The Privacy Office
Department of Homeland Security
Privacy Office Workshop Series
Operationalizing Privacy: Compliance Frameworks & Privacy Impact Assessments
June 15, 2006

OFFICIAL WORKSHOP TRANSCRIPT

GSA Regional Headquarters
Auditorium
7th & D Street, SW
Washington, DC 20024

TRAINING SESSION

Speakers:

Rebecca J. Richards
Nathan Coleman

MS. RICHARDS: Good morning, everyone, or afternoon. If you haven't already gotten it, you should make sure you have a hypothetical. That's the one piece of paper that was handed out at the beginning, as you were coming in.

My name is Becky Richards. I'm the Director of Privacy Compliance in the DHS Office. I and Nathan Coleman, our PIA Coordinator, will be conducting the tutorial today. We're pleased to see so many of you here today and, as was mentioned this morning -- as was mentioned this morning, we will be doing a repeat of this tutorial on July 10th -- 12th, excuse me. It's a Wednesday. Additional details will be up on our website next week.

We're here today to talk about how we ensure privacy is incorporated into the fabric of DHS, our programs and our information systems. In order to promote public trust and transparency in DHS and our programs, we must protect the personal information that we are collecting, maintaining, and using. Personal information is not only my name, my social security number, but it's also information that directly or indirectly identifies me.

We'll go into a lot more detail today about how that is as we move forward. The PIA process, though, is the means by which we begin to build privacy into the fabric of our DHS programs. Really, as we heard this morning, we want to build privacy into the culture of DHS and the PIA is one of the mechanisms by which we do that.

So all of you are probably looking at the schedule saying: Oh my, how long is she going to be speaking? I want to give you a sense of the structure of this afternoon. Nathan and I are going to switch back and forth going through the different slides. If you have questions throughout at any time, please put them on the card, pass them to the middle. Kathleen, Billy, and others will be walking up and down. At the end of our first session today we will try and take about ten minutes worth of those questions to go through and answer those. But again just be writing them down as you go along if you have questions.

If for whatever reason from a time perspective we don't get to them, we're here to answer your questions after the session. Also, call us. We're here to help.

You should have also received the hypothetical that I mentioned. This is a worksheet and you should have this (indicating) as well as your PIA guidance. These are the two tools that you need for us to go through this tutorial today. You're going to probably want to write down any notes on this. That's the reason we didn't give you the PowerPoint, because this is really the bible for how you're going to conduct and write your PIA. So you want to have both of those out.

We're going to follow pretty much what's in the PIA guidance.

So as I mentioned, we have quite a bit of material today. My goal, our goal in the Privacy Office, is for you to be able to leave here today and have a clear understanding of what is the different type of privacy documentations that we have here at DHS, understand when a PIA is required, and then be able to go back and fill out the PIA

template, be able to go back and write down at your desk when you're starting to create a program and do a very good first draft of that PIA. If we have done that by the end of today, then we've sort of succeeded in our goals.

So there are three types of privacy documentation. There's the updated privacy threshold analysis. We will be issuing an updated version in the next week or so and I'll talk a little bit more about that. There is the privacy impact assessment, which is basically the topic of much of today. And then there are System of Records Notice. We're going to go through each of these in a little more detail.

The privacy threshold analysis, otherwise known as the PTA, is the first document you should really think about when you're thinking about your system. If you're making updates to any of your existing legacy systems, this is where you start. It will tell you whether or not you need to do a privacy impact assessment.

You may have already come across this document and you would have come to it in the certification and accreditation process and the trusted agent FISMA program. As Bob West mentioned this morning, they have what's known as TA-FISMA and that's where they're collecting all your artifacts. The privacy threshold analysis was introduced through that process.

The updated PTA will be forthcoming, but basically what the process -- what it does is it tells us whether or not you need to do a full privacy impact assessment. But it also demonstrates to different folks, whether it's the IG, GAO, OMB, that as you were developing your system you thought about privacy and if you don't need to do a PTA then you've already documented it in a formal way in which the Privacy Office has also reviewed it and said yes, you're good to go.

So as I mentioned, we're rolling out an updated PTA based on our experience over the last six months and from feedback from different people like yourselves, whether you're system program managers, information security system managers, telling us sort of what they need in there and what they don't need in there.

