DEPARTMENT OF HOMELAND SECURITY

DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE

FULL COMMITTEE MEETING

WEDNESDAY, JUNE 11, 2008

Hilton Arlington
Galleries I and II
950 N. Stafford Street
Arlington, Virginia 22203

AFTERNOON SESSION

CHAIRMAN BEALES: If we could reconvene for our afternoon session. We've had some unavoidable delays in the arrival of our last panel, so I think what we'll do, is at this point, is go to our subcommittee reports, and get that out of the way. And then when our panel is here and ready to go, we will -- we will turn to that panel. So, if we could turn first to the Data Integrity and Information Protection Subcommittee, Ramon Barquin.

MR. BARQUIN: Thank you, Howard.

First, let me note that the -- this Subcommittee, the DIIP, we should refer to it as the DIIP Subcommittee. Not dip, no, DIIP Subcommittee.

In any case, we have agreed on two specific areas that we are going to focus our Subcommittee's work on, and let me just read both the title, as well as the -- the substance of what we're going to work on.

First, is to provide advice and guidance to the DHS Privacy Office on the underlying technology aspects of the DHS Privacy Impact Assessment, the PIA template. The Privacy Office uses a template to conduct Privacy Impact Assessments of DHS IT systems. This assessment is oriented toward capturing the privacy implications of a program's policy and technology for a specific IT system.

As programs complete the PIA, it is important to ensure that the answers contained references to the specific technical mechanism used to enforce the descriptions of the program's operation. This Subcommittee's guidance will focus on how best to build this more granular and technical layer into PIA process and the PIA template and guidance.

The second deals with something that came up already this morning, in a slightly different context, and that's privacy implications or privacy issues in implementing SOA. So it's to provide advice and guidance to the DHS Privacy Office on privacy issues in architecting and implementing Service-Oriented Architecture across DHS.

Service-Oriented Architecture, or SOA, is a modular architecture that enabled a variety of services to be offered through the assembling of different software building blocks. The dynamic nature of a SOA poses challenges to the application of traditional privacy assessment tools, such as the PIA. The DIIP Subcommittee will focus on understanding the department's current and anticipated use of SOA, and advise the DHS Privacy Office regarding how best to address the associated privacy issues.

So by and large, we're going to be working on helping to make the PIA template more technology-focused, and also on addressing some of these privacy issues tied to Service-Oriented Architectures across the Department.

CHAIRMAN BEALES: Thank you, Ramon.

The Privacy Architecture Subcommittee, Joan, Jim? Joan?

MS. MCNABB: Yes.

Okay, the Architecture Subcommittee has been cogitating for some time on making recommendations to change the -- to add to the process for -- for States applying to DHS for grants, to add to that process some questions that will require addressing privacy issues in the projects that they're proposing for support. And we plan to bring a paper, containing the recommendations, to the Committee, at the September meeting.

CHAIRMAN BEALES: Great, we'll look forward to that.

And the Data Acquisition and Use Subcommittee?

MR. PURCELL: Thank you, Howard. The company -- Subcommittee we affectionately call the DAUS, has been tasked by the Chief Privacy Officer, Hugo Teufel, to provide advise regarding the use of memorandums of understanding supporting computer matching agreements between -- inside the agency and between agencies. This stems from an DHS IG report on FEMA's response to Katrina, and computer matching agreements and demands for information during that recovery operation.

Our plan is to document the legal and the technical aspects of computer matching agreements, to examine the implementation examples that we have available from the Social Security Administration, the Department of Justice, and others, and create a template for that memoranda, as well as the computer matching agreements themselves. We're being very cautious to make sure that we incorporate both law enforcement data, more sensitive and classified data, as well as non-law enforcement data in explaining, in this template, exactly what kinds of precautions and protections to be aware of whenever setting up one of these matching agreements.

The hope, in the end, is that the agencies will create computer matching agreements prior to the need to execute them, so that during a crisis, they don't begin swapping data in an uninformed or potentially vulnerable way.

CHAIRMAN BEALES: All right. Thank you very much.

Do we have our panel? Great.

MR. HUNT: Yes, and they're going to be joined by one more member in progress.

CHAIRMAN BEALES: Okay.

MR. HUNT: We're going to cue up, they have a presentation.

CHAIRMAN BEALES: Okay, great.

Our first session this afternoon is to look further at the E-Verify program that we started hearing about at the meeting in El Paso. It is a very interesting and rapidly growing program that raises some challenges, and we look forward to hearing more about it today.

Are we -- are we separate presentations or are we one presentation? One presentation. Okay, well then let me mention all of who is here.

We have with us today, Rebecca Green, who is the -- with E-Verify Operations in DHS. We also have Sonja Barnes, who is with E-Verify's Customer Relations and Learning Management. We have Robert Gaines, who's the -- with E-Verify Strategic Planning, in the Verification Division, and is the Chief Strategy -- the Chief of Strategy for the Verification Division. He was previously the Chief of the Special Projects Branch, within Verification.

And we, finally, we have Claire Stapleton, with National Security and Records Verification in the Department. She is the former Privacy Officer for the U.S. VISIT Program, received a Bachelor's degree in Psychology from George Mason, and a Master's Certificate in Program Management from George Washington University, and she's a certified information privacy professional.

So, welcome all four of you, and we look forward to hearing more about E-Verify.

MS. GREEN: Alrighty, we'll get ready to start. If we can go to the next slide, please.

So, this is our agenda, kind of an introduction, E-Verify 101, and followed by education and outreach, and some technical and infrastructure and program criticisms, and then some privacy considerations. Next slide.

Okay, for the E-Verify 101 piece, the program -- we want to go over some of the program goals and the user statistics, how E-Verify works. We want to address the photo screening tool, and also let you know about some of our recent improvements and enhancements.

E-Verify is formerly known as the Basic Pilot Program, which was mandated under the Illegal Immigration Reform and Immigrant Responsibility Act of 1996. It's a partnership between the Department of Homeland Security and the Social Security Administration. And it is -- it provides a means for participating employers to verify the employment eligibility of their newly hired employees. Okay.

Some of the E-Verify Program goals are to reduce unauthorized employment, to minimize verification-related discrimination. It should also be quick and non-burdensome to employers, and we keep in mind that we try to protect the civil rights and civil liberties, and employee privacy, as well.

As of early this week, we have -- we currently have over 69,000 participating employers, and that's growing by leaps and bounds, about a 1,000 or more per week. As of last Fiscal Year, we did 3 million queries, and you can see that we've grown. This year we've already surpassed that, and now are at 4 million queries.

According to some of the evaluations that we’ve had on E-Verify, 94 percent of our verification queries are automatically verified as employment authorized. And we’ve just -- we're just listing the top industries that us our program, and you can see that you have a wide variety of different industries, from white-collared industries to traditionally blue-collared industries. Okay.

So how does it work? The first thing that an employer has to do after they've registered, is submit the information from the form I-9. That actually forms the basis of the E-Verify query. Once the form I-9 is completed and the data is input, the system then queries SSA, and if it's a non-citizen, then it will query the DHS databases.

One thing to keep in mind, is E-Verify is not used to generate an unable to work list, and it can only be used for new hires and it should not be used for existing employees. And any procedure that you use with E- Verify, has to be applied across the board to all of your newly hired employees, regardless of their citizenship.

So the initial verification -- so, once you've submitted the query, you'll get one of three results in about 3 to 5 seconds. The majority of them come back as employment authorized. Then you get some that fall out as the "SSA tentative non-confirmation." And that basically indicates that the information provided on the form I-9 doesn't match the information in the Social Security's Numident database. It doesn't mean that they're not authorized to work, it's just that there is a mismatch somewhere.

Or, if it's a non-citizen and they've cleared SSA, but they were unable to match it in -- automatically in the DHS records, then it goes to a DHS verification process. And this basically -- what happens with this, is that we have an immigration status verifier that will look at the case, and go through our data sources, and then respond within 24 hours, either with an employment authorized or a tentative non-confirmation.

Okay, we haven't -- we introduced last October, something called the photo screening tool. And, this tool allows employers to match the photo on the document that was provided by the employee, if it's an employment authorization or permanent resident card, to the photograph on file for that card. And it should be a 100 percent match. They can't come back and say, "Oh well, I dyed my hair or I'm wearing a different shirt." The database that we pull this from is actually the database that produces that card. So, it should be a 100 percent match.

This tool was designed to -- to help employers to detect instances of document fraud. There are some really good fraudulent documents out there that employers -- there's no way that they can detect it. You actually have to probably be a forensics or a document expert to detect them. And I mentioned, photo tool was actually incorporated into E-Verify in September of last year.

So, once you go through the whole process and you get a tentative non-confirmation, what do you do, how do you -- what is the employee supposed to do? One thing to keep in mind, is this the system's piece where the employee can actually redress their tentative non-confirmation.

So, all the employees have the right to either contest or not contest whatever the finding is from DHS or the Social Security Administration. If the employee chooses not to contest, then they can be terminated immediately. But if they do contest, then they're given eight Federal government workdays, from the date of referral, to either visit the Social Security Administration, or to call DHS to resolve the discrepancy.

An important thing to keep in mind is that any time during the verification process, the employee should continue to work. There should be no adverse impacts where they have their work hours reduced or they're told, Well, you can't come back until it's addressed, or training is not allowed. So, you know, they should continue business as usual at that point.

But once the employee takes care of their tentative non-confirmation, a response is sent back to the employer through the system. So, they would check that daily to see whether or not an employment authorization was sent back or not.

So these are the, kind of, the final resolutions following either a tentative non-confirmation or from an initial verification. So you can receive an “employment authorized,” which is sort of self explanatory, that they’re authorized to work.

A final non-confirmation occurs when an employee has actually contacted the appropriate agency, but the agency is still unable to verify their information. And then there's also a response, is a DHS or SSA no-show. And this is when the employee does not contact either government agency to resolve the case, and then this is -- this response is issued and is considered a final non- confirmation. And just like the final non-confirmation, they can be terminated.

There's been some questions about due process and redress. The E-Verify system actually has that built in with the tentative non-confirmation, but there's been some concerns about the final non-confirmation. And just to let you all know, we are -- we have been working on a process called “Request for Reconsideration,” that would allow employees to correct their records once the final non- confirmation has been issued. And we're trying to make sure that all of the legal, the privacy, and security concerns are covered before we actually release this into a formal process, into the program.

But some interesting stats on the tentative non- confirmation redress process, is that 5 percent of all queries are successfully contested by employees and found to be work authorized. And it's only .5 percent. Those that choose to contest and don't go in, or they can't resolve, those are the ones that actually, you know -- those are the ones that, you know, it's a good catch for us.

Also something important to keep in mind, is that we can't offer any judicial review, because of the authorizing statute. So, that would have to be something that would be changed in the future. Okay.

Recent improvements -- we've actually added some really interesting things to kind of help address the problems of some of the -- what people call error rates, but which is truly a mismatch. A lot of people that are naturalized citizens have not updated their records with the Social Security Administration. However, since USCIS is the holder of record on naturalized citizens, we’ve instituted what we call our NATS Project.

And what that does is, if SSA is getting ready to initiate a tentative non-confirmation on the employee, then that query is sent to DHS, to verify whether or not we have information on the naturalized status of that person. If we do, then we send back the employment authorized. If not, it falls into the SSA TNC.

We also have a second part to that. For those folks that appear to be naturalized citizens, they are given in their referral letter, the option to contact DHS instead of going to the Social Security Administration, and they can resolve their case with us, instead of with SSA. Okay.

The other thing that we have is information from the real -- it's real-time arrival data. And that was just recently included in May of this year. And basically that's taking data that the inspectors enter at port of entries, to verify newly arrived folks to find out whether or not they're employment authorized. Because normally, their I-94 documentation is sent to a contractor to be entered into, I believe it's the IBIS system, and it takes about 2 weeks, so this allows for them to clear a lot sooner, by using this data.

The other thing we introduced was our pre-TNC page. This allows employers to have one more opportunity to review the data before the tentative non-confirmation is issued. So, what actually happens is the query is sent through the system, and say it hits up against Social Security first. If they're not able to do a match at Social Security, it brings up the pre-TNC page to the employer, they can go in and they can change it, and then it’s resubmitted back to SSA for them to verify. And that's actually done really well -- we've had about 30 percent of our TNCs have been reduced over the last 2 months, so that's really good -- eliminating those errors done by data input from the employers. Okay.

And I just wanted to talk about future improvements. There's been a lot of concern about the type of language that we use in E-Verify -- things like tentative non-confirmation, final non-confirmation or even referring to designated agents. A lot of the people don’t understand that, especially the employees, and recently we had a workshop that was addressing 12 of the terms or phrases that over the years that we have heard complaints on, to try to figure out what words or phrase can replace that. And I have to say, it was a really, really good workshop, and we'll probably have some more in the future, but we're going to first address those 12 terms, and then begin to filter through the rest of the E- Verify language to see what else can be simplified.

Additionally, which also goes in with it, is we're improving our referral and TNC notices, so it's going to be in plain language, but the other thing that they’re going to do is it's going to provide instructions to the employee during the tentative non-confirmation phase when they contest, and when they have the referral. And it’s going to be very detailed information that they'll find beneficial.

The other thing that we're working on is the concept of a final non-confirmation letter. Employers have indicated that, you know, when they get a final non- confirmation, they tell the employee, they really have nothing to give them. And so this final non-confirmation letter is going to address that, it's going to be given to the employee, and basically it's going to say, "You've got a final non-confirmation, here's the reason why, and this is what you can do."

And then we're also looking at querying by passport number, and that actually should be coming out fairly soon. And the people that that's going to help, primarily, are going to be people who have derived their citizenship, because DHS records currently do not capture derivative citizens, unless they've applied to have a certificate of citizenship. So, we hope that is going to help those particular categories of folks. Okay.

Now, I'll turn this over to Sonja.

MS. BARNES: Thank you.

I'm going to talk a little bit about some of the things that we've done over the last year to reach our customers, to educate employers and employees about the program, and how we're meeting their needs in this respect. I'll talk a little bit about the education strategy, our customer service information lines, employee rights and responsibilities I'll touch on. Also, State legislation just a little bit, because things are different in different parts of the United States and also provide the contact information associated with folks getting in contact with the program.

In the last year, we've conducted more than 200 presentations on E-Verify. We've traveled across the United States, we've met with employers organizations, and employer groups, and employee groups. We've conducted webinars each week, on a continual basis, in support of the program, as a means to educate these organizations, employers, State legislators, on what E-Verify is all about.

Our strategy has also included the strategic placement of online print and radio. When Arizona legislation was signed, we immediately started working on a plan to get billboards, print ads, radios into the Arizona area. We've done the same for the D.C.-metro area, you may have seen some of those ads, and I also have copies here, for the committee.

We've also just begun a campaign in Mississippi. Mississippi has legislation that begins July 1st, requiring that both public and private employers in that State utilize E-Verify, and so we want to educate folks in the State of Mississippi. We're also there conducting presentations, as well, about E-Verify to educate folks in that area.

And our intention is to go back to Georgia, we just recently completed a series of informational seminars in the State of Georgia, again, as a means of educating folks in that State on what E-Verify is all about. There is legislation there in Georgia -- it's not mandated for the entire State, but there are public employers who are asked to, or encouraged to use the E-Verify system.

We've also made some changes in the last year to our website. There was a huge volume of information on the website previously, we've made that easier to read, more user-friendly, we provide updates to the website on a -- very frequently, and we just -- we sent everyone to that website, as many folks as we can, again to educate people, and to ensure that we are as transparent as possible, in terms of our services, for both folks who are using this system, and those who are thinking about it, or just want to know more about what E-Verify is all about.

And we're also doing what we can to foster those relationships and to be there, and available, to the folks who are using E-Verify and have problems with E-Verify, or have questions or they're -- we're receiving feedback from organizations about things that we can do better, and we're providing that information, and using it internally with our policy group to, again, to round out the things that we're doing in terms of improvements and policies with E- Verify.

