

One that we've used quite a bit is this Rubric of the grade point average of zero to 4.0 which is something people can relate to so you can map your metrics into those kinds of values.

Let me briefly mention score cards which is simply a way to assemble the metrics that you have, put them into a form that's somewhat digestible so you can monitor these things, again, being very strategic about it instead of waiting for failures and trying to anticipate problems.

That brings up another very important principle of information quality management. If you subscribe to the fact that you treat information as a product for a consumer or a customer, then you really need a blueprint of that product, you really need to have ways to map how that product is produced from its sources and from the various processes that take place in order to get to the final result.

Once you have that, then you can come to something what looks like on Slide 31 which is sort of a score card metric architecture, whereas, you look at the flow of data throughout the system.

For example, some of the systems you have talked about today, you can identify what we call key touch points which are points typically in places, for example, where data passes boundary from one system to another where there is some irreversible transformation that has been applied to the data.

You then identify touch points and establish what should be the quality metrics that you want to measure at that point, take those measurements, and typically they are stored at some kind of repository, you build a score card from that with different levels of score cards for that particular process for that department which can be rolled all the way up to the highest level to let people view what's going on and then from that make decisions about what are kinds of analyses or improvements that need to be undertaken.

Simply put on there are some examples of different kinds of representations, different school card systems, there are many that are commercially available, systems can be developed, and I guess overall is, the idea to implement, you have to have some kind of map of the flow in your system and identify the touch points and then develop the requirements and create metrics. With that, are there any questions that you may have?

CHAIRMAN BEALES: Thank you very much. That was a very valuable presentation. Larry Ponemon.

COMMITTEE MEMBER PONEMON: A nice presentation. Thank you. I have a question for you. I like the idea of metrics and it makes a lot of sense to me intuitively. What happens if data is used for different purposes, the same data, but say you have three uses where one might be around a marketing application, one might be an attendee validation or verification/application, the third might be just like an ERP, some internal accounting type thing.

How do you use your model, your framework, when you have different uses?

DR. TALBURT: As I said in the beginning you have to develop different metrics because, again, the quality, and I think that's something I see a lot of in practice is that people think of information quality as being totally intrinsic to the data, so they have just one measurement and it's intended to for all subscribers.

As you pointed out, that is simply not true, so the same data does need to be measured more than one time depending on a measurement custom for that particular application, so in that case I would say you need three metrics and probably more than that because you typically will be measuring different aspects for each of those applications.

CHAIRMAN BEALES: Jim Harper.

COMMITTEE MEMBER HARPER: I agree with our chairman. This is a very valuable presentation. It has helped me with my thinking about these issues. I am a big fan as are many of my colleagues they know of using the right terminology, some careful terminology, because if you can't get on the same language you cannot have a good conversation about things and reach good quality results.

I want to pick up some basic terminology that is sort of the hierarchy that I had thought I heard you say, I don't see it represented in the slides, but I think you talked about it in a sort of hierarchal fashion of data information, intelligence and knowledge and how the data is sort of the base to build from there information, intelligence, and knowledge, so could you sort of expand on your thinking about how data quality and relevance come together as you go through that hierarchy?

DR. TALBURT: Yes, I was simply referring to sort of the basic hierarchy of business intelligence and data management applications where you start with source data, you do some transformations to create more usable information data in context of other data and then derive intelligence from that, and ultimately, in my view anyway, the purpose of any analytical system is to enable decision-making which is ultimately what you are after.

So I would put decision on top of that, but I would say then that the information quality framework, again, the reason everyone has all of these synonyms, when you are measuring it from a quality standpoint, the same framework will work on all of those.

Even though we may make the distinction amongst those from their intrinsic standpoint from measuring their quality, again, the same framework will apply and that you simply need to look at what are your faulty requirements, and as a matter of fact, the decision on this one is very important is measuring the quality of the decision, but you can use the same framework to do that. Did that answer your question?

COMMITTEE MEMBER PALMER: Yes.

CHAIRMAN BEALES: Let me ask you to think about a particular example and talk about what you might think of as appropriate data metrics.

One of the problems this committee has looked at is matching names against a watch list. I suppose we could take the watch list as a given, although the data in the watch list is itself problematic in some respects in that there are mistakes and if there are names misspelled, there are all those kinds of problems with data.