If you have already conducted and completed a PTA that was approved by the Privacy Office, you don't need to worry about the updated form until you go through C and A again in three years or whenever your ATO comes up. If on the other hand you're one of those programs that has an Excel spreadsheet that has a few boxes or some other

form that is not the approved PTA by the Privacy Office, you need to make sure you get the updated form and you fill this out. This will begin to affect your C and A process, so you want to start thinking about those documents and you want to start working and making sure you have the right ones.

If you did this prior to February 2006, then you need to make sure you have the right documentation.

At this point I'm going to turn over to Nathan Coleman, who's going to talk a little bit more about what exactly the PIA is.

MR. COLEMAN: Can everybody hear me? Good.

Becky just gave a brief overview of the PTA, but this document (indicating) is essentially probably the reason you're here. This is the second major privacy documentation that the Department uses. This is the method by which the Department ensures that privacy's been embedded in every single system, program, and the practices of DHS.

Now, what we do -- like Assistant system Hawley speaking this morning said, it's important to embed privacy into not only the final result of the system, but also the beginning and the development of the system. What the PIA does is ensures that you're outlining the elements of the privacy concern, what are you collecting, what are you collecting it from, what security measures do you have in place, information-sharing, and things like that.

If you thumb through your guidance you can see all the various sections, and I'm sure some of you are already familiar. Additionally -- and I believe Eva Kleederman mentioned -- what's important about the privacy impact assessment is that at the end of each section there is an impact analysis section, which is a critical analysis of the section and the questions that preceded it. So we'll get to this in more detail in the second half of the presentation.

But for example, section one talks about the who, what, and why of your collection. The impact analysis for section one wants you to critically address the scope of your collection and things like that. So this is the ultimate document which we are looking for as far as an assessment.

A common question we get about a PIA is who should be writing it, who should be responsible for it. Our general answer is the program manager is ultimately going to be responsible for the documentation. Now, the program manager's name may be on the front as the responsible official. However, that program manager is going to have to lean on his counsel, his security folks, and other folks knowledgeable about the system that can give the detailed answers that the PIA actually requires.

So although the program manager's name may be on the front of it and he or she may be accountable for that document, the whole team is essentially accountable and ultimately the Department is accountable for that document. So what gets said in there needs to be accurate and forthright about what the system is actually doing.

Additionally, in addition to just the program manager and the security officials and things like that, you also want to make sure that you're working with your component's designated privacy official. Now, some components have an actual privacy officer. Sometimes that's done through the CIO's office, sometimes that's done through counsel's office. But it's imperative upon the program manager to make sure that that official is looped in.

As far as getting the PIA approved, Becky will speak at length about this later on, but basically when you design the system you say, okay, this is what we want to do, this is going to help the Department and its mission. That's the time you want to start thinking about doing a privacy impact assessment, because not only does this address privacy issues, but it really helps the system design process and the development life cycle, because these are -- contained in the PIA are questions that you should already be asking yourself about your system.

So when you reach this early in the design process, you may not know all the answers to that, but that's okay because ultimately by the time you get to going live or before launching your pilot, you will have solid answers to all these.

Which brings me to, when should I have my PIA completed versus when should I start the PIA. We like to say they should be done early and often, so you have several iterations leading up to the final point where you have a completed final document. As mentioned earlier on some of the panels, if the PIA is not done by going live the system does not go live. Even before that, if you're doing a pilot test, whether you're using

dummy data or masking data or anything like that, the PIA has to be done even before that, because the issue becomes if you are not addressing the privacy issues before going into the pilot, by the time the system goes live the privacy concerns will be too late or they could be debilitating to your system. No one wants to have the funding stopped or anything like that.

So it's important that a PIA is done regularly through the process and ultimately leading up to the final presentation of the document.

The second -- the last major privacy document was mentioned a lot this morning as well, the system of records notice. The system of records notice is triggered by the Privacy Act of 1974, which was also mentioned a lot. The key difference between the system of records notice, which actually serves as a basic notice, and the PIA is the PIA is an actual full analysis, whereas -- and the PIA is triggered by the collection. It's easier to -- it's easier to trigger the PIA than it is to trigger the system of records notice.

The system of records notice is triggered by the retrievability of the collection, as in are you retrieving information by personal identifier. Now, this is something that you will have to bring in your counsel on because this is something that requires legal analysis and legal conclusions. Feel free to call our office. Liz Withnell and Erica Perel are our counsels in the Privacy Office, as well as who you know your counsel to be on your component or even for your program.

But the General Counsel's Office should be involved in the system of records notice determination.

And that's it, hand it off to Becky.