Customer service, we've expanded customer services, also in the last year. It's now a tiered service. For years, there were just a few folks who were answering telephones and providing that kind of assistance, we now have a dedicated workforce who are responsible for answering those telephone lines.

The tiered service -- we are working with our agency's national customer service center, and when those answers can not be made from the scripting that is provided our Tier 2 services, they are provided to the E-Verify staff to handle.

Services are available from 8:00 a.m. to 8:00 p.m., Eastern Standard Time, Monday through Friday.

We have some future customer focus initiatives that we're very happy about, we've been working on these things for some months, and they are continually in our -- in a queue of things to accomplish. We're developing the registration flash demonstration, we've heard from groups in terms of, "We don't know enough about what E-Verify is all about, we want to know, or have an idea, of how much time it's going to take for us to go through the queries," and, "What is the registration process all about?" And so, we're making it -- developing an interactive flash demonstration that would be placed online, as well, and provided to -- available to those who would like to know more about the program.

We're also nearing the production phase of a video -- the video is focused on -- we're placing an emphasis on the employers activities as it relates to query process and their responsibilities and making them aware of employee rights, and ensuring that they are complying with the process as it is intended, and we're partnered with the Office of Civil Rights and Civil Liberties to produce this video.

Were also translating notices into other languages. We currently, online, have the employee rights document online in 9 different languages going forward, the referral notices and the tentative non-confirmation notices, as well, will be translated and available to those employees who speak languages other than English and Spanish, which is available now.

Our goal is to strengthen our contact with small businesses, and so we have begun discussions with the Small Business Administration to discuss with them how best we can work with them to actually reach out to the small businesses, and get to know that segment of employers more.

The critical infrastructure, that's a huge undertaking, and we've begun the research necessary to identify how best we can reach that group, and also educational institutions -- there has been recent legislation that impact the educational institutions, universities and colleges who have F-1 students, and so we are focused on them, as well, to provide them the information that they need in order to meet and deal with the students there.

Employee rights, and employer responsibilities -- all of our advertising is focused both employee and employer segments of the population. Print, radio, and billboard ads, that's a constant in all of our marketing. Employee rights document is available online, as I indicated before, in 9 different languages, and we also have a quick fax brochure for both employees and employers, and I also have copies of those here for the committee, as well.

Continually we're partnering with and communicating with the Office of Special Counsel for Unfair Related Employment Practices, issues that are presented to them, we are made aware of and those concerns are issues that we certainly want to know about. And also with the Office of Civil Rights and Civil Liberties, as well. Virtually every aspect of our planning, those are considerations and we meet with the persons from those offices frequently.

There is an emphasis -- when we're all talking to employers, and educating those employers and employees, the emphasis is always on the rights that the employee has, associated with the use of E-Verify, of the system. There's emphasis placed on, You must provide those employees with the opportunity to contest, or not contest, the findings of the query that's generated.

Also, we're -- we emphasize the expectation that the employers do post the Office of Special Counsel poster, advising employees of their rights, and we also provide that telephone number and contact information to them, as well.

And these are just examples of those posters -- these are the posters that each employer who uses E-Verify is expected to post in a visible place for employees, so they are aware of what their rights are.

State legislation -- as I indicated before, I'm not going to go through all of the States that are involved, or discussing, or talking about E-Verify, but just to highlight that Arizona has legislation that mandates the use of E-Verify throughout. Also, the State of Mississippi, beginning July 1st, will begin a phased-in approach to making sure that employers throughout the State are using E-Verify.

Just recently, legislation has been signed by the State of South Carolina, also requiring that public and private employers use the E-Verify system.

I just -- this slide, we just wanted to reiterate what you may already know, is that the Federal government is a user of the E-Verify system, and are using E-Verify today. And just recently there was an Executive Order that was signed that requires Federal contractors use E-Verify, as well.

And here's our contact information -- anyone who wants to know more about E-Verify, has a question, is already using the system, can call our 888 number -- 464- 4218, or go to our website which is there also, www.dhs.gov/e-verify, for additional information. And at any time, as we're talking to folks, we do encourage people to contact us with their suggestions and recommendations for what we can do to strengthen this program.

MR. GAINES: Great, thanks, Sonja.

Let's see, I'd like to talk about a few things here that I think will be of interest to the committee. One is to talk about the technical infrastructure of VIS, and the data model behind it, and some of how that supports our privacy and security that's necessary to support the system.

Also, looking down the list, we'll be talking about some of the monitoring and compliance, what we're doing in that to get those ready for the program, addressing some common criticisms of E-Verify, and hear you out in terms of what those may be, but addressing some of the common misconceptions that we've heard, and also speak about the data accuracy issues, specifically. Slide, please?

So, the VIS overview -- essentially this is a quick slide to talk about VIS. So, the Verification Information System is the technical infrastructure that supports E-Verify. So, the other thing to know about VIS that's important is it supports both SAVE and E-Verify. Now, we're not going to talk about SAVE very much here, but it's good to know that that's the sort of sister program to E-Verify, that allows government agencies -- benefit-issuing government agencies, State, local, or Federal, to be able to do the same kind of checks with E-Verify to see if someone had the proper immigration status. But it is -- it does a different story than E-Verify, it will share more information than E-Verify does, but that's the complimentary program for that.

VIS itself has a database, it basically has selective immigration status within it. There's over 100 million records currently in there, and right now we only maintain the data elements that are necessary to complete those searches for immigration status, for either SAVE or E-Verify.

On the next slide here, I'll talk about how it goes about, or what systems it checks. So, essentially, to derive this information, it has to check a number of system, both within DHS, as well as SSA, as Rebecca was talking about. Next slide, please?

So, let's talk for a moment, just about how data is organized in VIS. Essentially, our three main program goals, as far as the technical infrastructure are concerned is, we obviously have to fulfill our primary mission, to know that an individual is authorized to either gain government benefits or employment, and of course, use the minimum necessary information to do so, hence, relying on form I-9.

We also want to make sure that we can have sufficient safeguards in place that we're able to provide, or identify, you know, misuses or abuse of the system.

And then finally, safeguarding the privacy of the people who are being run through the system. So, the people themselves, the employees, when they're run through it, they know that they're being -- their data is being treated carefully.

So, one thing I wanted to touch upon which Rebecca had already mentioned, was the VIS data model itself is essentially transactional, which is to say, every time an E-Verify query is run, that is a new transaction in our system. We associate that with an employer, we do not associate those with an employee.

So, currently, in our data model, there is no way to run through and say, “John Smith got run through E- Verify 9 times.” There's no relation between those two data elements. So, essentially, you would have to mine through all of the data trying to find that information.

So the data model itself doesn't particularly support a no-work list, or a longitudinal employment history, and that's a common concern from our privacy folks, to say that, you know, Well, could you pull up, say, someone's entire work history, it's actually not designed around that -- it's designed around finding employer misuse. Next slide?

Here we go -- I apologize, this is a bit of an eye chart, but essentially, these are external system interfaces for our system, I'll run down through them, because I know it's a little hard to read. At the top you have the Social Security Administration's Numident database, which is, essentially, as Rebecca was talking about, how we verify U.S. citizens that are run through E- Verify.

The ones that follow are the various DHS systems that we have -- the CIS which is the -- potentially our mainframe system that holds most information on work eligibility for immigrants, CLAIM3 and RNACS, which again, have information on immigrants, and non-immigrants, and also starting to confirm citizenship for naturalized citizens. As Rebecca noted, that's one of the concerns with SSA is, they don't always know when a citizen has naturalized. So, we're pulling in -- you'll see me talk about in just a minute -- some of the data changes that we've put in to address that particular concern, so that people don't get mismatches for social security if we have a record that they have been naturalized.

From some of the CBP systems, you'll see IBIS, which Rebecca talked about as well, and is some of the incorporation of the real-time data. Obviously, to make sure that we have good matches in the system, timeliness in the system is an issue as well as data quality. So, if we had to wait 2 weeks, as we had been for some of this data to come in, someone could apply for a job in the meantime. With real-time information, we can actually get that much quicker, close the loop, and then actually be able to know that someone is work authorized more quickly.

From the ICE system, we have SEVIS, which is the Student and Exchange Visitor Information. This is actually more used on the SAVE side than it is for E-Verify. We actually don't use it as an automated check in E-Verify, but if a case has a mismatch, we'll sometimes use it for a secondary verification process, this goes to the manual process.

And finally, at the bottom, you'll see the person-centric query service, and of course, CLAIM4. The PCQS, is again, it's another tool that's used by our status verifiers on the back end, that gives them read-only visibility into the systems when they look to see a case that's been mismatched, so they can actually see more readily. So, this was an attempt to streamline our manual back-end processes, that we can clear those cases more effectively, and CLAIM4 is related, as well. Next slide, please.

So, talk for a moment about VIS capacity. Essentially that first paragraph is saying is that last summer we ran a stress test on E-Verify to make sure that the technical infrastructure was capable of holding up to a mandatory environment. To say that, you know, if we threw more servers at it, that's fine, but is the architecture itself, would that support that?

The test conclusively showed that, yes, the architecture would. The system scales, from a technical perspective, to be able to handle all of the queries, and I'll talk about my qualifying that, just slightly. But, the test, from a technical perspective is the infrastructure is sound, pending some -- the addition of servers, which we're actually in the process of doing right now, we're actually adding additional servers to the system, to get ready for mandatory. Obviously this is a good deal off, but as we're starting to see States come on board one at a time asking to be, you know, passing laws to make them mandatory, we're seeing the need to do this. So, this is more of a precautionary measure, at this point.

But, I think it's also important to note that, when we consider scalability, when I say the technical infrastructure is only one element to consider. We're actually taking a more holistic approach to it, as well. Some of the things that Rebecca was talking about in terms of a plain language or usability -- these are every bit as important as far as the technical infrastructure. The technical infrastructure will tell you, will the systems handle the load? However, if the system isn't clear to people, if it's not usable, if it's generating a lot of manual mismatches, then obviously that's going to put a lot of stress on our manual processes.

So, we're spending a lot of time looking at scalability more holistically, not just from a technical perspective which, I think, we've got under control, but also from more of the usability questions, as well. Which that ended with the human factor study that we did last year, as well. Next slide?

VIS security, again, I think there's -- this is more of a table steaks kind of slide here, this is the things that we absolutely have to do, obviously, that we follow the FISMA laws, and the DHS and OIT requirements. We actually just finished a CNA a few months ago, so that's being taken care of, that's all passed fine.

And, of course, the second paragraph there, talking about, again, what I would consider the table steaks, the fact that, you know, these are -- we have the administrative, physical and technical safeguards, we're not just looking at technology.

And also make sure it's on a need to know basis, and that the people within our system, like within DHS, are not looking at data that they don't need to do for their jobs.

However, the point here for security is also, again, much like, from the scalability -- it's best to look at it holistically. If you're just looking from a technical perspective, it's usually not enough. So, we're actually working a number of initiatives to broaden those.

I'll list off a few, for instance, I know that we -- the CNA audits, of course, are conducted every few years. What we're doing is we're trying to institute a, essentially, 2 percent monthly rolling CNA audit check. That way we'll know, you know, if you do 2 percent every month, then by the time the next CNA audit comes around, we'll have gone through a significant number of those checks already. That doesn't get us off the hook for doing a CNA audit, that is still absolutely required, but it gives us a sense that, once it comes around, that we avoid the Big Bang approach -- that's like you, you've had this problem for 2 years and never knew it. So, we're trying to be a little bit more aggressive in terms of that.

We've added more strict logging -- automated logging hardware, on the back end, for VIS, to know that if there are problems or breaches of security on the back end in the server realm that our administrators find out immediately. This was not a requirement for the CNA audit, this was considered above and beyond, but we've added it to make sure that we're taking the appropriate steps, to know that we're aware of these problems, as soon as they happen.

Similarly, and again from a more soft side, we've also joined the DHS anti-phishing working group, so from a phishing perspective, to know that if an employer -- if someone gets on the internet and purports to be E- Verifying, so it's sending out employers' email claiming to be E-Verify, how do they know that we're genuine, and how do they know that that's a fake?

There is, obviously, a lot of social engineering techniques in there, too, but again, security we need to look at that, just as much as the IT. Next slide.

So, we'll talk about data integrity initiatives, as well. I know we'll talk about some more of the breakdown which Rebecca has already talked about a little bit, as well. But, we do have ongoing initiatives to improve the data match accuracy. You'll notice I did not say increase the data match full-stop. Accuracy, of course, is the correct number there. Because, you want to make sure that you're doing valid matches. If we're -- if the system is correctly kicking out invalid matches -- that's a good thing.

I'll talk for a minute, in a moment, as to why getting to 100 percent match rate is actually not a good thing for our program.

So, this really has two elements to this that are important. One is, to do the data match accuracy, to push up that automated 94 percent that Rebecca was talking about earlier, but also to say, if someone does have to have a manual case looked at, what can we do on the back end to streamline that process? To make sure that our status verifiers can clear those cases as expeditiously as possible?

This is, of course, one of the key things we have to do to get ready in a mandatory world. Any time we have a manual process, we have to know that our manual processes are, a) being touched as little as necessary, and then, 2) is that when they do -- when they are necessary for a person to adjudicate their case, that we're doing so as quickly as possible and as accurately as possible. So, of course, this is speaking directly to document fraud, as well, which is one of the goals of our monitoring and compliance, as well. Which, I believe Rebecca talked about with some of the photo tool changes, for instance, that's one of the things that we're looking into. Next slide?

On the subject of document fraud, one of the criticisms, I suppose, of the photo tool, is that currently the photo tool only works for two types of photos -- green cards and EAD cards, which are both DHS-issued cards. Currently, we're looking to add additional data sources to broaden the usefulness of those tools.

The first point there, incorporating passport data, so we're working with Department of State on this, as Rebecca was talking about, was to reduce the rate of TNC.

So, to identify derivative citizens, so that when we do the match, that we can actually let someone be employment authorized, without having to go through SSA and resolve that.

The other two -- passport photos and visa -- really, it's visa photos, is primarily the interest there – is to bolster the photo tool, to be able to add additional types of photos there. So, if someone presents on the I-9 a photo identity document, that they're able to be run through the photo tool, just as we do currently with green cards and EAD cards.

As Rebecca was saying, the photo tool is there to catch that kind of photo substitution fraud. Again, it's establishing that this is a solid document that was issued by the issuing agency. It does not address all of the identity theft concerns that the program is sometimes accused of, but the truth is that, this is the -- within the limit of our mandate -- this is as far as we can go to combat that kind of identity fraud, and it's a step in the right direction. Next slide?

Registration reengineering is a project that we're -- I've got ongoing right now, actually, is something that we're aggressively looking at in terms of identifying, essentially, some of the gaps in our registration process – what information are we capturing, what information should we be capturing, and what are the risks that that associates to the program?

For instance, if someone comes on board, and you know, purports to be another employer, what would they have access to? Or if they were fraudulently misusing the system, do we actually know that we could get in touch with this person, to combat this kind of problem?

Essentially, the registration process is looking at validating two things. One is the authenticity of the companies that join the program. Is a company who they claim to be when they enroll in our program?

But also, establish stronger identity assurance of the individual. So, that way if a person is a user of our system, that we have a better idea of who this person is, who they say they are?

This is not the same thing as a person who has run through our system, let me make that clear. When someone is actually run through E-Verify as an employee off of the I-9, we get the information off of the I-9, and that's sufficient.

However, when someone has the power to be able to run these kind of queries, I think as good custodians of the data, it's incumbent on us to be able to identify that this is being used properly.

I think one of the challenges we're going to face, of course, is with -- on the employer side, various ways, of course, of validating an employer -- say, the EIN, the Employer Identification Number. We're looking into that, however, we're also identifying that there are some challenges there because currently, we in DHS do not have access to view the EIN data. IRS does, SSA does, but the statute that governs that doesn't recognize this as a valid use.