We have another source of name information that's coming from an airline passenger assistant and we somehow have to match the two, but the decision we really care about is the match, but we care about the quality of the information in the watch list

database, we care about the quality of the information in the airline name database and whatever other information we may have that is coming from the airline.

I'm just wondering what kinds of metrics you might see in that process so we can start to think about what does data integrity really mean and what does data quality really mean in that particular problem.

DR. TALBURT: The two cases you talk about, again, I would be reluctant to subscribe to wanting to go in and do too much with those databases themselves because probably those are given.

I mean one could say, I want to measure how faulty the airline or the watch list data are, so what you're really after is you're after the quality of matching as I understand it.

CHAIRMAN BEALES: In some sense that's the ultimate goal, but for Secure Flight, for example, where DHS will eventually be asking the airlines for what information it wants, it has got some control over what is in that information, at least, potentially, so that is part of the problem where more information presumably gets a better match, so that's part of the trade off and is part of the quality issue.

DR. TALBURT: In that case, I would say you've mentioned a couple of aspects that could lend themselves on that, one being monitoring the quality of the airline information in terms of its completeness and accuracy and coverage to be sure that you're getting all the information.

You brought up an interesting point and I heard it brought up earlier today, again, you don't want to get the idea that you're just measuring quality for quality's sake because you're trying to measure quality because you believe that it has some type of impact.

For example, you're saying that you believe that the better quality data that you get from the airline, and there are ways to measure that, but ultimately what you want to do is to correlate that with the impact that it has in terms of the matching.

I would look at what are the factors that give me better matching of the airline related to the watch list and start looking at those. Those would be where I would focus on metrics.

I could measure a lot of things on the airline data, but some of them and probably many of them wouldn't get me any farther along in terms of what I am ultimately after which is better matches to the watch list.

That's all I am encouraging is that kind of thinking, I guess, the very basic of the ends in mind, or in other words, what is the application of the data going to be and that should then drive where you tend to look at what aspects you want to measure because it

is very easy that I find often in practice, Oh, yes, we have a lot of data called neumetrics and they tend to measure things that are just easy to measure, things that they are already measuring and they put those forth as their data quality metrics which is okay except oftentimes those do not necessarily have any impact on the business value.

CHAIRMAN BEALES: We should sort of start by thinking about the business process and business application and then think backwards from there about sort of where could data mistakes screw this up, this is what we would like to measure.

DR. TALBURT: Absolutely.

CHAIRMAN BEALES: Joe Alhadeff.

COMMITTEE MEMEBER ALHADEFF: When you look at various data sources depending on what their use is for and how it was collected and why it was collected and whether it was original data or data that was collected by another party who was observing something, you have data that can be more subjective or more objective as the root of what you are going to make decisions based off of.

Are there different analytical frameworks based on subjective and objective data or do the same kind of metrics and analysis kind of work for both?

DR. TALBURT: Since there has not been extensive work done most people use it for both, but certainly there is a difference and that is a really an interesting area now of research and development in the area of information quality having to do with what they call data lineage or data pearl nuts, the idea of the traceability of the reliability or credibility of data through the chain so when you get to a summarization of that data for a decision you want to know: How did you get to that point? In terms of what is your level of confidence?

There is a lot of research work going on, but there are not a lot of things that are available for that right now, but they are typically treated the same, but they shouldn't be.

CHAIRMAN BEALES: Are there any other questions? Dr. Talburt, thank you again very much. We really appreciate your being with us, but we have one committee later this afternoon, good, so we will look forward to having a further discussions with you.

COMMITTEE MEMBER MCNABB: If I could ask? Could we get an electronic version of this so we could make it bigger?

CHAIRMAN BEALES: Which makes it colorful. We will move now to our subcommittee reports. I suppose we will start with the privacy architecture subcommittee with Joanne McNabb.

COMMITTEE MEMBER MCNABB: We left yesterday with a very profitable discussion with Commissioner Stoddart in which she explained to us a lot about her office's proposal for updating the Canadian Privacy Act which actually said this morning is modeled on the U.S. Privacy Act of 1974 and we think what we learned in the media and the process they're going through will be useful to us as we continue on our project with the NIST Information, Security and Privacy Advisory Board on reviewing the Privacy Act and privacy regulations in light of the new technologies and information management practices, so we expect to be doing some more work on that in the next few months.