MS. RICHARDS: So how do all these documents relate? There's a lot of different documents. Do you have a one to one relationship? What do you do? How do they work? We've actually spent a lot of time trying to think through, is there a one to one relationship and when are these different documents going to come into play.

So we have built sort of a picture, because pictures can be helpful. Here we start with a system. The system is the IT system that Bob West was talking about this morning. It's the nuts, the bolts, the pieces, the wires, everything. That's the little system.

Every system needs to have a C and A under FISMA. So it needs to be certified and accredited if it's an IT system under FISMA.

Okay, what happens next? Every C and A needs to have a privacy threshold analysis. This document is a very short questionnaire. It's meant to trigger whether or not you have to do the full PIA, which will take more time. So the PTA is really meant as a sort of trigger one. It asks you, give us a description of your system, are you collecting personal information, are you collecting information about individuals?

Based on that information, our office will determine whether you need to do the full PIA. So in this instance, for example, a LAN, a WAN, any of those types of things that are just sort of the wires back and forth, they need to go through a CNA process, they need the PTA. The PTA says, hi, thank you, you have finished your privacy documentation, you have no personal information.

The next step would be if you have a system that is collecting personal information. So in that case the PTA would determine and say, yes, you need to do a full PIA. From our perspective, we expect once you've had a determination that you need to do a PIA, that that PIA should be completed and approved by the chief privacy officer within six months.

So the PIA will be much more fulsome. It goes through the process of what information you're collecting and so on and so forth. Now, there are going to be some systems that require a PTA and a PIA, but they don't require the system of records notice. An example of that would be, for example, a system that has visitor badging. So you give -- a person gives their information and says, I'm going to be at the GSA building, here's my name and here's the time I was there. We've collected personally identifiable information, but the system of records notice only comes in if we're going to retrieve that information back out by the fact that Becky Richards was here on XY date, as opposed to many of the visitor log-in systems are only retrieving it by the day. But the PIA would help us determine that process and would determine whether or not the system of records notice is needed.

Now, you'll find that there are systems that have a one to one to one relationship. So you have a system, it's gone through the PTA process, a full PIA was done, and it determined that a system of records notice was needed. In these cases, as Nathan was

noting, you have to have your PIA and your system of records notice completed prior to you turning on your system.

So this might be any number of different systems where you're collecting the information and you have your system of records notice, you're retrieving the information by personal identifier.

Now, there are other ones, because of course it's not cut and dried. The PIA is not a one to one relationship between the system. There are lots of systems that do lots of different things. So what you may have is a system, the C and A is done for that, the PTA, but one PIA is going to cover that and there's one system of records notice.

U.S. VISIT is sort of an example of that. They have a PIA, it covers their entire program, and then they have a number of systems that have been C and A'ed underneath it. Again, that's where the PTA -- you in collaboration with our office will help determine what makes the most sense. We're not here to try and make people do PIAs just to do PIAs. We want them to be a meaningful document that actually provides privacy protection.

Another example is going to be a system of records notice with two PIAs. Now, an example here would be for example TSA-002. This is the system of records notice for threat assessment. Threat assessment is an umbrella. So imagine that the system of records is somewhat general. It's an umbrella that provides what I is being collected generally and how we're generally using it. The PIA helps get you more discretely.

So in this case TSA-002, threat assessment system of records notice, has right now three or four different privacy impact assessments that have been published on the website. Those would include things like the TWIC program, Transportation Worker Identification Credentialing, the port worker screening, Registered Traveler.

All of these programs are doing threat assessment, collecting basically the same information. But each of them is a discrete project, a discrete program, and so needs a PIA. Now, the interesting part of that is that for the most part those systems then have an underlying system that handles much of the information in the same way, so end up having one C and A and one PTA.

There are a number of different iterations you can imagine basically, but what you want to take away from this is that you want to make sure that all of our C and A'ed systems have the PTA and that you are clear whether the PIA is going to be required or not.

I really apologize for all of the acronyms at this point.

That gives you sort of the high-level idea of how these work together.

VOICE: (inaudible).

MS. RICHARDS: Can you write it down, please?

Now, a slightly different variation on this theme is going to be where you have a system of records notice and you don't have a PIA yet completed. People are going to say -- because I regularly will say, if you have a system of records notice you need to have a PIA. But there are some cases again where the system of records notice is your umbrella. So right now we have a system of records notice that is for training programs, but we don't have a PIA yet because we're still developing those training programs. So we're in the midst of writing those PIAs as we speak, but right now you have a system of records notice. There are just different timing things with that as well. But generally, if you have a system of records notice you're going to have a PIA as well.