In the meantime, we're looking at ways of addressing that, making sure that we can add that to the system. But the truth is, if and when E-Verify goes mandatory and we run through that legislation, I believe we would look to try and have that stipulation added to the EIN, say, “Could we check this limited subset of data for this specific purpose?” To know that we can verify that an employer is who they claim to be. Next slide.

I'll talk briefly about the monitoring compliance, this is branches within the verification program that are being stood up and actively working on things right now. But essentially, the purpose here is to evaluate the employer usage of the program. That's not necessarily looking for misuse, although that is part of their mandate, but also to know that sometimes the reasons a person might be having bad queries is because the system is complicated, his ability was unclear. They didn't know that they were supposed to do certain things. So part of their mandate is what we call compliance assistance, which is to say, ass things like a self-assessment tool for E- Verify users. We don't want the first encounter they have with compliance to be a knock on the door from a Compliance Officer, saying, “We're having problems with your data, we want to look at your I-9s.” I think a lot more of what we’re going to have to deal with is frankly more of the educational things, like if people are perhaps not understanding how to use the system, which is historically what we've been seeing.

So, we're looking to more identify patterns of what might be wrong, but also identify ways of helping the employers help themselves, as well.

Monitor and compliance, obviously one of their key goals is to reduce discrimination within the program, to know that this program is not being used for prescreening, to know that they're not -- they're passing on tentative non-confirmations to employees correctly, and not just sitting on them, that the employer is acting in the correct way.

And also to educate employers and employees, frankly, on what the rights are, and what Sonja was talking about as well, in terms of what are the employer responsibilities, and the employee rights. So, that's a portion of it, too. And I think I talked about the employer usage of the program, how it's being supported. Next slide.

I'd also like to take a moment to talk about two of the major, I guess, concerns or criticisms about the program. The first being data accuracy, and then the second one is, essentially, how do we scale to mandatory, and what are the challenges that we face there, and what are we doing to address those challenges? Next slide, please?

Data accuracy -- so essentially these first three bullets gives a breakdown of how the queries run through E- Verify, which Rebecca has already talked about some, but I think bears repeating. When we said that there's a 94.2 percent match rate, so that means that that is instantly -- or within 24 hours -- the vast, vast majority of those being instantly, essentially within 3 to 5 seconds, that the person gets a verification -- employment work authorized, thank you very much. I think that's the last 1 or 2 percent of that 94 percent is within 24 hours. So, again, no action was necessary on the part of the employee, and this was a pretty quick response for the employer.

The 5.3 percent leftover is -- or not entirely leftover -- but the 5.3 percent is either queries that were not work authorized, so they contested, they went to SSA or DHS, and said, "No, this isn't right." And after that they were still found to be not work authorized, for whatever reason. Or that 5.3 percent could also be people who voluntarily choose not to contest. These are people who got a tentative non-confirmation, and for whatever reason they decide, you know, I don't care to contest this, and they can walk away. There's no harm, no foul in those instances.

The .5 percent -- and this is what Rebecca was talking about earlier, as well -- is the successfully contested. So, they say, "No, no, this mismatch is incorrect, I'll go in and I'll contest it," but then they were later found to be, "Yeah, that's correct." You know, "You were right and we were wrong, you are work authorized, so please continue working." That's a number that we focus on quite a bit as well. The truth is that E-Verify -- we don't want a 100 percent match rate, automatically, right away. That's wrong, because if we got 100 percent, those are all employment-authorized. There will be some people here who are not legal to work, who are not legal to work, who are not employment authorized, therefore, that automated match should not take place.

So, the question is, how high do you want it to be? It's not 100 percent, but -- so you want to bolster up that 94.2 percent to make sure the most automated matches are happening correctly, and to know that whatever is left over, are the people who genuinely either chose not to contest, or genuinely were not work authorized.

Down at the bottom, we talked about some of the enhancements that we're using to address those specific concerns, so from SSA's concern, obviously was naturalized citizens, sometimes we would receive tentative non- confirmations for U.S. citizens, simply because SSA didn't have a record of the fact that they naturalized.

We have gone through a few phases of upgrades to pass that data on to SSA, and to be able to automate that check. So, before we say this was a not -- this was a mismatch, check the DHS systems first, to see the, to make sure that, "Oh, this person didn't naturalize, never mind."

As well, we continue to add additional data matching algorithms to look for things like slight name misspellings, some that already exist. But we're also looking for other reasons for mismatches within the data -- data birth transposition errors, for instance, if someone got the day and month transposed. These are sort of thing mismatches that we look into to make sure that this is a genuine mismatch, and we're not, you know, adding additional false positives to the system. But, we want to make sure that we're addressing those things, I this was a, genuinely, a data transposition error. Next slide?

The other big, I guess, concern or question is towards E-Verify going mandatory. And we've not been idle for the last 2 years, as we've sort of been wrapping up our processes and procedures and technology in anticipation of going mandatory. We look at it as a when, not if, because that is the only way, again, to be good custodians of the system. We don't want to be caught unawares if Congress chooses to do this.

So, a lot of our processes, we look to streamline, as I've talked about already, we're looking to upgrade the technical infrastructure and remove any manual processes within there, as well. And we talked about some of the systems testing and systems capacity, which, again, I think is fine administrative assistant the infrastructure goes.

I think one of the things that we would certainly be interested in getting from the committee and hearing more about is, what additional steps could be taken to truly ensure data privacy and integrity, as we go mandatory?

The game does not significantly change as we go mandatory, in terms of how it's played, but the volume, of course, will magnify any problems. Things like security and privacy are things that we want to address right now, before we go mandatory. To, to the extent that we can get some feedback into the process early, and make sure that we're taking all of the right steps, we always welcome that sort of feedback. Next slide?

And, I think this is Claire, thank you.

MS. STAPLETON: Here's what I'm going to talk to you about, if you can just go to the next slide, please.

So, data retention -- we hold our data for 10 years, unless the data is part of an active investigation, and we'll hold it longer in that part. We based on 10 years on the statute of limitations for false statements and misuse and regarding passport, citizenship or naturalization documents. ICE is using that same statute, so it makes sense that we also keep the data for 10 years.

And for pictures, the picture comes up and the employer can see the picture, and then the image is not kept on their machine. Next slide, please?

Our privacy protections, E-Verify has a current PIA and a SORN, of course, and we've updated the PIA a couple of times, and we will continue to update the PIA and the

SORN, as needed. And we also have a dedicated privacy staff and we're growing, so we -- we're very lucky to be part of almost everything that's going on, so we're there from the beginning to help look for issues that could later be problems, and to try to make the right decision with privacy in mind from the very beginning. Next slide, please?

We base our privacy program on the Fair Information Principles. We provide information to the job applicant -- you've seen the posters in the earlier slides. We share only the minimal amount of data necessary with employers, so they send us a query with a whole bunch of information, and we're basically giving them red light, green light -- we're not giving them additional information on yes, this person's authorized to work, because they came into the country on this date with this kind of visa, it's a "Yes, this person can work," or the TNC process starts.

And then, as far as sharing access or sharing data, or even within our own team, access to PII is limited to need to know. For example, I do not see any PII, because I don't need to in the course of my job. It's only the people who are actually working on the cases who see that data. Next slide, please?

We provide privacy training, both for our own employees and for our users. For the verification employees, our privacy program is relatively recent. I started in October, so we have a basic training that all new hires do, and all verification employees have mandatory training once a year.

In addition, we're rolling out a new set of training, starting with the people who use the data the most. So, we've already trained the Status Verification Team -- they're the people who actually go in if there's a mismatch, and look in other systems, to see if they can find if the person is truly authorized or not, they're looking for that mismatch information.

So, we did a targeted training to them to kind of focus on, when you are accessing information, "Here is what you need to do in the course of your job." This is the kind of information that you can write down on your piece of paper, this is the kind of information that has to stay in the system. This is the information that you can talk about, this is what you can't talk about. How can you protect printouts on your desk? All of those kind of life day-to-day activities for protecting data, so that we don't have data laying on a fax machine all day or printouts, or things like that -- just trying to have from the very beginning.

We have our TNC letter, so it's not that we're just arbitrarily saying, "You can't work." The letter is given to the individual and says -- you have a problem, here's how you fix it. And I apologize, I forgot to bring the letter as Joanne had asked for. But we can get you that.

But just to say, “We looked you up, here's the information, here's what's wrong, here's how you fix it, you have your 8 government days.” And then, of course, our PIAs and SORNs that we love to do. Next slide, please?

So, we've done our certification and accreditation as Rob was talking about. We're updating our system, making sure that we're doing everything that we can, and as we add these new databases and photos that, working with Department of State, we have the same security in place for all of them. Next slide, please?

And then just to be clear, we're not creating a national ID database. We are limited in how we can use our data, and we follow those limits. We're only storing information in a transaction form, so it's not person- centric, and we're not looking at creating a longitudinal employment history. If you wanted to look somebody up and say, “What are all of your jobs?” It would be very difficult to do so, if not impossible.

And that's it.

CHAIRMAN BEALES: Well, I wanted to thank you all, again, for being with us, today, it -- and I want to commend you for thinking about -- thinking now about the -- what if this is mandatory problems, because I think those are very real. And, you know, based on what we heard in El Paso, I think this reengineering registration is something that really needs to be at the top of the priority pile in addressing those issues.

Let me ask you a couple of what I think are just sort of, I hope, simple clarification questions, and hopefully get relatively short answers, because I don't want to steal all of my colleagues' time.

In -- you mentioned that E-Verify must only be used to verify new hires. Are there controls to make sure that that use is what's happening, or is that just dependent on the audit and compliance of particular companies?

MS. GREEN: Right now, the monitoring and compliance folks will actually be taking a look at that, but with some introduction of some things with the Federal contractors, we're having to reevaluate that, maybe, tighten it up or employers that are not part of that Federal contract mandate.

CHAIRMAN BEALES: Okay. In the tentative non- confirmation, do you know whether that's -- when that goes out, does the individual know whether the -- they're told whether the source of the problem is SSA or DHS?

MS. GREEN: Yes, they are.

CHAIRMAN BEALES: They are, okay.

MS. GREEN: They have a letter that they’re given, and it specifically says, either SSA or DHS, with the appropriate instructions on how to resolve it with either agency.

CHAIRMAN BEALES: Okay. And as I understand it, the photo screening tool would be, at this point, at least, immigrants only?

MS. GREEN: For those with, yes. Immigrants and non -- and certain non-immigrants.

CHAIRMAN BEALES: Okay. What happens if nothing happens within 8 days? Either there's no contact, or there is, you know, there's contact, but not yet resolution?

MS. GREEN: Okay. I they've contacted, either government agency, and say there's a problem, say, for example, that, okay, we don't have it in our automated records, and we have to go and pull an e-file. Then the status verifier can actually put that case into continuance, and the clock stops.

The same thing happens with SSA. If their date of birth is wrong in their SSA record, the person's going to have to not only show their birth certificate, but SSA goes an extra step, and checks with the State Vital Statistics Offices to make sure. So, we recognize that that time period is not necessarily conducive, so that’s why we have the continuance piece.

CHAIRMAN BEALES: Okay, so all that really has to happen within 8 days is the employee has to start the process in some plausible way?

MS. GREEN: That's correct.

CHAIRMAN BEALES: Okay, and that answers my other question there, as well.

In introducing this pre-TNC check, the pre-TNC page, it seems like there's a good way and a not-so-good way employers could use that. The good way is to correct typographical errors in entering the data, the bad way is to find out whether this person is going to be a hassle, and kick him out. Do we know how many of the ones that don’t match, in that pre-TNC screen, are, in fact, resubmitted?

MS. GREEN: We could probably pull that data, I just don't have that information available at this time. But I do know that if a person hits the “back” button, the system will actually capture it as an incomplete transaction, and those are the ones that we can target.

CHAIRMAN BEALES: Okay. It would be interesting to know how many of those there are, because that goes to this question of how employers are actually using it.

Do -- on the .5 percent that are successfully contested, do we know anything about what the causes were of the error?

MS. GREEN: We don't have that broken down in a report, but I'm sure we can pull that from our database. We do know the reasons for the TNC, but not what the 5 percent fallout is, or the .5 percent.

MR. GAINES: Yeah, we currently do have some data-matching initiatives going on right now, to really look at the data matches, either good or bad, essentially, to determine the reasons behind them. And some of them could be typographical in nature, some of them could b more systemic of a particular class of citizens. We obviously endeavor to really address that -- the latter category. If we think it's a particular class -- like the naturalized citizens -- we get right on that. But that's -- we're essentially looking at the data right now to determine why it is. You can slice it up many different ways, but I know that that's part of the analysis, as well.

CHAIRMAN BEALES: Right. And I appreciate that you don't, necessarily, want 100 percent match, because it's easy to say, yes, everything matches, whether it does or not. And that doesn't help you much. But it's also that -- the .5 percent is small as a proportion, but it is an enormous -- and will grow rapidly -- number of people that have to be dealt with manually. And, you know, sort of, anything you can figure out about how to make that go away, seems like it's good for everybody.

MR. GAINES: definitely. As you say, .5 percent sounds small, but in a mandatory world, everything gets magnified. So, it's certainly an area of concern for us, as well.

CHAIRMAN BEALES: Right. Of the 5.3 percent that are either not work authorized, or the employees didn't pursue, do we know what the mix it?

MS. GREEN: We can actually pull that data for you, we have a report that show all final non-confirmation and no-shows, and the breakdown for those.

CHAIRMAN BEALES: Okay, that would -- that would be very useful information, as well.

MR. GAINES: That might be in the WESTAT report, as well, too, I don't -- I think it is, actually, if memory serves.

MS. GREEN: Okay.

CHAIRMAN BEALES: And that -- that goes to the SSA database, right? The WESTAT report?

MR. GAINES: It addresses both sides.

CHAIRMAN BEALES: Okay.

MR. GAINES: Yes, it actually breaks down to say, like, what percent is SSA's versus DHS at all levels.

CHAIRMAN BEALES: Okay.

All right, well again, I thank you -- thank you for being here, and I think what we want to do is to help and –

MR. HARPER: The question I want to ask is closely related to that.

CHAIRMAN BEALES: I have the queue, but you were second, so you can go first, Jim.

MR. HARPER: Well, that made me quite obnoxious, didn't it?

[Laughter.]

MR. HARPER: The usual, good.

I was very interested in the numbers, and I think I got a new number to work with -- it's sort of like trying to put together a jigsaw puzzle, and one piece is all blue, and one piece is sort of mottled green, and you know you've got a sky and a tree, and none of them are edge pieces.

But actually, we've got edge pieces, because I added up the 94.2, the 5.3 and the .5, and it comes out to 100. And I was delighted to know -- at least know that I have a solid grasp of how these are breaking down.

I do think it's important to try to figure out what's going on with the 5.3, because I think it's easy for people to carelessly assume that the 5.3 who go away are all illegal immigrants, and we're done, and that's quite irresponsible. Because some of them are probably work- eligible American citizens, or immigrants who have been pushed out of lawful employment by the system.

And that -- focusing on that, I want you to check me on sort of overlaying a new statistic that you gave, which is the 30 percent improvement based on the fat finger TNC page, if I'm coining a phrase you want to pick up and use, feel free. The fat finger data entry is obviously responsible, or was responsible, for at least a 30 percent of your TNCs before this new page. Which suggests the data sets may overlap in time.

So, this might not be perfect use of the numbers, but it suggests that -- and this is what I want you to check me on -- is that if 5.3 percent o your applicant pool are going away, and you've now improved that by 30 percent, 1.59 percent of the people going away were because of -- because of TNCs, and if you back out the .5 percent that could successfully contest, you have 1.09 percent who are likely entitled to work in the U.S., but they're going away because of the fat finger thing, and just not resolving it.

How poorly articulated was that?

[Laughter.]

Well enough to check my thinking on that?