We are also beginning to receive some information from DHS on the DHS procurement processes which will be helpful in another effort we have going on determining whether privacy considerations are being raised early enough in the procurement process particularly for new technology and systems. So we have got ongoing things but we do not have any documents ready to bring forward at this point.

CHAIRMAN BEALES: Are there questions or comments? The Data Integrity Information Protection Subcommittee. Charles Palmer.

COMMITTEE MEMBER PALMER: Thank you, Mr. Chairman. The subcommittee, as many of you know has been spending quite a bit of time working on our report on the use of RFID for human identity verification. We are pleased to say that our next draft is available in the back as well as to members of the committee.

I have to begin this comment with thanks to the subcommittee and to the members of the full committee for their hard work on this, in particular, two members who not here today Reed Freeman and Lance Hoffman who were not able to attend.

The committee's comments we have received over the last few days have been absolutely enlightening and have added to the overall quality of the report and will help ensure its success which is what we all wanted to see.

Just as a remainder. The purposes of this paper, this is not an RFID tutorial, it is to offer a framework by which DHS might determine whether or not to deploy an RFID enabled system to identify or record the presence of an individual and to offer its best practices to consider when DHS is choosing to use such an RFID system.

The paper tends to focus on border crossing contexts, however we think the issues and best practices related in the paper would be equally relevant to other credential or human identification applications.

We recommend in the paper that DHS carefully weigh the considerations that we provide when they go to deploy such a system.

In very brief form, the two key findings: The RFID system should be secure and narrowly tailored to effectively accomplish a specific objective and it be the least intrusive to privacy and security in like alternatives otherwise the use of RFID standing alone may not be the best choice or best suited for purposes for identifying an individual, so other solutions should be considered.

The committee further recommends that if the Department determines that deployment of the RFID system is appropriate that it build in from the design stage the safeguards outlined in the report to the extent possible to ensure that it does indeed advance the mission objectives as well as respecting and protecting privacy and secure the information collected.

I would ask of the full committee if there are any comments or discussions on the draft.

CHAIRMAN BEALES: Before we take comments I would extend my thanks to you, Charles, and to the rest of the subcommittee because I know there is a tremendous amount of work that has gone into this paper and given the extent of public comment that we have gotten and the extent that interest in this project has been more difficult than usual you have done us all a great service. Jim Harper.

COMMITTEE MEMBER HARPER: Thank you. I want to extend my congratulations and my thanks to Dr. Palmer for his hard work and patience under a variety of pressures.

Many of us don't know very well what it is like to hear his soft-spoken fury, but I suppose I have been at the other end of it once or twice during this process.

If I were the sole author of this paper I would have made it quite a bit stronger. It is a tribute, again, to Charles Palmer's patience that he tolerated my attempts or my continued efforts to strengthen the paper, but resisted overstatements that he was not comfortable with that committee maybe should not adopt.

Let me suggest that there are two audiences that really need to take this paper to heart - they may not be here - but all of us who helped to carry the message of the paper to them.

The one audience is the RFID provider community who, I think, came to us after the first draft was released and said, You really don't understand the technology, and to the extent that that community was saying that they really don't understand the identity and securing of privacy issues.

This is as carefully considered a paper as this committee could put out and that group means to learn from our work rather than pushing back against something that is a product of ignorance.

Secondly, the DHS components that are working on RFID at this point need to take this paper to heart. They came after the Privacy Office and our committee to some degree after the draft was released not having taken to heart what is in here and they also need to study carefully the information we put forth to them.

This is an opportunity for them to do right by the technology and by the country and its people and by accepting and learning from what we have put forward of Charles Palmer's and many other people's yeoman efforts have put forward would do them a very good service.

I endorse the paper and I do appreciate the work that has been put into it. Thank you.

CHAIRMAN BEALES: Joe Alhadeff.

COMMITTEE MEMEBER ALHADEFF: Well, Charles should be used to this because when Jim speaks and I speak Charles gets a headache between the two of us, but it's part of the way it works.

Let me pick up one thing that Jim was talking about and that was what a lot of people focused in the early version of the paper on what was perhaps a drafting deficiency of the paper in the way it presented some of the issues of some folks jumping to the conclusion that the paper was in some way an implication of the technology as a technology when it was dealing with the technology as a application in specific circumstances.