Now, one of the discussions that was earlier this morning we heard from Bob West and Eva and Barbra, was talking about where's the connection that exists between the security and the privacy. Again, we're working on this and it's still very much a work in progress. But the new PTA will be collecting information from you about what is the FIPS-199 categorization for the information that you're collecting. So how have you dealt with confidentiality, integrity, and availability. These are words that don't mean a whole lot at this point. You want to talk to your security officials because they will mean a lot to them.

What that will help us do is connect and make sure that the way you have categorized the system from a security perspective matches the risks that we have identified and mitigated from a privacy perspective. The two of them are very much coexistent. If you haven't appropriately secured the information, then you are going to

have data security breaches like we've heard about from the VA, you're going to have some of these different problems.

On the other hand, if you don't know what information you've collected, you don't know what you've collected and where it is and you don't know what the information flows are, so from a privacy perspective you're not sure what you're doing, then from a security perspective you're not going to know how best to secure it from a most efficient and effective manner.

You don't necessarily -- if all you've collected perhaps is a name, that's going to need different security level than if you're collecting name, social security number, and biometrics. So there's very much an interplay between those two that you want to make sure is captured.

Now, these will be -- this information will also be captured in the new TA-FISMA. If you're not familiar with TA-FISMA, this is where Bob West's group is putting every single system that they have found within the Department and they're making sure that we are accountable for not only the security but also for the privacy, accessibility, a number of other things.

We will be making updates over the next couple of months to the TA-FISMA to better capture the privacy perspectives and so that we're able to report this information to all the outside authorities that need to know what we're doing. There's OMB reporting under FISMA now for privacy that was relatively new this year. GAO likes to come and ask us questions. Congress likes to ask us questions. We need to be able to do this, and this is going to be the tool by which we're going to do much of that tracking.

I think with that I'm going to turn it back over to --

MR. COLEMAN: After giving a brief outline of the document, of the three main documents you're going to encounter doing your privacy compliance, I want to talk a little bit about the situations in which you will encounter these documents. Now, this may sound a little redundant because we're still going to talk about OMB and C and A and FISMA and things like that. But just keep in mind as a perspective these are the situations you may encounter a request for privacy documentation.

As Becky mentioned, it was nice to have Eva Kleederman here because she could come and talk directly about what OMB's requirements are. OMB conducts -- you have to submit your financial documentation to OMB for them basically to give you money. Some of you people in the room are responsible for submitting OMB-300 investment information, so you're already familiar with this. But OMB may come to you and ask for information.

Now, with that said, please do not send your privacy impact assessments to OMB. They come through us and we submit them to OMB. So it will be part of your investment package that's made to headquarters, but it will not -- you specifically will not send it to OMB. Actually, CFO will ultimately send that to OMB.

OMB asks specific privacy questions. They will ask you specifically, do you have a PIA completed, do you have a SORN, what's the citation for the SORN, where can I find it, where I can find your PIA? If you don't need one that's fine, but that determination will be made long before the budget submission gets made.

Moving on to the next slide, as we talked about, Bob West was here to talk about TA- FISMA and how we've been working with his office to marry privacy and security concerns in the same process, so that hopefully it's easier on headquarters folks, components folks, to make sure there's sort of a one-stop shop for all these requirements.

But that doesn't mean that CIO, the CISO, or the CFO's office won't ask you for your privacy documentation. It could come up in an area just during the regular course of business. The CFO once again is in charge of the OMB-300 submissions to OMB. So they are going to be asking for that documentation per us. So please submit your PIAs to us and we'll finalize them with you.

Additionally, as you can probably gather, the system of records notice through the Privacy Act -- the General Counsel's Office may be asking for privacy documentation. Please feel free to call us if you have questions, but the General Counsel's Office also has its legal duty and responsibility to make sure the privacy documentation for the Department is in place. They work with us on that and they also work through the components. So please make sure you have a working relationship with your counsel or your boss has a working relationship with your counsel.

Additionally -- and these are the more fun ones -- the Inspector General's Office may be doing an audit on privacy documentation or security paperwork, things like that. PTAs, PIAs, SORNs, just like at OMB, just like in C and A, just like the General Counsel may ask, OIG may be asking for that information.

Additionally, GAO may be asking for that information. They are regularly doing reports and reviews of government-wide privacy documentation and related things, particularly with the VA incident that's occurred. They're asking questions.