MR. GAINES: I guess the first thing is the numbers, of course, get more and more complicated the closer you look at them, so I'll always caution on that. Because, first of all, if you start with the 5.3 percent, you want to start looking at, well, how much of that was

SSA versus DHS, so that, did you even get to that point? But holding the actual numbers constant.

It's a good question. I mean, really it boils down to, like, who chooses to contest? And currently, to your -- as you say -- we don't assume, necessarily, that this is an illegal. I mean, I could just say, "You know what? I chose not to work here, it's not worth my time, that's okay. No harm, no foul." So, we don't have any bad things associated with the individual.

MR. HARPER: Or, of course, if the employer never communicated to the --

MR. GAINES: Exactly, I mean, yeah, that's just – which one of the things we certainly will look at in our monitoring program, and see, lie, if there are a lot of final non-confirmations coming out of an employer, that could be evidence of a bad employer who never tells, "You know what? It's not worth it to me for these guys to lose a day to go talk to whatever," and just never bother to tell someone. We're not assuming that, but it's certainly a concern.

I think to the point, though, saying like, you know, addressing the -- the naturalized citizen, and sort of the pre-check versus afterwards -- I think it's that you want to check the point at which a person is able to make a decision. For instance, the person with their fingers in the keyboard, the employer, who chose to hit the "back" button and say, "Hey, never mind, I chose not to."

But, once it's been referred to an employee, it's instructive to know, well, did they just chose to say "never mind." So, it's kind of the question of who has the ball, really. If it's the employer, or we -- we're not sure, then we want to make sure that we're addressing the right problem. If it's pre-screening and progress and what we'll see is a lot of the employers saying, "Ha, ha, ha, I'm not going to bother."

But, if it's a lot of referrals to the employee who just never bothered to follow through, it could be an illegal, or it could just be someone who didn't both, or didn't care. But it's a valid concern.

I don't know, Rebecca, do you have any other thoughts on that?

MS. GREEN: Yeah, actually, we have several initiatives that are either in planning phase, or in the evaluation phase that directly affect the employee. And I mentioned two of them, and that would be the final non- confirmation, and the Request for Reconsideration process.

We're hoping that this process that we're developing, not only can they update their records, but say they had, for whatever reason, they did not contact a government agency in the required time period. That they would actually be able to go in and say, “Hey, I believe I'm authorized to work,” and they would have that recourse, after that particular case was closed by the employer.

The other thing that is actually in the evaluation stage, is looking at ways to have the employee more involved in the verification process. USCIS has a really good thing online called the case status online, where employees can actually go out and -- to check whether or not, where in the process are they being adjudicated? Where is their request for an EAD, or the request for an actualization? And we're actually looking at that to -- as a model to kind of incorporate into E-Verify for employees, to check on their own personal case with E-Verify.

The tricky thing, though, will be, how do we go about doing that with minimal amount of data? Because we do not want people going in there, and phishing, and putting names and numbers in. And it would have to be something that is not PII related -- probably our case verification number. But again, as a -- so that's kind of on the table as things we're looking at.

We have some other initiatives we have to get out the door first, but I mean, it is a concern for our office, and we are moving forward to address some of those things.

MR. HARPER: Okay, thank you.

CHAIRMAN BEALES: I just wanted to clarify, I think what -- the way I understood what you said in response to one of my questions was that you did have some data on how the 5.3 percent breaks down, as to where they drop out, and that you'll provide us.

MS. GREEN: Yes.

CHAIRMAN BEALES: Okay, thanks.

Renard, who was supposed to be first.

MR. HARPER: Thank you, Renard, I'm very sorry.

Mr. Francois: I just have a quick question about those employees who receive a TNC notice and who decided to challenge the notice. I know you all provide 8 days for them to begin the process in some way, shape or form. Do you have a sense, in the feedback that you've received, or in the information that you collect, for how long, on average, it takes to resolve the dispute, for those that got a TNC notice, challenge it, and then are cleared to work?

MS. GREEN: Actually, we do have that data. The DHS data, we actually, for E-Verify side, it's part of the statistics that we report up to the Director and the Secretary. So, we don't have cases out there for longer than 30 days, for DHS.

SSA, they just implemented a new system in October that allows us to view how they're working their cases, as far as statistical reporting is concerned, and we have a report that was just recently developed that actually breaks down how many cases were worked in one day, how many cases were worked in three days, and that type of thing, and we can provide that to you, as well.

Mr. Francois: That would be great.

MS. GREEN: Do you have it?

MS. BARNES: Yes, I believe I do have some statistics -- 99.5 percent of work-authorized employees are confirmed instantly or automatically through the system. Ninety-nine percent of all SSA TNCs are resolved within 2 days after the case is referred to the SSA agency.

And, unfortunately, we'll need to get you the additional information. But that's just some information that might be helpful.

CHAIRMAN BEALES: Okay, a preview of what's to come.

MS. GREEN: A preview.

CHAIRMAN BEALES: Ramon?

MR. BARQUIN: I'm sorry, but I still don't understand a lot here, so I'll try to go quickly through what are some very direct questions about the presentation.

First of all, is this service free, or do employers have to pay?

MS. GREEN: It is free of charge.

MR. BARQUIN: Okay. Now, you said that, because the emphasis is on employee rights, and so it's only for new hires, not for existing employees, but you said that individuals should continue to work until -- but is, you know, getting the okay from E-Verify not a condition of employment? Otherwise, why is the employer doing it?

MS. GREEN: It should not be a condition of employment.

When Congress passed IRIRA, it was to help employers out with the document review portion, because there’s a lot of documents out there that are very hard to validate, and so they're like, “Let's validate the information that these folks are providing.” So, it was initially as a tool to help with the form I-9.

It's kind of morphed a little bit over the years, especially after 9/11, moving towards looking at document fraud with Federal substitutions, and it's just been kind of an evolutionary process for us.

MR. BARQUIN: All right.

MS. GREEN: I mean if you want some more, I can – if you need some more.

CHAIRMAN BEALES: As I understand it, this was originally a, sort of, a safe harbor for immigration enforcement. If you went through this and nonetheless, an employee turned out to be illegal, they wouldn't prosecute the employer. Is that –

MS. GREEN: It's only if the government said they were employment authorized.

CHAIRMAN BEALES: Right, right, right.

MS. GREEN: If the -- I mean, if the employer doesn't do what they're supposed to do, following the procedures and the MOU, then they do not have any [indiscernible] option.

CHAIRMAN BEALES: Right, I understand that, that would be -- but that was the carrot.

MR. BARQUIN: Well, I guess that one of the things that I would certainly suggest might be need -- it may already be there, but you didn't -- because the focus was on employee rights, and I can understand and applaud that, but given the fuzziness of where -- I would think that employer rights are also important here, too, because you could get into trouble. And especially if you're dealing, also, with a number of people that should be able to work, but just throw their arms up in frustration and say, “Huh.” Which happens.

What is a derivative citizen? Which I saw in one of your slides? MS. GREEN: A derivative citizen normally is a person whose parents has naturalized before that person's 18th birthday, that's a good portion of them. So, I mean, it's just, you know, most of these folks have U.S. passports, so that's why we're wanting to do the Department of State piece.

MR. BARQUIN: And on data retention, you said 10 years, but 10 years from when? Ten years from the -- a specific transaction, 10 years from --?

MS. STAPLETON: Well, it's transaction-based, so each transactions is kept -- so, if you're run through E- Verify now, and then 5 years from now and 10 years from now and 15 years from now, we'd have the last two transactions, but not the one that would be 15 years old.

MR. BARQUIN: Okay, last --

MS. STAPLETON: It's not based on you by, by number.

MR. BARQUIN: Got it.

Last, and this is just a comment -- my, I think there's a certain amount of fuzziness here vis-à-vis the redress program, because you can see that up to a certain point, it may lie with the employer, and up to a certain point it really is more of a systemic redress that probably should lie with USCIS or with E-Verify.

And I just didn't get a good sense that it was all concisely and clearly put together in one pace. Maybe it is in an E-Verify, you know, help or FAQ, but again, it just question and advice that maybe it needs to be integrated into a much more clearly and visible and accessible approach, here, for both employees and employers.

MS. GREEN: Right.

Speaking of redress for the tentative non- confirmation, employers actually have to go through about an hour to two and a half hours worth of training. And that process is discussed in detail.

Additionally, there's a user manual that they can refer back to, and my employer instruction and training unit, they are in the process of even simplifying that further, into quick reference guides that they can actually have on their desks.

The other thing, is with the tentative non- confirmation and the referral process letters, we're actually addressing that issue there, and it really is explaining to the employer and the employee what their rights are, and what their responsibilities are under those processes. And those are letters that we're hoping to roll out very shortly.

CHAIRMAN BEALES: Dan Caprio?

MR. CAPRIO: Thanks, Howard. Just a quick follow-up to, I think, Renard's question then a couple of quick questions.

So, I mean, we've sort of heard the best case scenario for the resolution of the .5 percent. I mean, as part of the request, I think we'd all like to know, sort of, what's the worst case? You've said 30 days within DHS for resolution, but, you know, I think we need to as part of the record, to get an understanding of what they -- what the worse case is. I know you can't answer it right now, but --

MS. GREEN: Well, I know we have, like, timeframes built out for the case in continuance, and I believe the cutoff date for DHS is 30 days.

SSA has a more elaborate process and theirs in 120, because they're actually -- especially when they're talking with State vital statistics offices, you have to allow for them to respond back, because some of them are not as automated as others, and it may take some time.

But, because we're looking at our own personal data, we consider 30 days an appropriate amount of time.

MR. CAPRIO: Okay, well, that's -- thank you.

So, three quick questions, really, for Robert. You discussed, or talked about planning for mandatory, but in fact, I mean, you're going mandatory with the Executive Order for contractors. So, the question is, you know, what kinds of -- first question, what kinds of specific requirement do you plan for subcontractors, i.e., small business-related to protecting privacy and security?

MR. GAINES: Make sure I understand the question. So you're asking, in a mandatory world, or just in general, because we know we're going there, we should, what are we doing?

MR. CAPRIO: No, I'm asking in the, I mean, in the example, the Executive Order. I mean, the contractor example. And so, it's really a general question, but with respect to a small business or a subcontractor, I mean, there are certain obligations, really, to protect privacy and security in the network. So what -- because the chain is only as strong as the weakest link.

MR. GAINES: Right.

MR. CAPRIO: And we all know that, you know, the profile of a small business or a subcontractor can often look like a home user.

MR. GAINES: True.

MR. CAPRIO: And so what, if anything, do you -- do you have planned in terms of, I mean, I guess it would come out in the NPRM or the final rule -- but to deal with that community which is obviously not as sophisticated as sort of, some of the larger businesses that are already -- or a contractor, already engaged in E-Verify?

MR. GAINES: Rebecca, I'll take this, but I don't know to what extent we can talk about the rule while it's being, you know, worked on.

But, I think I can go over some of the things that we're doing, regardless of that.

As part of our registration reengineering, one of the things we're looking very closely at is, as I said, sort of the identity assurance and all of that, and to know the company is who they say they are.

But equally important, from our perspective, is to know what the hierarchy is within a very complex organization, or perhaps in situations of, where we have, say, a designated agent who then has clients. What is -- what are the relationships between everyone in that hierarchy? So, when someone registers to use our system, it's very important for us to get to know how it's going to be used, and in what context?

So, for instance, a designated agent might have many, many people that they serve. But we -- right now, frankly, we're a little weak in actually knowing, specifically, who those companies are, and what their profiles look like.

As we look to tighten up the registration process, we want to ask more intelligent questions. So, from a usability perspective, the way I usually put it is this -- is usability for a small, family-owned pizza shop is a wildly different question that usability for a large, multinational conglomeration like, you know, Northrop Grumman, or what have you. And I think we're looking to address both communities, obviously. But as far as the, like, the subcontractors, and what-not, that I think falls into some of the same category of going like, well, what's the hierarchy, to say like, well, Hey, I run E-Verify, but I run subcontractors. Is it enough to know that they run E-Verify and they've run through the system, or do I have to do it on their behalf to know at the end of the day.

From the rule perspective, I don't know if that's been decided, at all, if that's going to -- how that’s going to work.

MS. GREEN: No, I don't think that's been decided yet.

MR. GAINES: But, I think we acknowledge the idea, the fact that that is a problem that will have to be dealt with, but -- and right now the -- ironically, the registration and engineering is a good place to look at that.

MR. CAPRIO: Well, let's continue to work together on that, because in the pizza example, the subcontractor or the small business could be running it off of a laptop, without any sort of network security, without a firewall, without anything. And so, we need to educate, and sort of plan for that contingency.

Two other quick questions, you mentioned your work with the anti-phishing working group, but I'm wondering, kind of, what kinds of initiatives or education and awareness, I mean, you've -- that's a big issue. What do you have planned, specifically around phishing and social engineering?

MR. GAINES: That's an interesting question, I'll be honest, we haven't gotten deep into it. But the way it started off, or the interest was, essentially, to address concerns that, you know, could someone approach one of our employers, pretend to be DHS, like in an email, and then say, “Oh, please send us your SSN information to us, because we need to verify it, because we didn't get it through E-Verify.” There are broader initiatives across DHS to do some of that, so we're mostly looking to align with that.

That was the primary thing, but I think the other more, like, the social engineering attacks, but with certainly one of the wonderful side effects we're looking to look into as part of that group.

But, to be perfectly honest, we haven't gotten too deep into that, yet.

MR. CAPRIO: Okay, one final question -- you mentioned in your comments about photo validation tool, and I thought I heard you say that that was the only tool, or the only way that you can fight identity theft and fraud -- did I hear that correctly? Because that -- we need to be paying an awful lot of attention to identity theft and fraud.

MR. GAINES: Indeed, I'm glad you clarified, if I said that then I spoke incorrectly. The truth is that's -- I meant to say, it's certainly one way, and it's maybe not as strong as it could be, because people, you know, one of the criticisms of E-Verify is saying, currently we don't fight true identity theft. If I register with E-Verify, you know, pretending to be you, and I have all of your information, how would we know? Because all o my documents would check out as authentic.

Well, that's true to a point, because obviously we have the photo substitution. So, like, the photo tool will catch that kind of photo substitution. So, if I put in all o my information and say you, but I substitute the photo, I'll catch that particular kind of check. But, I you and I happen to look alike, and this kind of identity theft happens, what can we do?

And again, it's sort of a hybrid solution, we can't just look at one area of identity assurance. Our monitoring group, for instance, might notice that, "Hey, it looks like you're working in 100 different jobs across the country simultaneously." Seems unlikely, you know? And of course, the problem is, if it's a small thing, it's like hey, you're working 5 jobs, you might genuinely be.

So, I think that the photo substitution -- like, the photo tool is there to catch, essentially, photo substitution fraud. It's really not what I would consider a strong identity check, it's there to catch that specific kind of fraud. And there are other kind of fraud, but I think that's an important point, is people kind of assume, "Oh, this is part of, you know, facial recognition," or something like that, which is absolutely not the case.

MR. CAPRIO: Thank you.

CHAIRMAN BEALES: I don't want to cut this off quite yet, because I know we have a lot of questions, but we also have more tents than time.

So, if you have a question, can we think about whether we can -- what I propose to do is to send a letter from me asking for more questions and more answers in writing, including all of the stuff I already asked for, and then we could spend a few more minutes on this, but I you can make you question a written question and that works, then we do still have two more panels this afternoon.

MR. PURCELL: I just wanted to quickly ask for your attention to be paid to a statistic that we've been talking about all day, but we haven't focused on at all, and that's the false positives.

In other words, if 94.2 percent of E-Verify submissions, transactions, come back within a very short time saying, "Cool, you're good to go," how many are wrong? How many of those "You're good to go's," end up verifying somebody who actually hasn't a right to work? And that's a big deal. How many times -- I we're saying half a percent are false negatives, you say, "No, work it out, oh, it's really a yes." How many of the initial yes's actually should be no's but you don't know that, and are you doing anything to figure that out?