One of the problems that we see when we look at the issue is people have not spent the amount of time to actually articulate why they see the benefit of the specific technology in the specific application versus other technologies that may do the same thing and we saw some of that going on with the idea of their contact versus contactless card and how fast you can or you cannot get a reading, and what level of study was done related to that question and what were the alternative technologies.

Not enough of a statement is done on the benefits, like, Well, it's just not prepositioning of information to get someone through a gate faster, but it is also for the security of the officer because that actually may have a more tangible and realistic benefit than whether or not there is another three and a half seconds in line or not.

I think as people start to develop PIAs in this phase and start to work on this phase they really have to start taking more than a 360 degree look at these issues and make proof across a broader range of the issues.

We highlight some of the safeguards that can be also highlighted as one of the ways in which you thought about the issues and addressed them in terms of making the appropriate balances by saying, We thought that there might be some dangers and we

have addressed the dangers by using encryption and by using certain protective measures, et cetera.

One of the things that the report is reflecting is the way information is being presented and in some cases the way technology is being justified as being insufficient so far. It's not at the end of the day that it may or may not be beneficial.

Jim's point is right. People have not thought the issues through, at least, in the way they are reporting about them, so more needs to be presented on that in the way they are reporting so that there is a better understanding of the benefits, the risk management, the balancing, and why the conclusion was reached.

CHAIRMAN BEALES: Tara.

COMMITTEE MEMBER LEMMEY: As a quiet member of the committee watching many rounds go by it's a real testament to the committee as a whole in how much work went into this and I do applaud everybody who is on it.

One of the issues that we saw through this because it came out of emerging technologies is the desire on the security side to apply new and emerging technologies rapidly to help with the security issues and not really thinking through the application compliance as much. There is a very strong desire on all parts of the government, not just DHS, to aggressively address technology as much as possible and a nice thing about the committee is that many of us who are technologists really like to take a step back and try to figure out what the appropriate technology is at the appropriate time and not get caught up in the use of the technology.

As the committee goes forward and as the Department goes forward that will be a critical issue of always saying, “Just because you can doesn't mean you should”, And with technology that comes up a lot.

This is a good example of the kinds of papers that should come forward on the emerging technologies.

CHAIRMAN BEALES: Are there other comments? If not, I will entertain a motion that the committee adopt the report that has been submitted by the subcommittee.

Somebody has to move it. John Sobo moves. It's seconded. Is there any further discussion?

If not, then all in favor of adopting the report, please say aye. Any opposed?

The report is adopted.

Is there anything else Charles in your report?

COMMITTEE MEMBER PALMER: No, I cannot imagine anything else that we might have.

CHAIRMAN BEALES: John Sabo.

COMMITTEE MEMBER SABO: Now that the report is adopted, I have a comment on adopting reports.

It would be really great to see our reports especially where we have guidelines and very specific recommendations in the form of bulleted questions, and lists used, so I would ask the Department and the Privacy Office to encourage its use particularly in the development of new programs where the architecture has not yet been selected and then give us some feedback as to whether or not it was used and if it was usable.

We did our framework but I don't have sense that the framework has really been used for anything although our analysis framework is a valid approach, for example, the risk of identification.

That's my request that as we adopt these that are specific and not general white papers, but they are actually used. Thank you.

CHAIRMAN BEALES: Lisa Sotto.

VICE CHAIR SOTTO: Along the same lines as John commented, I would echo those thoughts and add to them in that none of these papers are static.

We know that privacy and data security issues are moving incredibly quickly so within a few years these types of papers may in fact be obsolete or may need substantial revision, so I would encourage us to consider these as dynamic documents and we consider them on an ongoing basis as need be.

CHAIRMAN BEALES: We turn now to the report of the Data Acquisition and Use Subcommittee. David Hoffman.

COMMITTEE MEMBER HOFFMAN: Thank you, Howard. The primary work of our subcommittee over the past few months has been in developing the draft report on the use of commercial data and we are proposing that to the full committee for adoption at this time.

I will give you a brief summary of the current draft of that paper. The paper builds upon the prior work of the subcommittee and the prior document that was adopted by the full committee on the use of commercial data to reduce false positives in screening programs and that prior document concluded a number of things and recommended that commercial data be used for screening programs only when it's necessary to satisfy a defined purpose, the minimization principle is used, data quality issues are analyzed and satisfactorily resolved, that access to the data is tightly controlled, and potential harm to the individual from a false positive misidentification is substantial, use for secondary process is tightly controlled, transfer to third-parties is carefully managed, robust security measures are imposed, the data be retained for the minimum necessary period of time,

the transparency and oversight are provided, and the restrictions of the Privacy Act regardless of whether an exception may apply and a simple and effective redress is provided and less invasive alternatives are exhausted.