Our privacy documentation as a Department needs to be in place, so these are the characters who may be asking for privacy documentation. Now, once again, please work through our office. If the GAO calls your desk and says, I need your PIAs from this, I need your PTAs, please make sure to call our office because those efforts need to be coordinated on a Department level as well.

So I guess those are the positive aspects, getting everything in order. There are also -- there are also risks associated. So I guess if I just held out the carrot I get to hold out the stick as well. There are real fundamental consequences. Now, I don't know what everybody in the room is doing on a daily basis, but I'm sure we have program managers in the room, we have security officials in the room, people who are concerned about getting their programs shut down.

If you do not have your privacy documentation in place, for example in the OMB process, you do not get money for the next fiscal year or the fiscal year that the OMB investment review is being done. If it's not in place they simply won't approve it. Our office won't approve it and it won't even make it up to OMB because they'll just send it right back. So you put your funding in jeopardy if you do not have your privacy documentation in place.

Similarly in the C and A process, you cannot get an authority to operate if you do not have your privacy documentation in place. That's another show-stopper. If you don't have your privacy documentation -- I don't know how more simply to say it. If you don't have your privacy documentation in place for the security processes, it's game over. You've got to get it done. It has to be done. That's why we always urge you to get it done early and often in the process, because it's easier on everyone. Nobody likes a fire drill on the day before go-live and that will be a show-stopper if that happens.

Additionally, like I mentioned before, OIG, GAO, and Congress can come. Some news event happens, Congress starts asking questions. Congress has no problem pulling somebody's funding or telling somebody to shut down, because ultimately we're all beholding to what laws they pass.

So for example, DARPA's Total Information Awareness just got gutted because the privacy documents weren't in place. There was bad press. I can't say it any other way. You guys know with the VA situation that came out everybody is now reviewing the notice procedures.

We need to make sure these documents are in place because ultimately, not only for the privacy, you should want to do this because it makes your system better, but you can minimize your risk on the back end by not getting your program funding cut, not getting your ATO when you were making sure, trying to make sure that you were going to get it, as well as getting simply bad press and, for example, the Secretary or our office come down on you because everything wasn't in order.

MS. RICHARDS: Just one of the important things you want, the PIA has benefits and it has benefits associated with actually doing it. You're going to increase the efficiency of your system if you're doing it early and often. It's much easier and much cheaper and much more efficient to actually build those privacy protections in at the beginning of the development of the program, when you're starting to think, what is it I'm trying to do and how is it I'm going to implement it?

So it's better to do it early. Your benefits far outweigh. Now, you may be saying, oh, this is just one more piece of document before I go live. But as Nathan has just outlined, the risks associated with not doing your documentation and having not -- not even just the documentation, but not having thought through and be able to answer those questions about privacy when they come up, is very, very serious.

So you want to think about, from the benefit side, this document has demonstrated that I've thought about privacy, I've been transparent. It's also a means by which we create a trust with the Department, between the Department and the public. We are telling them, this is what we're doing and this is how we're doing it. So there begins to be a level of trust that's very important.

So you want to think about the PIA not just from a, I'm going the check this off, but from how it's going to make my system better, how I'm going to be able to better tell officials who are asking questions about my system that, yes, I thought about privacy up front, these are the changes I made and this is how I'm doing it.

So as Nathan said, we will regularly say you want to do your PIA early and often. I think earlier -- Barbra was talking about the system development life cycle and somebody had a question about the system development life cycle. The PIA should be done at KDP-1. I'm not sure if we're calling them those, but key decision point 1 these days.

It should also be done when you're ready -- you should be doing it as you are developing it. You should be thinking about how exactly you are going to mitigate the risks that are identified. You think about what information I'm collecting. The number of people that we ask the question and they come back to us and look somewhat blank indicates to us that they haven't thought through whether they needed every one of the pieces of information.

From a legal perspective, from the Privacy Act, from the E-Government Act, from the Homeland Security Act, it is all our duty to make sure we think through whether or not we need all those pieces of information or if we would be able to do our job and secure the homeland with only a few less pieces of information.

MR. COLEMAN: So we've outlined what the documents are. We've outlined certain contexts in which you might come across these documents or be required to draft these documents. Now we're going to get a little bit more granular, like, okay, what about these contexts will trigger me to actually have to write these documents?

Now, in the back of your guidance there is an appendix that lists the OMB triggers for a PIA. I will talk about a couple of the major ones here, but I will just give you a general overview of when PIAs are triggered.