CHAIRMAN BEALES: Let me add a slight twist to that, because in terms of my big fear about the program, of people getting in and creating name and social combinations that will pass, where that's going to show up, is that false positive rate's going to go up over time, and it's really important to have a feedback loop to figure out what's going on.

MR. GAINES: I totally agree. I mean, these are obviously huge concerns from us from a security perspective, because to say that we let someone through that essentially that shouldn't have been, is a big concern.

I don't know that we have specific data on that. I will say, however, that currently our processes are pretty simple in terms of our check, in terms of something like doing an exact match of, like, name, date of birth, and if there's ever a mismatch, send it to a tentative non- confirmation.

At this point in the program's evolution, I think we're being overly cautious, and that's to say, like, "Hey, if we get a mismatch, send it to a status verifier, and let a human make the determination."

However, the truth is that every time we talk about, Hey, we'll have a soft, fuzzy name mismatch, you know, algorithm to do in there, then you introduce the concept of potential false positives.

I don't think we have specific data on that, but I will say that these are not, like new algorithms. Like SSA has built this into Numident systems, to do these kind of --

MR. PURCELL: Understood, but algorithms be darned, what if a person matches one-to-one perfect match, 100 percent, alpha to numeric, match to match, but it's not that person. And since they are not an immigrant, they are a born citizen -- the data represents a citizen of the United States -- you don't have the photo matching, you don't have anything else -- you're fine, good to go.

MR. GAINES: And that's actually -- well, partially our reason for wanting to add the additional sources of data, say the passport photo, or the visa photo or what-not, to be able to kind of catch more than just people with a green card or an EAD card.

MR. PURCELL: But it seems like what you need to do is you need to build a link with the enforcement arm, because that's where you're going to find out where the false positive was –

MR. GAINES: Yes.

MR. PURCELL: And, you know, that link needs to be built as soon as possible, because you're not going to find it in your system by the nature of the problem -- you're not going to see the false positive -- it's the enforcement guys who see the false positive and -- but you need to find out about it.

MR. GAINES: That's good feedback. I think the only thing that we do is like, in terms of our data- matching analysis, we are, essentially doing a full-on data-matching analysis.

The only way to look for false positives, essentially, is to look at the data, know the data completely, and then run through and see what comes through, based on what you know of the data.

You're right -- see the day to day usage of the system would never bring out a false positive. The only two ways is to catch it after the fact, as you say, like, “Hey, enforcement has already flagged this, why did you let it through?” You know, or more of the closed loop, it's like saying, So, essentially this is what we're doing from the data-matching analysis, is to take the data, freeze it in amber for a time being, and set it aside as our testing playpen, to be able to truly look at the data analysis matches. But the feedback from the enforcement side is actually a good idea.

CHAIRMAN BEALES: Neville?

MR. PATTINSON: I'll submit a question in writing about the jurisdiction of how you get together with the passport data. That's unclear to me as how you're creeping from the SSA and DHS information and then going after DOS information. But that's some -- I'll be bringing a question in writing.

The specific question I'll ask now which is quite short -- actually it's not a question, it's more of a comment -- the photo tool could actually be a very useful tool to people making fraudulent documents. You're giving people the actual photograph to an employer. So, I would recommend that the photo is obscured, watermarked, or filtered in some way, so that even though it is the exact photo used when they originally applied and enrolled in the system that you don't make it useful to make that to be substitutable on a document. Because you're giving them the very photograph that they need to make the false document.

MR. GAINES: That's good feedback, actually we have -- I don't think that it's any secret -- we've been talking to DMVs to see if any of them were interested in joining that -- we've gotten very similar feedback from them, as well, but that's absolutely a good point.

CHAIRMAN BEALES: And that really feeds back to the registration problem.

John?

MR. SABO: So many questions, so little time.

So, let me just hit one, and that gets to -- you’re getting into a space that other agencies have faced before, which is an escalating workload. So, we have a lot of security issues, here, which I'll, I'm sure will feed into the questioning.

What size of staff do you have? What do you -- what's your process now for evaluating some of these issues that impact the workload and the sustainability? I'm not talking about the speed of your servers -- you mentioned this earlier. But as you move into all of these new -- you're now talking about links to State and passports and DMVs -- and as you build the system, and you move into the mandatory contractors and everything else, what's the -- who is estimating the work-year cost, or FTE cost, and what are your estimates for the FTE cost to SSA, and to your own organization as you scale this? Do you have any data like that?

MR. GAINES: I believe we've provided some data in some of the GAO testimony, as well, do you guys know off the top of your heads?

MS. GREEN: I just don't have that off the top of my head.

MR. GAINES: We don't have that information --

MR. SABO: Well, I don't think I want it off the top --

MR. GAINES: Well, that's good.

MR. SABO: -- I'm saying, do you have such --?

MR. GAINES: Absolutely. I mean, in terms of scaling up the program, I know that SSA is putting their two cents in terms of what they feel will be necessary from a manpower perspective, to scale up.

And from our perspective, from a program perspectives, I think there's really two branches, in particular, that need to be able to scale-up in a large way, in a mandatory way.

One is our status verifiers, on the back end we're dealing with the mismatches. And we've already, standing up another, second site, essentially, to house them specifically, so they have plenty of room to grow there.

The other group is, essentially, our compliance group. Is, if we want to have a certain touch rate with employers, to reach for, either for assistance or for investigation purposes, it would be good if they were more regionally based, so they could be closer to the companies that they're serving.

Those are the two ones, and I know that both of those groups have been aggressively looking at like our projected volumes as we go mandatory -- or even just as we grow normally -- and then what that equates to, in terms of FTEs. So, we don't have it right now, but yeah, absolutely, that's a huge one.

MR. SABO: Does that include SSA FTEs?

MR. GAINES: I know they have done their own analysis, too, based on some of those projected query logins.

MR. HARPER: Mr. Chairman, just briefly for John, there was a GAO report that came out in the last couple of days, I think, expressing in dollar terms what the needs would be at USCIS -- $765 million to cover Fiscal Year 2009 through 2012, and $281 million to cover SSA for Fiscal Year 2009 through 2013. So, it's a sense thing.

CHAIRMAN BEALES: All right, I want to thank you all for being with us. I think this is an important program, and one where we'd really like to help you as much as we can, in trying to make improvements. We do, every once in a while, have a good idea, and we would -- we look forward to continuing to work with you as this program moves forward.

With apologizes to our last two panels, we now move on to talk about the Information Sharing Environment. First, we're going to hear from the Department, from Susan Reingold, who's the Deputy Program Manager, of the Information Sharing Environment Program Management Office, in the Office of the Director of National Intelligence. And she has been in that position since November of 2005.

She was previously the Associate Director of the Office of State and Local Government Coordination in Homeland Security. Before she joined DHS at its inception in 2003, she managed State and Local Outreach of the Critical Infrastructure Assurance Office.

MS. REINGOLD, welcome.

MS. REINGOLD: Thank you. I appreciate you inviting me back to talk about the efforts to enhance information sharing. And when I last talked to you, I guess it was last September, I provided an overview of the Program Manager, and talked about some of the activities surrounding information sharing, specifically between the Federal government and State and local governments and Fusion Centers.

And so, what I wanted to do today, before Deborah Draxler talks, is to give you an overview of a couple of other initiatives that might be of particular interest, related to the information sharing environment. Go to the next slide, please?

Since we were last here, the President issued the National Strategy for Information Sharing in October of 2007, and I know that there were copies that were provided to everyone. The important thing about the strategy is that it builds on progress that's been made since the September 11th attacks, and really, for the first time, lays the foundation to establish an integrated, national information-sharing capability.

The strategy itself was developed through a very collaborative process, and based on significant input from both the member of the Federal Information-Sharing Council, and that's an Advisory Council to the Program Manager, as well as right from the beginning, working with State, local, tribal, and private sector officials from across the country.

And many of the principles and priorities that I shared with the group last September have been incorporated into the strategy. In particular, it recognizes that partners must be assured that their information will be protected from unauthorized disclosure. Another important point is that the American people must also be assured that their information privacy is being protected and also the strategy also expresses the commitment to ensuring that those responsible for combating terrorism and protecting our local communities have access to timely and accurate information. Next slide, please?

The strategy identifies two key mechanisms to support enhanced sharing with State and local officials. One is the establishment of the Interagency Threat Assessment and Coordination Group at the National Counterterrorism Center and that's to facilitate the production of Federally-coordinated information -- terrorism information products that are intended for dissemination to State, local, tribal and private sector partners.

And the strategy, then, also calls for a national information sharing capability, through the establishment of an integrated network of information fusion centers. And there's an annex at the end of the strategy that's outlining the roles and responsibilities of Federal, State, local and tribal authorities in the establishment of this national integrated network. And this is really the first time that there's been guidance of this sort. So, that was an important step forward since we last spoke. Next slide.

Another initiative that's very important, and I'll go back to December 2005, where the President directed that information privacy and other legal rights of Americans be incorporated into the ISC and that instructed, very specifically, the development of a set of guidelines, additional guidelines that specifically address the acquisition, access, use and storage of personally identifiable information in the ISE.

And so, basically, in response in November 2006, the President approved and the Program Manager issued guidelines to ensure the information privacy and other legal rights of Americans are protected. And what's on the slide is really -- it's a snapshot of our webpage and it does show you, essentially, I'm going to be describing 3 documents and such, that are there covering privacy issues.

The first was the actual privacy guidelines, and they for the first time required each agency, Federal agency to have -- to designate a Privacy Officer, if they hadn't done so already, and also develop a written information sharing environment Privacy Protection policy that sets forth the mechanisms to implement the privacy guidelines.

At the same time, the Program Manager established a privacy guidelines committee, to make sure that there was consistency and standardization in implementing these privacy guidelines, and the other reason was to have a forum to share best practices, and resolve interagency issues.

So, this committee, actually, is comprised of ISE privacy officials that are designated by each of the 16 Federal agencies that are members of the Information Sharing Council, and the committee also serves as a resource to ensure privacy principles are incorporated into all activities related to the Information Sharing Environment.

The next step in September, this past September 2007, was this Privacy Guidelines Committee developed, and then we issued Privacy and Civil Liberties Implementation Guide for the ISE, and so the first step was the guidelines, then an implementation guide to help the agencies, and it really describes the processes for ISE participants to follow when they're integrating privacy and civil liberties safeguards into their information sharing efforts. And that includes an assessment of whether their current activities actually comply with these ISE privacy guidelines.

So, just a couple of kind of descriptors, in terms of the guide itself. The point is, it was supposed to be descriptive to provide guidance on effective ISE privacy protections, wanted it to be realistic and practical to encourage the use of existing resources, and efforts to implement privacy requirements and most important to try to avoid duplication of effort. To not be too prescriptive, to basically, tailors implementation to each agency's unique environment, let the agencies do that and to be flexible, so that it can could be used in whole, or in part, in any way that would be effective for an agency. And finally, for it to be iterative, understanding that it will be reviewed and updated periodically, with additional guidance, best practices and lessons learned, as people implement the guidance itself.

So, there were two stages with this implementation guide, the first one is for the agencies to assess their existing information privacy frameworks, for sharing ISE terrorism-related information, and then develop or document an ISE privacy protection policy. And then stage two is to assess any existing or planned systems, sharing arrangements and protected information that’s covered by the ISE, and then protects such systems and information by documenting their training, reporting, and doing audits.

These guidelines and the guide and such were also made available to our State and local and tribal partners. Obviously the Federal government can't compel their use, but they are made available and I know are helpful in that environmental, as well.

Finally, this last February, also on the website, the third of these documents was published, which was an implementation manual, to provide resources and tools for ensuring compliance with these privacy guidelines.

Finally, what's important, kind of, with this whole process and I want to mention, particularly because of the next panel you have, both the privacy guidelines committee and the Program Manager, make a point to consult with both privacy and open government advocacy groups, to ensure that we understand their concerns, and take them into consideration as documents and policies and such are being developed. Next slide.

Go onto a different initiative that is a little bit more recent, that is the concept of controlled, unclassified information. Just last month, the President instructed Federal agencies to begin to standardize the way that they share sensitive but unclassified information and he formally established a controlled unclassified information, the CUI, framework. And this was basically, this resulted from almost a year and a half to two year- long process that was the result of Presidential direction to review current practices that impeded sharing, and to propose this new framework.

So, what happened was the Program Manager set up an Interagency Committee, again, with State, local and private sector input, to examine the problem. And what happened was research really showed that Federal agencies set their own access policy for sensitive, unclassified, information, that led to a growing number of markings and designations, and it was confusing, both to producers and users of the information.

Basically, we stopped counting after identifying about 107 markings and about 130 different labeling and handling processes and procedures for sensitive but unclassified information. And this is, you know, at the Federal level alone.

You know, an example is just marking For Official Use Only, FOUO, and markings like law enforcement sensitive, as well.

And basically, where we are right now, and why we're moving to this new framework is that many existing information sharing practices not only impede the timeliness, accuracy and ready flow of terrorism information that should be shared, but also often fail to identify and control a more limited flow of information that really and truly needs to be protected. So, coming at it from both sides.

So, what the President's memorandum did is it establishes a single policy for the Federal government and reduces the over 107 different markings to about 3. And again, having worked with State and local partners, as well as primarily the critical infrastructure private sector partners, as well, they were very interested in implementing, as well, and so this was something that everyone thought could happen.

I do want to clarify that the purpose is to standardize and to simplify. It's not to classify or declassify new or additional information. The new framework is not a classification system, and it will not change the public's ability to gain access to information that's otherwise available under the Freedom of Information Act. Again, the memo wasn't designed -- the President's memo -- it doesn't explicitly change anything as part of the FOIA, the Freedom of Information Act process. And current practices and procedures related to FOIA, and whether to disclose or release the information to the public, those remain in effect.

So, I just wanted to emphasize, the whole point was to standardize and simplify, and to minimize that information that really needs to be protected, but that information that does need protection, do it in a standardized, simple way that everyone can understand.

So, basically, this framework was developed by representatives from over 12 different Federal agencies, and as I mentioned, consultation with designated State and local and private sector, as well. Congress, as you might be aware, has also called for uniformity of this SBU information, and Senators Lieberman and Collins recently sent a letter, in April, to the President and even more recently, Congresswoman Harman introduced legislation specifically identifying for DHS to implement this CUI framework.

So, just to close on the CUI piece, the transition from SBU to CUI across the Federal departments and agencies is supposed to be fully implemented within 5 years. There's a lot of discussion and such -- the framework was set up to be flexible, so that there could be discussion about how to implement, and there's going to need to be policies put in place, and training, and such.

But there are some departments, such as the Department of Defense and I know DHS also has had discussions, where they're already looking at how they’re going to implement the framework.

The final point is that the -- there is an Executive agent for this, that's the National Archives and Records Administration, and they have established a new office to do this job. They're also going to, as part of, the President put in the memo that they're going to set up a CUI Council, comprised of Federal agencies, as well as private sector, and state and local membership to advice during implementation.

And I've got one more initiative, next slide, please, to make you aware of, and that's talking about, for the Information Sharing Environment, that there's now a standard for suspicious -- terrorism-related suspicious activity reporting.

Again, when we talk about the Information Sharing Environment, it's not about building a massive new information system. It's all about aligning and leveraging existing information sharing systems and policies and business processes, technologies, as well, and then promoting a culture of information sharing, through increased collaboration.

And we've, as part of all of these discussions, implementation really does vary from community to community -- by that I mean, defense community, intelligence, homeland security, law enforcement, diplomatic -- because there are different mission needs, and there's different capabilities of each of those.

So, rather than striving for identical implementation, we've worked to produce common frameworks that are supplemented by mutually-agreed upon, what we like to call, mostly common policies, business processes and standards. And so, one of the ways we do this is through a program we set up that's called Common Terrorism Information Sharing Standards, and these are business- process driven performance-based common standards for preparing terrorism-related information for maximum distribution and access, and again, to enable the acquisition, access, retention, production, use, management and sharing of terrorism-related information within the Information Sharing Environment.