The recommendations in this new document build on those prior recommendations. They do not replace them.

At this point both of these documents are intended to be living documents. We have just recently gotten some comments during the past couple of weeks on a prior document and we plan on taking a look at those and reacting to them and we also want to make clear that we are looking forward to getting comments from the public.

We are also looking forward to getting comments from employees at DHS, if there are any and it would be particularly helpful to us if we haven't gotten those in and some of the comments that we have gotten on the prior document have come from DHS employees and I thank the people for time the time to look at them and to provide those comments.

That being said, I would like to describe a little bit what we are trying to do in this document. We are trying to describe some controls that could be put in place by the DHS Privacy Office to further protect to make sure that commercial data when it is used by the agency or agency component would be done in a way that would respect the privacy of people whose data about them is included in that commercial data.

The first issue we had to confront was how to define commercial data. That ended up being a difficult problem to solve. We decided to try to define commercial data broadly, but then to make sure that the recommendations for the oversight mechanisms that we were recommending in this document were of a sort that are scoped to be things that are already generally in place at the DHS and are things that we think are practical to being able to put in place for this greater scope of commercial data.

The commercial data definition ended up being and the way we defined it was to personally identify the information accessed or obtained by a government agency from a non-governmental entity including commercial and nonprofit enterprises.

Then we specifically wanted to call out that there are certain categories that are not exempted from that definition, particularly what we refer to in the document as publicly available data and also public record data when it is used outside the scope of the use that it was initially intended for.

The reason why we wanted to specifically call out that those are not exempted is we think that it is very difficult to determine especially in a situation where government agencies are encouraged to transfer data amongst themselves and in the situation that we live in where information can be obtained off the Internet and it is very difficult to understand what the source of that data was.

We felt we needed to draw that broadly to actually put effective mechanisms in place.

After the definition the second concept that we tackled was the idea of whether the control mechanisms that we were going to recommend should apply to all data that fit that definition or a subset have data.

There is preexisting guidance from the DHS Privacy Office which is included in Appendix I of the Privacy Impact Assessment Guidance document that states that an assessment should only be done on systems of records that include commercial data when those are systematic uses of the data.

We looked at that and analyzed that and came to the conclusion that we don't think that that necessarily makes sense from the perspective that the individual who that information applies to could potentially be significantly impacted by use of that data even if it was not a systematic use.

Instead part of our recommendation is going to be that the control mechanism should apply whether or it is a systematic use or it's an ad hoc use that could have a substantial risk of harm to the individual.

That being said, then that led us to the recommendations that are included in the document. As I said before we focused our recommendations upon processes and policies that we believe are already in place at the DHS and in the DHS Privacy Office to make this something that could be implemented, but first, we believe that it should publish a system of record notices for new or revised systems of records that use commercial data within the scope of what would occur in the document.

We also recommend applying via impact assessments to programs where the privacy threshold analysis shows the commercial data is implicated in the program.

The third recommendation is to revise the privacy impact assessment template and guidance documents to include a commercial data module and may give an outline of different things that we think should be in that commercial data module in the paper.

Our fourth recommendation is that the DHS Privacy Office should analyze template contract language and propose modifications for the language that should go into the contracts with commercial data vendors.

We think that our initial look at the currently existing template language for those contracts does not in our opinion appear to be sufficient to cover everything it would need to cover.

We have not done a detailed enough analysis to make a firm conclusion on that so we are recommending that the Privacy Office do that analysis.

We are also recommending that the Privacy Office should be reviewing those relationships with commercial data vendors and reviewing the contracts that are going to be put in place with them.

We also recommended, and this is our fifth recommendation, to make certain in the DHS Privacy Office that PIAs will be filled out for programs that are implicated and the privacy risks that are noted in the PIAs are going to be mitigated.

To do that, we need to make another recommendation, as Mr. Pietra noted earlier today, which is that, if everyone is anticipating a large value of privacy impact assessments over the next couple of years the subcommittee had concerns about resources and whether the Privacy Office has enough resources to be able to effectively review those documents and not just review them because just filling out documents does not necessarily help to improve the world of privacy, but taking a review of that and then driving necessary changes back into the agency components of the programs where changes need to be made.