First and most major, developing or procuring any new technologies that handle or collect personally information. It doesn't get any more straightforward. So you developed this system, you've got a great idea, pitched it to your boss and said, you know, this is something that can really help our operations. If it's going to involve the collection of personal information, you're going to need a PIA. There's no doubt about it.

Just to keep hammering it home, OMB budget submissions. If this is your new investment, you're developing or procuring a new technology, if you're asking for money for it and it handles personal information, you're going to need it.

Additionally, the C and A, security. If you're developing a new technology or procuring this new technology that's going to collect personal information, you're going to need it. OMB's going to ask for it, our office is going to ask for it, the CISO and CIO are going to ask for it.

What it does is -- just like Becky said, you do these early. You get a draft done early so you're thinking about the issues and continue to dialogue with our office before you go live. Make sure that privacy is embedded in every system that DHS develops. It helps make better systems along the way and prevents trouble and reduces risk at the back end.

I mentioned the budget submissions to OMB. Pilot tests, I mentioned these. Becky mentioned these as well. Having a PIA submitted to our office the day before you say you're going to go live does nobody any good. You need to have the PIA done before the pilot test starts, because we can't implement any meaningful privacy protections and neither can you by the time your pilot test is done.

We would like to know what goes on in the pilot test, what results you get back, any flaws. That way we can implement better privacy protections throughout the system.

MS. RICHARDS: From a pilot test, you may say, oh, I'm just using dummy data. Dummy data doesn't matter. If you're developing a pilot you need to do the PIA, because if you already know what fields you seem to think you want then you haven't done the privacy impact assessment, you haven't thought through how you're going to implement privacy into the program. So just because you have dummy data doesn't get you out of the requirement to do the PIA.

MR. COLEMAN: Thank you.

Moving on, another major OMB trigger that you find in the back of your guidance once again: Developing system revisions that affect personal information. Now, the key word here is going to be -- it's not up there, but the key word is "developing a significant

system revision." We would like to have a dialogue with you about whether you think your system, system revision, is significant. However, OMB -- we're now what, four years out on the passage of E-Gov. It is highly unlikely you haven't done a significant revision to your system.

If you have done revisions and you don't think they're significant, call our office, because we're going to see your system through the OMB-300 process. We're going to see it through the C and A process. So please proactively call us and say: You know, I'm doing these revisions to my system; do you think I need to do a PIA? Maybe, maybe not. Just give us a call, give us an email, and we'll talk to you about it.

Go ahead.

MS. RICHARDS: An example of something that wouldn't need a PIA would be changing out the servers. An example of something that would require a PIA would be your giving access to the information over the web now. Those are two different ones. What we're seeing in our experience of having reviewed upwards of 200 PTAs and at least that many PIAs is that three or four years out technology has gotten better. So we want to make sure that we're capturing those things.

I think an equally good question would be if you have a legacy system you haven't made any significant changes to, is that system still efficient in doing what you need it to do? Are you using that the best way possible?

MR. COLEMAN: Additionally, so let's say you have your system and you actually have a PIA in place, it's published and ready to go, or it's published and on the go. The system -- and you say: Okay, Dear Privacy Office, I want to make revisions to this system; what do I need to do to my PIA?

Well, you have one or two options basically. You can amend that PIA in the actual PIA and say, okay, well, on this date system revisions were made that affect, for example, web access, we gave these people web access. Well, at that point you're going to want to expand on the sections of technical security measures, how are you securing that access, and the user roles and the people who are now going to have access.

That's the first, where you can amend the actual PIA. Or you could do essentially what's a codicil to it. U.S. VISIT does it sometimes, when they slightly amend the system,

when they don't want to go in and amend the complete PIA, but the cover page will say: On this date we have expanded this to include this. Simple, straightforward. The public knows what changes you've made to the system, it's clear, and it's not time-intensive. Just draft it up and get it on the way.

MS. RICHARDS: Now, one of the things you want to remember about what the PIA is is it's a transparency tool for the public. We'll go over this when we get to how you draft the PIA, but the tool is -- the PIA is meant to be read by the public, and to that end if you are making just a few small changes, we're not here to tell you you need to do a whole new PIA. We don't necessarily want to read the same language that you put in these other past ones.

So if it makes sense, then we are all for doing a one-page that goes on the front of your existing PIA that says: On such-and-such a date we are expanding the number of individuals who are going to be -- are going to be affected by this particular question. These are the things that we've done to mitigate the risk, end of story.