So, this past -- in January, we issued the first such standard, and that was on the topic of suspicious activity reporting, and again, that is publicly available on our website if anyone is interested, that's www.ise.gov.

Just to clarify, Suspicious Activity Reporting, we would define it as, it's the process of documenting the observation of behavior that may be indicative of intelligence gathering, or pre-operational planning related to terrorism, criminal or other illicit intentions. And so, the whole point the effect of sharing, of Information Sharing Environment Suspicious Activity Reports, the point is, that it's -- it will enable the discovery and analysis of potential terrorism-related patterns or trends on a regional and national basis, which would be beyond what would be recognized, simply within a single organization, a jurisdiction, a State or a territory.

And so, this standard very specifically supports a limitation of the President's National Strategy for Information Sharing, which identifies Suspicious Activity Reporting as one of several priority information exchanges between the Federal government and our State and local partners.

My office is currently sponsoring what we like to call Evaluation Environments, in partnership with DHS and the Department of Justice, to actually test implementation of this standard.

And an important component of the Evaluation Environment is to assess the impact to privacy and identify if any adjustments need to be made. There's a -- the standards have a technical piece, and then they have a functional piece that's really just business process, and the practice of sharing itself.

And in addition to Suspicious Activity Reporting, we currently have efforts underway to identify whether standards are also needed to enhance sharing of alerts, warnings, and notification information, as well as watch listing information. And again, as with all ISE activities, assessing the impact to privacy is an integral part of all of these efforts.

So, that was just a quick snapshot of some activities that we thought you might be interested in and perhaps if you're interested in pursuing in any detail, we'd be happy to provide additional information.

I appreciate the opportunity to talk to you, I'm going to turn it over to Deborah Draxler, to talk more specifically about DHS. Thank you.

CHAIRMAN BEALES: All right, Deborah is the Branch Chief of Information Sharing and Collaboration in the Intelligence and Analysis Directorate. She leads the identification of information users needs, and facilitates information sharing, and coordinates information activities. She's been a defense contractor and an independent consultant teaching personal financial skills to soldiers in South Korea. She served for 13 years as an Air Defense Artillery Officer in Army. And, she received her Bachelor's degree from North Dakota State University and her M.B.A. from Gonzaga. Welcome, Ms. Draxler.

MS. DRAXLER: Thank you, good afternoon. I'd like to start by thanking you for inviting me to share the insights on how the Department of Homeland Security is addressing the information sharing challenge. I'd also like to thank our partners at the PMISE for their continued support. We closely align our efforts with Ms. Reingold and her staff. I'd also like to thank Mr. Ken Hunt for coordinating my participation here today.

I'm delighted to be here because I recognize the critical role that the Offices of Privacy and Civil Rights and Civil Liberties play in ensuring that information sharing and collaboration is successfully achieved. While we are a branch within the Office of Intelligence and Analysis, we are responsible for enabling the efficient and lawful sharing of information and providing structures for collaboration across the department. The Privacy Office and the Office of Civil Rights and Civil Liberties are at the forefront of many of these efforts.

We support the Undersecretary for Intelligence and Analysis in his role as a DHS Executive Agent for information sharing. Now, before I discuss the DHS information sharing strategy that the Secretary recently released, I first want to provide you with some of the context for our work and the foundation for developing the strategy.

As the Department was standing up, the primary focus was on creating the necessary organizational structures and processes to manage across 22 components. Missing from these initial efforts were the steps necessary to integrate the diverse organizational cultures that comprise DHS. This integration is necessary to leverage the Department's authority to achieve the information sharing missions of the -- of Homeland Security. It is this next phase of integration that I believe will significantly contribute to the success of the department.

So, you might ask how we are accomplishing this daunting task. Integration has two key components, information sharing and collaboration. The first component, information sharing, is about connecting people to information, while the second, collaboration, is about connecting people to people, in order to work more efficiently. Over the last 2 years, DHS has worked toward achieving the integration by establishing the Information Sharing Governance Board, the Information Sharing Coordinating Council, and now the Shared Mission Communities.

This governance structure for information sharing enables a more integrated DHS, by engaging all components at all levels of the organization. At the senior executive level, we support the operation of the Information Sharing Governance Board, or the ISGB. The ISGB is chaired by Undersecretary Charlie Allen, in his role as the Executive Agent for Information Sharing, a position designated by the Secretary. Under Mr. Allen's leadership, the ISGB convenes quarterly to address key information sharing issues and to provide direction to the department's information sharing efforts.

Also represented on the ISGB are the Director of the Office of Operations Coordination, the Assistant Secretary for Policy, the Chief Information Officer, the Assistant Secretary for Infrastructure Protection, the General Counsel, and the Executive Lead for the law enforcement shared mission community. The Chief Privacy Officer sits on the ISGB as an ex-officio member.

The ISGB is empowered by the Secretary to set information sharing policy for the department. Since April 2007, the ISGB has approved the DHS Information Sharing Strategy, the DHS Law Enforcement Sharing Strategy, and the DHS Shared Mission Community Framework Charter.

So before turning to the strategy and how it was created, I want to explain very quickly the term shared mission communities. The shared mission communities represent the critical cultural foundation for the governance structure. Representatives across the Department with shared missions, such as law enforcement, form the shared mission communities. These communities are the embodiment of the collaborative nature of our work and are the next level of integration.

Now, on April 18th, 2008, the ISGB approved the Shared Mission Community Framework Charter and we're quickly moving to establish the first of the three communities. There are currently six potential communities we’ve identified. The first three will be law enforcement, infrastructure protection, and intelligence. The policies, strategies, and resulting implementation plans that have been recently approved by the ISGB, were developed by the action officers of the ISCC and were presented to the ISGB for its coordination and approval, or excuse me, its consideration and approval.

The ISGC action officers also worked to implement the directives across the Department. The strategy is an excellent example of the work of the ISGB. Actions officers from the Office of Policy and the Office of Civil Rights and Civil Liberties led the effort, with participation from across the Department.

The DHS information sharing strategy is a significant milestone for the department. Putting together a strategy for 22 components is a challenge, and the strategy provides a vision for successfully implementing and enabling the DHS Information Sharing Environment through the DHS ISE. The strategy is formed -- informed by a number of guiding principals, of particular to this group is principal five, that States' DHS must maintain information and data security, and protect privacy and civil liberties. The strategy also recognizes that all applicable laws for privacy and civil liberties will guide and support the development of information sharing standards and procedures.

Creating a broad foundation for information sharing requires trust between all information sharing partners, applying the privacy and civil liberties standards helps build this trust by ensuring that information is being used appropriately.

The DHS strategy also aligns with the national strategy for information sharing, as it recognizes the need to protect information from unauthorized disclosure. We strike a careful yet critical balance between the homeland and ensuring that our citizen's rights are fully protected.

I would also like to call your attention to the three tenants of information security addressed by this strategy. First, DHS must develop robust information protection and data security protocols. Second, DHS must develop sufficient resources to train DHS personnel, and our information sharing partners, in appropriate security requirements, protocols, and practices, as well as privacy and civil liberty standards. And finally, DHS must adopt technology solutions that support information and data security, and commit sufficient resources to the electronic and physical protection of information media.

We look forward to the next steps of development, which will include an implementation plan. This plan will also be a departmental effort, developed by the action officers of the ISCC and through our shared mission communities.

Now in addition to the DHS information sharing strategy, my office is also leading key efforts in DHS support to the Information Sharing Environment. As discussed by Mr. Reingold, two of those key efforts are the controlled and classified information and Suspicious Activity Reports.

On controlled and classified information, my office continues to work very closely with the Office of Security, which has leadership for DHS implementation. We are also currently developing an enterprise approach to Suspicious Activity Reports, which is consistent with the ISCC SAR functional standard and the national SAR efforts.

At DHS, Information Sharing Coordination Council, SAR Integrated Project Team, was stood up in April and includes representatives from the Office of General Counsel, Office of Privacy, and Office of Civil Rights and Civil Liberties. This team is developing a DHS concept of operation for Suspicious Activity Reporting.

We are also working with the program manager for Information Sharing Environment and other federal entities, to ensure a SAR regime that comprehensively addresses privacy issues, and that all processes receive the appropriate privacy impact assessments and any subsequent systems of records notice.

Now, I've just touched very briefly on a few of the information sharing efforts that we are working on throughout DHS, and we recognize that there is much work to be done. This is my first visit to this Committee, and I hope that my presentation was useful. I appreciate the opportunity to share with you a portion of the DHS efforts to improve information sharing, and we look forward to working with you in the future.

Thank you.

CHAIRMAN BEALES: Thank you very much. Joe Alhadeff?

MR. ALHADEFF: Thank you.

I guess this is a question for both speakers, but I'm going to anchor the question off the national strategy itself. And, in looking at the two guidelines -- two of the guidelines in the national strategy, guideline one and five, there's a concept of maximizing the -- maximizing the acquisition access retention protection use, et cetera, of information.

And then guideline five, which is the privacy rights and other legal rights of Americans must be protected, which seems to create a certain tension, when one of the main tenants of privacy is data minimization.

So, maximizing access and minimizing data seem to be concepts in opposition, or at least that require some level of balancing. And I think when one looks at the core privacy principles, the question of how that balance occurs gets put into play. So, there's the concept of determining the nature of protected information, but the question is not is it just PII or not PII, but also is it PII with certain limitations as to how it can be used. And that becomes especially important as government starts to access private sector information, which has significantly more limitations on it than governmental information in many cases. Because promises made by businesses when they collected information, also have to be factored into this process.

And then, the part which -- if you -- you may not have been here this morning, so I'm harping on the same issue I started this morning. So, to those on the panel, you might be bored of me by now, but, so be it.

The concept of ensuring agencies disclose protected information to other entities, providing comparable protection, is an interesting concept, but I think there has been great focus and commendable focus among the agencies, of essentially getting the issue right within their remit. So, all of the agencies, I think, have done commendable and very hard work in making sure that they understand their information, and how to protect it, and what rights should be associated with it, and how to enforce those limitations.

But I don't see that there is a similar basis of work in what happens when information crosses organizations. Because they might not have those data fields, they might not have those limitation tags, there might be a very difficult challenge facing them at the systems level, of how to respect some of these conditions, or how to capture some of these conditions when the information comes in.

The other concern which is raised, is when information is transferred for a specific purpose, then it becomes part of the system. How do you make sure it's not used for any other purpose that was beyond the purpose of the original sharing? So, if I'm allowed to share this information with you because there is a terrorist issue related to it, how do I make sure it's also not used once it gets into a system of an agency that has application beyond those issues. Because that system is now sitting -- that information may now be sitting in their system. And maybe their system doesn't differentiate how it got there. And therefore, they don't know that they're not supposed to be using it at a later date, not because the policy told them not to, but because the system doesn't differentiate the information that way.

So again, it's not that an agency is necessarily intending to do the wrong thing with information, but at the system level, how do you help work the protections? And that may be something that is beyond the strategy and more at the agency implementation level, but I would assume the strategy has a coordinating role related to how that agency implementation gets done.

MS. REINGOLD: These are all, as you said, very difficult questions, and I'm not going to pretend that everything's all worked out. But, one of the reasons, particularly as you talk about information that, for one reason or another, needs to be protected in some way, and then tracked through the system, so that whatever controls were put on it appropriately, people recognize that. That's actually one of the very reasons for trying to simplify and standardize and have a rational approach through this CUI framework.

And, as I mentioned, there's a lot of work to be done, relative to the implementation, but a lot of the things you just described, is actually the intent of the whole CUI framework, so that there's a registry of all the markings, that's there's the ability -- I didn't go into all the details -- but to basically specify dissemination. And then there has to be discussion across all the agencies, all the participants and such, about exactly what you're talking about, how do the systems need to be -- everyone knows that their systems -- a lot of this is automated -- that they're going to need to be adjusted and such to make sure that the information is tracked, how it’s marked is tracked, and then it's handled appropriately?

So, there's a lot of work to be done, but the point is that there's a recognition that this does need to be done. There's also a recognition, and the reason that there needs to be private sector representation, there's acknowledgement, there are a lot of legal issues relative to private sector information, that they need to be part of this discussion.

So, as I said, you're right that the national strategy eludes to all of this, it basically says that these things need to be done, and then there are certain initiatives, like CUI, that lays a framework, and five years of work to make sure all this is put in place. But there's also a reliance on the individual departments and agencies, as you said, to implement within their own organization, as well.

So, I know that was kind of a general answer. I don't have specifics to each of your points, but absolutely – and just to your very first point, there is a natural tension here. That's just life and that's the way it is. And -- but the whole point is trying to work through this, simplify it, put processes in place that make sense to people, and again, try to utilize existing systems and make changes where necessary.

CHAIRMAN BEALES: John Sabo?

No, go ahead.

MS. DRAXLER: I just wanted to add that we don't have to go too far outside of the Department or even anywhere outside of the Department to run into all of the issues you just mentioned. We have a microcosm of all them within the Department, and unfortunately, or fortunately, however you look at it, to be able to address that on a daily basis.

We started with the development, or the policy that was propagated, the one day adjust policy, which said that if you are entering into an agreement for information outside of the Department or even internal, that you would be entering on behalf of the Department, which has caused some very interesting discussions throughout the components, as well as at the Information Sharing Governance Board.

So, as we've grappled with the implementation of that policy, we have been able to talk through some of those issues. Most of what we've discovered is it's just understanding what the data is, what you're doing with the data, why you're touching it, when you get that data, what are going to do with it, and getting a much better handle on what we as a department have.

We don't have a data library per se, that is robust enough to be able to immediately have the answers to all those questions, but we're working through the shared mission community concept. Through the law enforcement community, we're having numerous workshops and discussions on the data that that particular community has to offer.

And we stand up, our next community will be infrastructure protection. They're very eager to stand up and talk about, okay, so when you bring in the private sector information, into either in the law enforcement arena or into the intelligence arena, how do you handle that appropriately and how do you share so that we can get the data to the people that have -- have a need to see it, but to share it responsibly?

So, I don't know if I touched on your questions but that -- we have recognized all of those issues and we are working towards that.

MR. ALHADEFF: I think the one thing I would highlight is, the concern usually is again, not the concern of the intention to comply, because I think that's clear, manifest, and correct. But what happens is, the person who requests the information and the person who needs the information and uses it, and the person who technically manages it, are all different people. And, the problem is that they may not know the conditions that came with it, they may not know the conditions that it's subject to, and they're going to do the best they can to honor the policies they have, but it's very difficult to translate that unless you have an automated layer underneath that's also helping provide that information with the transfer.

MS. DRAXLER: And to start in that direction too, is just to have the data architects in the room with the operators, which we've been able to do with the law enforcement community, and we've seen a lot of light bulbs go off and say, "I didn't know that that's what you did with that data." So, it's been very useful in a lot -- in a lot of areas.

CHAIRMAN BEALES: Now, John Sabo.

MR. SABO: Really, it's a follow-up to Joe's question.

I mean, I work a lot in the information -- critical infrastructure protection community with DHS and track the ISE. And there was a lot of input into this on the private sector. As I said earlier, in the prior panel, there's a big gulf between operational processes and your broad policy statements and the CUI. There were two references today to privacy that are very important.

And I know, Ms. Draxler, you talked about the fact -- I wrote down -- the development of privacy standards. So my question is, what is the current plan to work with the private sector, with this body, with the DHS Privacy Office to develop these privacy standards?

And I presume that doesn't mean technical standards, but you're talking about business process standards for DHS and the private sector and the ISE. And it would get directly to the usage questions, redisclosure constraints, it would get to tagging of certain sensitive information that might be PII. When will see a DHS reach out to the private sector to begin developing those standards, so we can begin implementing the environment?