That is the scope of the recommendations in the document and at this time we propose that the report be adopted.

CHAIRMAN BEALES: Thank you, David. Let me thank you and the members of your subcommittee as well for your tremendous effort to work every bit as hard, if not quite as loudly as the committee working on the RFID report. We appreciate that effort as well.

Are there questions or comments? Joe Alhadeff.

COMMITTEE MEMEBER ALHADEFF: Yes, actually having early on been part of that committee and working on it I realized and I want to make sure that we are not giving the misimpression of the concept that I just realized of the annotated outline which was something that we had started with because we had a much more abbreviated document.

I think this is no longer an annotated outline. This may actually be the documents so we way want to remove that little piece of it.

The other question is not related to the document, but is related to something that's observed in the document, so I don't know if you want to approve the document first and then I ask that question or if you want me to do it now.

CHAIRMAN BEALES: You might as well do it now.

COMMITTEE MEMEBER ALHADEFF: That was: What we have seen throughout the number of the testimonies that have happened today and previously and in working on this paper and what has been alluded to in the paper when you look at the commercial

data is that one of the concerns with commercial data is that it doesn't necessarily stay in the same organization required to and there are transfer implications for that.

That is not unusual and it is likely to happen and in many cases it may be necessary to have them because one of the failings in some of the issues related to terrorism has been the inability to appropriately share information in some cases because systems do not talk to each other.

One thing we looked at which has been highlighted in the paper, but which has not really been addressed as much, unless I am missing it, is the concept of how do you do a PIA across systems?

Because, realistically, you need to now assess the environment. I know we just spoke about 500 PIAs and I know that the Privacy Office has been thinking about this issue. This is not new to them, but it may be one thing the committee could help the concept on, "How do you apply a PIA concept across systems as opposed to within a system?"

CHAIRMAN BEALES: Thank you, Joe. Are there any other questions or comments?

If not, then I would entertain a motion to adopt the report. It is so moved. Is there a second? Seconded. All those in favor please say aye.

Any opposed?

The report is adopted.

I believe that brings us to the end of our agenda. It is now time for public comments and we do have a public commenter. Probably tell me who that is.

MS. RICHARDS: If you would please identify yourself.

CHAIRMAN BEALES: Give us your name and any relevant affiliation for the record we would appreciate that. We look forward to your comments. Under our rules you have three minutes.

MR. OLEINICK: I am Lou Oleinick Defense Logistics Agency, chief of the privacy FOIA Office.

One question I had for this committee and for DHS is whether there is consideration from, when I was listening to the FOIA brief, it is just an idea that crossed my mind that we as an agency are experiencing the same problem I am sure you are experiencing with the new electronic systems for processing whatever it was.

The commercial products we have seen have been very unsatisfactory. The E-Government initiative suggests that when there is a cross-governmental problem requiring a solution that there may be opportunities for partnering.

This, to me, sounds like it may be one of those types of opportunities where there could be a cross-governmental partnering opportunity.

It's an idea I wanted broach for consideration. This may not be the appropriate venue, but I did want to bring it up as an idea. That's really the only comment I have. Thank you.

CHAIRMAN BEALES: Thank you very much. This is appropriate forum for almost any idea and we thank you for your comment.

MR. TEUFEL: Shall I comment?

CHAIRMAN BEALES: If you would like.

MR. TEUFEL: Do I get three minutes?!

CHAIRMAN BEALES: Hugo, for you, four minutes!

MR. TEUFEL: It is certainly something we could explore. When I headed general law in DHS and Interior one of the things I did was to put together the general law working group which was general law managing lawyers at most if not all of the cabinet level agencies to work on cross-cutting issues, so it wouldn't be the first time for me to work with other agencies in ways we can partner to fix issues that we all jointly have to address.

It is something we could look at and if there is anything I can do to get that 41 percent of the federal government's FOIA backlog down, I am happy to do that.

CHAIRMAN BEALES: As long as it is not increasing the backlog at other agencies.

MR. TEUFEL: I hadn't thought about that one.

CHAIRMAN BEALES: Are there any other closing questions or comments from the committee?

In that case, the committee stands adjourned from the public meeting and we will move to our subcommittee meetings downstairs after a brief break. Thank you all for coming. We are adjourned.