We want to work with you. We don't want this to be all of a sudden you have additional work. On the other hand, if you have significant changes to what you are doing and you have an existing PIA, then we want to again work with you to figure out how best to capture that. Sometimes the changes are, it makes sense to do the one-page and sometimes it doesn't.

So we're here to have that dialogue back and forth about how best to be transparent to the public and to those who are holding all of us accountable for privacy within DHS, so they can do that. These are the tools by which they hold us accountable.

MR. COLEMAN: The final -- this comes straight from the Homeland Security Act, section 222. If you're doing a new or updated rulemaking that affects the use of personal information, you have to do a PIA. The statute couldn't be more clear. So basically, Congress says we need these provisions implemented; okay, well, we need to promulgate a rule that says how we're going to change our procedures in the Department to meet that mandate.

At that point you would initiate your PIA and say: Okay, how is this rulemaking, how is this change in procedure affecting our current systems and the way DHS operates and collects personal information.

MS. RICHARDS: This is something -- I think also earlier today someone mentioned that there is a law on the Hill right now. But this is an existing requirement that is for DHS that is specific to DHS. I think -- the two laws that really are requiring the PIAs are the E-Government Act section 208 and the Homeland Security Act 222. The rest of the federal agencies obviously don't have the Homeland Security Act, so they're going to have slightly different -- their rules may be slightly different.

The other is that from the Homeland Security Act the first one is that the Chief Privacy Officer is meant to ensure that privacy protections are sustained and not eroded by technology. The PIA is the means by which we do this. So that is where much of the requirements for the PIA are coming from, is those three sort of specific portions of the law.

MR. COLEMAN: We mentioned, okay, you're procuring something, you're revising something that collects personal information. Okay, well, next question is what's personally identifiable information as defined by the E-Gov and the Department? Well, as you can see in your guidance, and I believe it's in the introduction - - and much of what I'm about to say is actually in the introduction of the guidance -- personally identifiable information is defined as "information" --

MS. RICHARDS: Slow down.

MR. COLEMAN: Sorry.

MS. RICHARDS: Slow down.

MR. COLEMAN: Am I talking too fast?

Is defined as "information in a system or online collection that directly or indirectly identifies an individual, whether the individual is a U.S. citizen, legal permanent resident, or a visitor to the United States."

Now, you could have a question, okay, well, I am developing a system using this technology, but all we're doing is taking a body scan, a picture, a picture of someone. You need a PIA for that because not only is that personal information, even though you don't have the person's name, that technology needs to be reviewed for privacy concerns,

because just imagine if you were out there or your grandmother out there. They'd want to know if their picture was being taken. They would want to know if their body scan is being taken. So that's something we need to generate and review that technology and make sure that it's meeting privacy concerns.

As you'll note, in the PTA it talks in broader language. This question has come up to us: What information? The PTA specifically says, when we ask you if the system collects information about individuals, either indirectly or directly, to us on the PTA we want to hear about that the individual includes DHS employees, contractors, citizens, noncitizens, and legal permanent residents.

The reason for this is we want to know the broad scope of what your system does. It's not helpful to us for you to make determinations about whether something applies to your system or not. That's why we are here. We make those determinations and help you move along to get the proper documentation in place. Without all the information about what your system does, even if it's just an HR system -- we need to know what that system does because we're accountable on several levels for accounting to OMB, GAO, OIG when they ask what systems they're managing and what privacy documentation is in place and the determinations we made why or why not a certain provision would apply.

Go ahead.

MS. RICHARDS: On the e-Government Act, Eva this morning talked specifically about the fact that, while on the requirement for employees or contractor information, a PIA is not necessarily required, that OMB highly recommends it from a policy perspective. That is the same policy that we have here at DHS.

So you will see PIAs on the major DHS employee systems. There are several on the Match- HR and their associated systems talking about the privacy, because privacy of our employees and our contractors is just as important as it is for the public.

So from a policy perspective. But we are also now capturing that. If you have some systems that, for example, have user name and password, we want to know about that system. At this point in time we may not -- we are not likely to require a PIA. But if you begin to make major upgrades and things we still need to know about that. So that's what the PTA does and that's why there is a broader definition under individual than there is for the PIA.

MR. COLEMAN: I think actually Becky touched on a couple more things. So we just talked about when you need a PIA, a couple of the basic definitions you would work off of. But you're probably trying to find out, okay, do I really need to do a PIA. There are a couple circumstances we want to outline.