I mean, all of the great global talk is wonderful, but when are we going to see that start? Is it beginning and what is your game plan for implementing the business process and policy standards?

MS. DRAXLER: I share your frustrations with the time it takes to get this all set up. Like I said, we spent the last couple of years setting up a structure so we can bring these things to the table. We didn't have the capability to really talk about these types of things at an enterprise level. Strictly looking at the information sharing aspects of it, we have that now through the ISGB. The next shared mission community that's standing up is the infrastructure protection community, and naturally, IP is managing that community.

I -- they have great plans for us. We're still putting the charter together, which we should have complete in the next couple of weeks, and then you should shortly see some things that that community will be developing. We anxious to get to the implementation side as well.

MR. SABO: Just a quick follow-up to that, and we talked about service-oriented architecture before. I mean, there is a point where the underlying systems, whether you're dealing with law enforcement, the tribal community, State and local Fusion Centers, or the private sector, you’re going to be utilizing the same infrastructure to a great degree, and you're going to be segmenting information data, et cetera. So, one of the issues you have, is if you balk or not -- it is, it's great to have the input from the stakeholders who are going to be interacting with it because the needs may differ, but the infrastructure is the same.

So, I guess my only caution is, if you balk -- if you have one organization leading this piece, and not part of an integrated plan working with you and the Privacy Office, and maybe even the ISE, you're still not going to address these broader issues of an overall system, which I think Joe was alluding to, that you have data flowing in from all types of sources across all these communities and it's not properly tagged.

So, I guess I would just encourage you to look at a way to organize this and to get input from the stakeholders, but still do it in the context of an overall architecture.

MS. DRAXLER: And to address that, we also get engaged -- we have an information sharing segment of architecture that is reflected in the DHS enterprise architecture. It's in the fledgling stages. Again, we're trying to get this implemented as quickly as possible. So, we do have a close alignment throughout DHS, with the OCIO, as well as Privacy and CRCL, making sure that all of those things are addressed. So, it takes time, unfortunately, to get all the -- herd the cats, if you will -- but we’re getting there slowly.

CHAIRMAN BEALES: All right, Ms. Feingold, Ms. Draxler, thank you very much for being with us today. This has been -- this has been very helpful and we appreciate your time and we're sorry to make you wait.

Our last panel today will be Privacy Advocacy Perspectives on the Information Sharing Environment.

And our first speaker will be Jim Dempsey, who's Vice President for Public Policy at the Center for Democracy and Technology. Jim has been with CDT since 1997. He was the Executive Director from 2003 to 2005, when he moved to San Francisco and launched CDT West.

Jim coordinates the Digital Privacy and Security Working Group, which is a forum of over 50 computer and communication companies, trade associations, and public interest organizations. Before joining CDT, Jim was the Deputy Director of the Center for National Security Studies and Special Counsel to the National Security Archive. And from 1985 to 1995, Mr. Demspey was the Assistant Counsel of the House Judiciary Committee's Subcommittee on Civil and Constitutional Rights.

Jim, welcome, it's nice to see you again. And again, I'm sorry for keeping you waiting, but we knew it would be worth waiting for.

MR. DEMPSEY: Mr. Chairman, members of the Committee, thank you, and it's a pleasure to be here this afternoon. I'm accompanied today by Greg Nojeim from CDT, who is the Director of our Project on Freedom, Security, and Technology. And Greg is somebody that you should all look at to know, if you don't know him already, as a resource and an expert on these issues as well.

Now, in order to be able to try to say something useful to you this afternoon, and in order to address specifically the issue of privacy in the context here, the Information Sharing Environment, which is the issue that I was asked to focus on, I think it's important to -- in order to get privacy right -- we have to understand the operation, the function, the business model of the entity or the environment for which we're developing privacy rules.

I think we all -- all of you as experts in privacy, know quite well that one of the biggest mistakes that someone can make about privacy, is to treat it as something distinct from operations, and to think that you can have your privacy rules developed without a sense of what it is that you're developing them for. And instead, I think the most powerful vision of privacy and the most effective vision of privacy is the understanding of privacy that works together with operations. And it sees them not at odds with each other, although sometimes there are clearly trade-offs. There are going to be some no-go rules.

But really what we're talking about here, is the view of privacy reflected in the FIPPS, the Fair Information Practices Principles, which have to do, all of them, purpose limitation, use limitation, retention, accuracy, they all relate to what is it, the system that we're doing.

And I think one of the reasons why, or the major reason, in my view, why the privacy issue has not been solved, the reason why Chairman Feingold could not answer Mr. Alhadeff's question very well, because I'm not sure, but I am of the opinion that, there is not yet a coherent explanation of just what the Information Sharing Environment is, and how it is supposed to work. And I say this with huge respect for the amount of work that has gone into the development of the environment, of the work of the Program Manager and that office.

Clearly, some very huge complicated issues here, but still, I think, there is not a good understanding when you look at all this material. It's not just not clear, to me at least as an outsider, what Information Sharing Environment -- what the Information Sharing Environment is. And until you can get that understanding, I don't think you can specify the rules for it.

Now, I can start by saying what I believe information sharing is not. Information sharing is not, I don't think you're doing a good job, give me all of your information and I'll use it, and maybe I'll tell you what I find, and maybe I won't. That's not what information sharing is about, although that's -- clearly I have heard – what some federal agencies believe information sharing is. Information sharing is also not, "Here's this mass of information I have, I can't find any good value out of it, but the hint of the next terrorist attack may be in here, so I'm going to give it all to you, and then, if the attack occurs, you will get blamed for not connecting the dots just as well as I did. So, here, take it all." That's not information sharing, either.

Now, if you look at the definitions that have been forth by the program manager and by the White House and Congress, the one sentence definition is good. "The Information Sharing Environment is defined as the combination of policies, procedures, and technologies linking the resources, people, systems, databases, and information, of all federal Executive Branch agencies, to facilitate terrorism information sharing, access, and collaboration," and I stress the word collaboration.

And, if you look at elements of the implementation plan developed by the Program Manager, and issued in November of 2006, again, you see some good hints of what, at least, is the vision of information sharing, that it leverages ongoing systems. It is -- the ISE will not result, says the program manager, in the implementation plan for the ISE of November of 2006. The ISE will not result in the construction of one government-wide computer system.

And if you look at the legislation put forth by Congress, again, you see some of the key concepts, in terms of the vision. This is section 10-16 of the Intelligence Reform and

Terrorism Prevention Act. “The ISE provides the functional equivalent or support a decentralized, distributed, and coordinated environment.” And Congress, in fact, went back in 2007, and further amended section 10-16. It allows the full range of analytic and operational activities without the need to centralize information, permits analysts to collaborate both independently and in a group, known as collective and non-collective collaboration.

So you see here, this is vision that I see of the Information Sharing Environment, decentralized, distributed, and coordinated. But when you get to the plans that have been issued by the Administration so far, you don't get a lot more sense of how this is going to work, you don't get a sense of who gets what when, and how can they use it.

And in fact, some elements of the plan actually contradict these directives, I believe, from Congress, and contradict internally, the statements of the -- of the Program Manager. In the White House's strategic plan, national strategy, for information sharing of October 2007, under sharing information at the federal level, it says, “The National Counterterrorism Center, NCTC, serves as the central and shared knowledge bank on terrorism and terror groups.” The central and shared knowledge bank? Well, the Program Manager has just said the ISE will not result in the construction of one government-wide computer system. Congress has directed the -- supporting the full range of analytic and operational activities without the need to centralize information, and yet the President has designated the NCTC as the central and shared knowledge bank of counterterrorism information.

So, I -- you see right in the plans, this -- and it’s impossible. How could and why would we ever want the NCTC to be the central knowledge bank? Why would we ever want to take all the FBI's data, all the CIA's data, all the NSA's data, and all the State and local data, and dump it into the NCTC? How could they ever possibly manage that information?

So, I think that the -- despite all the good hard work that has been done, there is still no answer to who gets what when, and how can they use it.

Now, let me give you a couple of examples of some rules that I would propose, almost rules of thumb that begin to get at this. For example, here's one that I came up with. If you are the requesting agency, that is, you're asking somebody for information, and you are not planning to create a team or a partnership or otherwise include the disclosing agency in the use of the information, then you are presumptively not entitled to it.

That is, you should be denied information sharing if you're not going to work with the holder of the data. Because after all, one of the fundamental principles of privacy is that information, as it moves away from the source, gets harder to interpret, more likely to misinterpreted, and yet, if you're not -- as the requesting agency -- seeking information sharing and citing section 10-16 as your authority to get, and claiming to be entitled to this information, and you're not going to work with the person who collected it and knows most about it, and tell them, "This is how I used it," then that is not the collaborative vision that information sharing is about.

Secondly, sort of a rule of thumb -- and these are a little exaggerated, but they give you a sense of what has been lacking, so far, in my opinion, from the vision and implementation plan of the Information Sharing Environment.

Data sharing on a particularized basis is presumptively favored -- should be presumptively favored -- while data sharing in bulk should be presumptively disfavored. So, if you are asking, "I am trying to find out more about Khalid Sheikh Mohammed." You go to an agency and you say, "Do you have anything about Khalid Sheikh Mohammed?" And you go from agency to agency -- I think that's a legitimate understanding of the concept of information sharing, the information sharing shouldn't be, "I'm interested in Khalid Sheikh Mohammed, but I'm not going to tell you, instead just give me everything and I'll run it against what I'm looking for."

The third principle, and this goes into a bit, Mr. Alhadeff's question, again, a somewhat overstated rule, but there should be no tertiary use of data, which was, I think, the question you were asking. You've already got the secondary use, which was Agency One collecting it for one purpose, gives it to Agency Two for another purpose, and then it sits in the database of Agency Two, what could Agency Two do with it? And can they, then, go on and use it for a third purpose? And I would say the rule should be, as a presumption, at least, that Agency Two should go back to the creating agency and at least tell them, "We're planning to reuse your information."

Now the privacy rules that have been set up so far don't come close to providing any way of addressing these questions. We have the December 2006 guidelines, we have the September 2007 Implementation Guide, and then we have the February 2008 Key Issues Guide.

Now, let me take two examples of how, still, despite all of this effort, some -- in my mind -- some fundamental questions have not been answered.

In the Key Issues guidance, they talk about the fact that if you're trying to redress, you're often going to have a situation where an agency is relying upon information that they did not create, or generate. And so, an individual is complaining, "I was kept off of an airplane," and they complain to TSA, and it, of course, TSA got the information from the FBI, who may have gotten it from yet another agency.

So, TSA has to have a way to figure out how to disburse and get on the watch list in the first place, because TSA cannot begin to provide redress to this person, unless they can go back and trace that information.

And yet, nowhere in the guidelines, these privacy guidelines, has anybody said, When information is disseminated, it must contain an indicator of who it came from.

Instead, if you look at B-7 of the Key Issues guidance, To the extent feasible, and consistent with Agency legal authorities and mission requirements, agencies should consider developing or expanding their data to include information about the provider of the data. So, to the extent feasible, you should consider. It doesn't even say do it, to the extent feasible, it says, consider it to the extent feasible.

I don't know why someone hasn't just come forward and said, as a general rule -- recognizing that it's not going to be possible with all legacy systems -- information should be tethered, it should have its providence on it, so that when there's a mistake or a dispute, you can go back and find out where it came from. Nobody, apparently, has been willing to say that.

In fact, I think it was discussed, actually, and the question was raised, and it was decided not to do that, in some of the internal deliberative processes. And yet, I don't see how you can possibly have a redress system, I don't see how you can have a privacy system, without knowing where the data came from.

One other example. No where, really, in here is there any requirement for auditing the quality of data.

There's a lot of talk about auditing where data goes, although no one's been quite willing to say, “You've got to tag it with where it came from,” so audits for misuse, but how about audit for data quality?

Again, if you look at the guidance, the guidance talks about audit, and then simply refers one to Section 7 of the December 2006 Guidelines, and then the December 2006 Guidelines have a very generalized statement about “each agency shall implement adequate review and audit mechanisms.” Yet, no one has said, what is an adequate audit mechanism?

So, as I've said before, we have a set of guidelines that really don't give anybody any guidance. To say you should consider something, to say you should have review and audit mechanisms, and not tell people, even, what that is, I think, is not getting us there, yet.

Now, I will say that from the outside, I haven't come up with the -- I haven't drafted these guidelines, either. I wish I had. I would like to be able to get to that point, I'm happy to work with the Program Manager's Office, the privacy and civil liberties folks at the Department of Homeland Security, and those at the Office of the Director of National Intelligence, they have welcomed such input, I'm afraid as a matter of bandwidth, I haven't given it to them, so I accept my part of the blame for the lack of specificity here.

But, I just think if you look at all of this stuff that has been produced so far, you're not a lot better off than you were beforehand, in terms of what actually the system is, and what actually are the rules for sharing information, and who gets it when, and how they can use it.

CHAIRMAN BEALES: Thank you, Jim.

Our last member of this panel is Meredith Fuchs, who's the General Counsel of the National Security Archive. She was previously a partner at Wiley, Rein & Fielding where she was a member of the Litigation, Insurance, Privacy and E-Commerce practice groups.

She served as law clerk to the Honorable Patricia Wald on the Court of Appeals for the D.C. Circuit, and to the Honorable Paul Friedman in the District Court for D.C., and she was a former Supreme Court Assistant's Project Fellow with Public Citizen Litigation Group.

She graduated cum laude from New York University School of Law, and was a member of the Journal of International Law and Politics.

Welcome, we look forward to hearing from you.

MS. FUCHS: Thank you.

I should explain what the National Security Archive is, first. It's a non-governmental research institute at George Washington University and we rely on declassified government records for publications on a range of national security issues.

I'm here, I think, to introduce another tension into the ones that were discussed in the prior panel, which as I understand were the maximization of access to information by those within the Information Sharing Environments, and the minimization of collecting and using personally identifiable information.

The tension I want to add in is the public's right to know. And I think I was invited here today to talk about the new Controlled Unclassified Information Framework, which you heard about in the prior panel.

I testified in Congress this morning about a bill that would impact the implementation of that framework at DHS, and I'm going to summarize the Open Government Community's concerns about the framework. And you've had, I gather, a long day with lots of acronyms, so I'm going to tell you the three that I'm going to use, and I will define them, and then I promise to try not to use any additional ones.

The first one is SBU, Sensitive But Unclassified Information, and SBU is the description given to all sorts of labels, over a hundred labels that government agencies have slapped on records, in order to control who gets to see them, and how they're handled. SBU is considered bad now.

The second one is CUI, Controlled Unclassified Information, that's what I'm going to talk about, and that's the new system that's been laid out by the President in a memorandum issued May 9th.

And the third is FOIA, which is the Freedom of Information Act.

I come from the perspective of, open government is more likely to make a good government. History teaches us that the government bureaucracy will make information secret for any number of reasons, whether it is to protect power, to control public opinion, or simply for administrative convenience.

And, of course, when we perceive that we're in danger, the natural reflex is to make even more information secret.

As I'm sure you know, the 9/11 Commission found – one of its principal findings Was that prior to September 11th attacks on our nation, the government's intelligence and law enforcement communities too often controlled information to the detriment of effective security.

The SBU problem is an example of that, because SBU problem made it impossible for them to share. That, of course, was compounded by the fact that agencies have a traditional of trying to protect their power and protect their turf, and so there wasn't a sort of trusted way of sharing information.

Well, in reaction to those attacks, as I just mentioned, there was a proliferation of these SBU titles for documents, and my organization actually did a study 2 years ago, which was government-wide, that looked at how these policies conflict with each other, and interfere with information sharing. They also, of course, interfere with public disclosure, because they gave the appearance that documents should be protected, regardless of whether they needed to be protected.

All of that led to the President issuing the CUI framework that was discussed in the prior panel. And the CUI framework is sort of a broad description of a program that will allow sharing of information between Federal, State and local, tribal authorities and private entities.

I will mention that that description of who is going to be part of this CUI framework omits the public. Because private sector entities do not necessarily mean members of the public. And that's a troubling omission, because the public has, you know, a strong interest in the protection against terrorism. Not only does the public care about preventing attacks, but they need information to protect their families, when the first preventers, and first responders are unavailable.

I mean, if you think about the crime reports that most of us receive in our communities, those give us the information we need to take measures to protect ourselves, if we know our community is being targeted. Whether it's the sudden increase in cars being stolen, or homes being broken into.

So, in other words, sometimes information should be made available to the public, regardless of whether it's sensitive, because it's needed.

So, turning back to the framework, there's some very positive aspects of the framework, and it was undoubtedly necessary. It's going to reduce these over hundred different record control labels, to three primary labels. The procedures for handling the materials marked with these labels will be much more straightforward, it's going to enable better protection of information that needs to be protected, and it will be easier for the public to understand what the label means. So, those are the positives.

The negatives, however -- I have two major negatives here that I want to just highlight here for you – is that any kind of control on information can be dangerous if it is not carefully watched. The CUI framework perpetuates and extends the system of information control that's been abused in the past, and we know that it's left us vulnerable to harm, in the past.

As Ms. Reingold mentioned, the purpose of the framework is standardization. What it is not, and what is missing, I think, is reduction of secrecy. While the establishment of the trusted pathways that the CUI framework creates is obviously essential to coordination amongst the Federal, State and local, and tribal authorities, and the private parties, those pathways are just as susceptible to manipulation and failure as the individual agencies that jealously guard their secrets.

True information sharing is best accomplished by the elimination of unnecessary secrecy, and the minimization of such controls. It also leads to better protection of information that should be protected, which I know is of concern to the privacy community.

The CUI program, obviously, is vulnerable to these same kinds of unnecessary secrecy that we've seen elsewhere in the classification area. And one reason it's vulnerable is because it's not -- what is CUI is not actually defined in the President's memorandum. CUI is anything that is pertinent to U.S. national interests, or important interests, and requires protection.

That's obviously a very expandable concept, and each agency is going to have to substantively define it for themselves. We hope that DHS will have a transparent process for defining what CUI will be within the Department of Homeland Security, because that would make it more likely that, if public comment is available, it would make it more likely that they will narrowly tailor the protection to information that needs to be protected.

There are some touchstones in the President's memorandum to support measures to reduce unnecessary control labeling, however, the memo itself does not include any provisions that directly counteract the natural incentive to insert a control marking on materials.

My second major concern with the CUI framework is that it is going to have an impact on FOIA decision making – that was my third acronym. The Freedom of Information Act is the one mechanism that the public has to ask its government for information and documents about what the government has done, and about decision making, it is a critical part of our democracy.

The President's memorandum permits a CUI label to be considered, but not determinant in a FOIA disclosure determination. I can get into details, if you're interested, of why that is inconsistent with FOIA, but for the time being, I want to just mention it as a major concern of the Open Government Community.

I mentioned that this morning I had testified in Congress about CUI and its implementation at the Department of Homeland Security. Obviously, CUI has just been introduced by the President, Congresswoman Harman has introduced a bill that would impose additional standards on the Department of Homeland Security that would control, for some of these issues that I've mentioned. We are hopeful that many of the provisions of that bill will actually be adopted government-wide, and that it will indeed be adopted by the National Archives and Records Administration, as it issues implementing regulations for the CUI program.

And with that, I'll close, and I'd be happy to answer any questions.

CHAIRMAN BEALES: Thank you very much.

Joe Alhadeff?

MR. ALHADEFF: Thank you.

And I guess I want to address my questions, and I'll be formal, also, I'll say Mr. Dempsey, on a number of the issues, because I think you correctly characterized some of the concerns I raised, but I also think we have to correctly characterize the environment in which this is happening, and I think your last comments about, you know, the guidance -- it's very difficult to come up with, is telling, and I think it's some of the reason that we don't see it yet.

I also think because some of the technology is only now becoming ripe to enable it. So, for instance, the concept of sticky policies that can be developed using technologies like CARMEL, are just developing now where you can actually pass condition statements along with information, and that might be a methodology of tracking or creating the providence of information that you were looking for.

I also think we have to have a recognition that, things like the NCTC example, if they hold in perpetuity or for long periods of time the information that they require for analysis, that becomes a problem. But, you need someone in this group of organizations to also be a source of truth, which is based on the ability to look across information, and not just assemble information on an as- needed basis.

So there is probably a need to have a repository for a point in time in order to do analysis to become that point in truth, it becomes problematic when that repository is a repository in perpetuity, as opposed to the repository of the analytical result. Because the analytical result is important, otherwise, we're all working with much less- than-perfect information.

So, those are issues that -- and that brings us to the concept of -- when is it appropriate to have data sharing where the sharing is actually an access for a purpose, rather than data sharing where I give you the data? Because both of them are sharing, but the concepts are different. And you might be able to accomplish a lot with the access but not retention, because I process against this data, I reach a conclusion, and what I maintain is the conclusion.

What you see in a lot of the identity management frameworks is the use of information, but a separation of duties related to the information, to further ensure its security and appropriate usage over time, and that helps address some of the tertiary use situations.

The other thing I think which is almost -- which is more unique to the government than it is, perhaps, to the private sector information, is the variety of levels of security associated with information, and people who wish to access the information. And therefore, that might go to the concept of also -- why the concept of the tether of the information isn't always obvious, because in some cases I can't even tell you I have the information, but the information was provided to help resolve a problem.

So, the tether, you know, the question of whether there should be a tendency towards providing the tether, but I think we have to face the realistic conditions within government, where the tether, in many cases, may not be available. And that may run counter to an open government view, but that is the probably, reality that we're operating in at the moment.

And it's interesting, because I think it was Mr. Sullivan, earlier on today, in his testimony that kind of discussed there were some people who would prefer to provide more information to get themselves off a list, because for them that was better than the privacy constraint of not providing the information, and we're always torn between those -- well, there's a beneficial use for using this more information, but there's also a potential detriment inherent in that. And it's -- depending on what end of the result you're sitting on, it's a better or a worse idea.

So, I think those are things we have to keep in mind, and I would say the thing which we all have to keep in mind as we look at these issues is the need to have flexibility in approaching them, and not assuming that we've figured out the best way to do anything, yet. Because I think what technology has demonstrated to us is that none of us have figured out the best way, we've all figured out ways in which it can be done, and there are probably better ways in which it can be done, all around.

And I think the more we get a rich variety of opinion -- so the more your bandwidth opens up and you have an opportunity to provide comment, I think the more useful it is for all of us, because we actually see different ways of doing things, and I think we learn from that collaboration. And where there's a possibility to perhaps open things up a little more, then, I think, that's better. Just like, where there's a possibility that we found out data's not useful, then let's not collect it, because that's another thing that gets in the way.

So, issues that we, maybe, should be taking on board.

MR. DEMPSEY: I think those are excellent comments. You know, in referencing my point about tethering, you said there ought to be a tendency toward it. And I agree with that, I don't even see that level of impetus towards any one of these things.

We're never going to have a perfect solution to any of these problems, and any strategy, any rule, any plan, only has to be good enough to get you down the road, to the point when then you know enough to revise it, but right now, we're not even giving people, I think, enough guidance to head in a -- to tend in a certain direction.

Now, on NCTC, I agree with you entirely on the analytic role of the NCTC. So in that sense, as an all- source Fusion Center, as an analytic center, I agree with the notion that the NCTC should have the access to all information, from all agencies, and to some extent, to be the source of -- what the White House strategy calls -- comprehensive, Federally-coordinated analytic products. So, sort of as close to the truth as we get on any given issue.

However, where I think the NCTC departs from the Information Sharing Environment vision, is in the notion -- also reflected in the President's plan and White House strategy -- that authorized agencies may request information from NCTC, and that NCTC serves as this knowledge bank from which all other agencies get their information. And I just think that's impossible, and I think that the vision of the Information Sharing Environment is, yes, you have an upwards flow ultimately to the product that's presented to the President every morning, but also, and what has been missing so far, is the downward flow.

Because there are analysts all across the Federal government, and at some level, you know -- when Ahmed Rassam crossing the border on December 31st, 1999, heading towards Los Angeles airport to set off explosives, and a Custom's officer stopped him, he was acting as an analyst in a way. He was saying, “What's going on? I'm going to put two and two together, I'm going to pursue it.” When that FBI agent sent that memo, the Phoenix memo, he said, “I've got an idea here.” It went all the way up to headquarters, and headquarters said, “All flight schools, al Qaeda, we just don't have the time for that.”

Today, if that same issue went all the way up to the NCTC, it's very likely that the NCTC would say, “Well, we don't have time for that.” Whereas, the purpose of the Information Sharing Environment, is to empower that FBI agent in Phoenix to say, “Okay, fine, I understand you guys up at the top don't have time for this, I'm going to spend a little more time on this myself. And I'm going to find information. And then I may -- instead of having a one paragraph memo, I may have a two page memo. Then I'll send it up, maybe.”

But, you can not expect, no matter how many contractors you put into that building out there at the NCTC, you can not analyze all of the issues, answer all the questions that are occurring at the operational level. And that's where I see -- and those people are hungry at that operational level for that information -- and that's where I see a deficiency in the plan. And that's where I see a lack of guidance in the guidelines.

CHAIRMAN BEALES: Lance?

MR. HOFFMAN: Jim, your comment sticks with me. These guidelines do not guide anyone, I think you said, or something like that. And this is something that's been frustrating me, and I think some of my colleagues here also, in terms of how do we develop guidelines or procedures or something -- how does really, DHS develop procedures that can be used to effectively guide programs at the beginning, so they end up being useful, and to -- and to not have programs get ahead of steam, go forward -- and we've seen, I would say some fairly recently that, you know, they've had mission creep and they do something else now, but, you know, nobody will turn them off. They just go.

And I'm wondering whether -- I know CDT in the past at least, has had conversations with organizations, commercial organizations, non-commercial organizations that have to -- I don't want to reinvent the wheel -- that had to have had similar problems, and some bureaucracies. Do you see any differences in, maybe, successful things that CDT has done in the past, or other organizations have done in the past, versus what we're doing now procedurally? Because I think a lot of what you're talking about is tied with procedures and development of programs.

MR. DEMPSEY: The order of magnitude and complexity, is clearly much greater here -- I think it's fair to say -- than with any other information system, anything that any companies you're familiar with have grappled with. So, you know, recognize that.

The main point I'm trying to make is if, you know, if you look at the Program Manager's implementation plan, in terms of status of recommendations submitted to the President, in accordance with the Presidential requirements. Guideline 5, protect the privacy rights and other legal rights of Americans under recommendation status, that's marked completed. It's not close to completed.

Now, at some level that's less of a criticism -- or more of a criticism than it suggests. It will never be completed, but we need to forward incrementally. And what I'm trying to propose is, take -- again, going back to data quality. If you look at the, again, the February 2008 guidance. So now, we're pretty far down the road in the implementation of the Information Sharing Environment, and you go to data quality, it really -- the text of the guidance largely repeats what was issued in December of 2006.

And if you look at the, sort of, resources, there's two pages worth of policy guidance and standards. You know, someone once said, “The great thing about standards is there are so many of them.” And this is an example of that. Somebody ought to pick just one of these and say, “Follow this.” It's not going to be -- and recognizing it's not going to be the -- chances are, it won't be the best one and it won't be perfect. But, saying pick one of them that's imperfect, is far better than saying, “Here's, probably 20 of them here, consider them.” And currently, the guidelines say, Consider these. And that's just on the question of data quality and auditing, for data quality, as well as auditing for misuse.

And so, I think that, you know -- again, I had, at various times over the past two or three years, had thought I was clearing the decks for really drilling down on this issue, and this FISA thing keeps going on forever and ever and ever. And, if -- well, if we ever had a President who said he would follow the laws enacted by Congress, and if people were ever willing to accept responsibility for not following the laws, we might have resolved it. But, that's sort of neither here nor there for this group, I guess.

But, I just haven't -- so, for see -- I would love to see CDT or somebody else, sort of chair that process. There is an inter-agency issue here, which is, I think, you know, nobody has been willing to say to another agency, “Do it this way and make it stick.” Now, I thought that's why we created the DNI. I know that's why, obviously that's why we created the DNI, but we still don't have, “Do it this way or you lose your funding.”

CHAIRMAN BEALES: Jim Harper?

MR. HARPER: Thanks to both of you for being here and contributing your thoughts, very helpful.

I actually just wanted to sort of briefly echo what you opened with, Jim, in terms of the program in general. And not just echo with my own opinion, but I want to point out that, obviously, in our framework document, sort of, the first -- the first question we ask when we look at a program, is what is the benefit, what are we getting, what security comes from this thing. And I think that's a major weakness or perhaps failing of the Information Sharing Environment, is that no one has ever articulated what we get from it.

Good folks -- good folks at the DNI have called me up on the phone, and I've taken the opportunity to quiz them about how it works and what we get from it, and I've never really gotten a very good answer, though they've tried to sell me on good privacy protections. Well, if we're not getting anything for it, there's really no -- no loss of privacy is worth it, but I don't think my opinion is necessarily the most important. I mean, there are others out there, and I just finished reading a book called "Crush the Cell" by a guy named Michael Sheehan, who's no slouch when it comes to counterterrorism, and he's no civil libertarian. And writing about the NCTC and the DNI, he said these were a classic Washington solution to a problem, create a new agency, hire more bureaucrats, and increasing the outsourced work to contractors.

The cost of these new organizations is absolutely staggering, but I've yet to see how they've appreciably helped the so-called War on Terror. That's question one, that's the starting point for determining what we might give up in terms of privacy, what practices we might undertake to minimize privacy loss to get that benefit. But that benefit isn't there.

I get hung on question one and kind of stop there, and maybe that's a mental defect. Others have the ability to hold their noses and say, "Okay, probably shouldn't happen, but if you're going to do it, here are the steps you should take." And I think -- so, I think both of your recommendations are welcome and appreciated. But I think it's -- it's important to me to reinforce the fact that we don't have yet an articulation of why these things should be there at all.

MR. DEMPSEY: I would disagree with you on that. As you know, I was a member of the Markel Task Force on National Security in the information age, and endorsed the recommendations -- helped develop and endorsed the recommendations of that task force, which did recommend the creation of something like the Information Sharing Environment, at least as I described the vision of it, as a decentralized, a collaborative environment for sharing information across agencies and empowering people at the lower levels of agencies.

I believe that the value of that is intuitive obvious. I don't think we've realized that value yet, I would say that. I think the goal is a goal that continues to be worth pursuing. So, I -- I think the payoff at the end of the day hasn't been documented. I think the objective, to me, is an intuitively meritorious objective.

MR. HARPER: I can take as intuitive an information sharing attitude, but for all the money, all the everything else moving around, I think we need better than intuitive. Someone needs to say how this works and why it works.

MS. FUCHS: If I could just add, I mean, I would agree that to some extent with -- I think it's like the undercurrent of what you're saying. I mean, one of the major concerns of my community, is that the Information Sharing Environment is just sort of a bigger group of elite who get to get the inside information, not necessarily making a difference.

And that's really part of the reason why we think that the secrecy needs to be reduced as much as possible, and the public, the real public needs to be as engaged as possible. You know, not so directly, focused on the privacy issue, but I think that, as it appears now, the Information Sharing Environment has not really addressed how the public can be part of that. And that's -- that's essentially where we're coming from.

CHAIRMAN BEALES: All right, I want to thank you both for being with us. It's been -- it's been most helpful and most informative. Do we have anyone who's signed up for public comments?

MR. HUNT: I'm not aware of that.

CHAIRMAN BEALES: Would anyone like to sign up for public comments?

[No response.]

CHAIRMAN BEALES: If not, I guess that brings us to the close of our day. And, thank you all for being here, and we look forward to seeing you again in three months.