As Eva said today and as Becky reiterated, if you have made no significant changes to your system prior to 2002 and up to this point, you don't need a PIA. However, up until this point technology has advanced, security measures have advanced, types of collection, user access, usability. There have been several developments technologically in these areas.

We're going to want to review whether or not you think that change is significant. So please talk to our office through the PTA process and then ultimately through the PIA process if we determine that the change is significant enough to warrant a PIA. Please talk to our office before you prejudge the system.

Additionally, Becky mentioned the HR systems. As a Department policy, we like to see high-level, the major HR-type systems do PIAs because it is our belief that you as employees and contractors don't lose your privacy rights at the door. You have just as much a right to have your information securely protected as anybody else walking down the street, because once you leave this building you are the person walking down the street.

So we'd like to see those high-level HR systems do PIAs as well. So please come talk to us in that regard.

MS. RICHARDS: We're sort of done now with the high-level process. If you have questions, Lane and Kathleen are on either side. Ken's going to come up and read some of your questions and Nathan and I will try and answer. We're going to go with this for a little while. We'll go from there.

After we're done with this Q and A part, then we will break for coffee so that you all are wide away and ready to go through how to write the PIA, which is probably why you're all here. You'll want to make sure that you have your hypothetical, your guidance, and a pen because we're going to make you work.

MS. SYMONDS: The first question's an easy one. You may have already answered it, but just to confirm again: What does the acronym "C and A" stand for and what does "TA-FISMA" stand for?

MS. RICHARDS: All excellent questions. I think one of the rules on writing a PIA is don't use acronyms, and then I realize I'm sitting up here doing nothing but that.

"C and A" is certification and accreditation under the Federal Information Security Management Act, otherwise known as FISMA. "TA-FISMA" is Trusted Agent-FISMA. This is a tool that is being developed by and for the chief information security officer and it is the means by which individuals going through the C and A process upload whatever their required artifacts are in order to get certified and accredited, and then our office reviews the privacy documents that are put on that particular one.

MR. COLEMAN: C and A -- let's say that you're going to design a system. You're going to have to ensure that by certain standards through NIST and FISMA and things like that you're meeting certain criteria. There are criteria under which you can't just have sort of a rogue system, okay, I'm going to plug this thing in and go. You have to meet certain guidelines in which to operate that system.

The C and A process, the certification and accreditation process, ensures that you're meeting certain federal guidelines so that you can plug in your system and be ready to go.

MR. MORTENSON: A question connected to that. Basically, when we're looking at the discussion here there was a lot of focus on C and A and how that spawns the privacy impact assessment process. However, there is a connection to the system development life cycle. How does that fit in with regard to the privacy process, and kind of explain, if you will, the two paths?

MS. RICHARDS: Excellent question. Your PIA, early and often. If you go away with pretty much that and a couple of other key questions, you're going down the right track. The PIA should be done in the system development life cycle early. By the time we see it in the final form, you should have already been dialoguing back and forth with us on whether the PIA was needed, whether the PTA was needed, because the C and A is sort of that last gate.

At this point in time, we're still catching things at the last gait. My goal is a year from now I won't have to use that gait. Instead, I will just have a processor going in and when you upload your document I will have already had many conversations, our office will have already had many conversations, you will have already done your PIA, and that's the final one that's approved and you're now ready to go live.

MR. MORTENSON: One thing I might add to that in terms of the system development and actually the investment review process. The Privacy Office is working with the different components of that, the Enterprise Architecture Board, the Investment Review Board, in order to have at the very front end of the development of any system a review of what we're going to call privacy requirements.

We're looking at that both from a technology standpoint impact, looking at the facts of which technologies you've selected, and also in a way similar to the PIA process of looking at the use of personally identifiable information.

Again, just to stress what Becky was saying, this is something that happens throughout. The focus here on the C and A is that this is a very good point at which we can catch things and getting you involved in that process -- many times this is the first time people are running into that. But certainly, hopefully you're doing it throughout the process.

Some questions here about looking at individuals, that is who is an individual, who is covered, and some questions about, well, when we're talking about individuals does that include non-citizens, does that include LPRs? What's the definition?

MS. RICHARDS: The definition is broad and this is particularly true for the PTA again. So an individual is basically anybody. It doesn't matter if you are a legal citizen, a legal permanent resident, an illegal coming across the country. We want to know about what you're doing with the -- within the PTA, so we can help you make a determination.

When we move to PIA, again if you're collecting information about somebody -- you, me, anyone who it is -- then it's likely going to need a PIA. So it's a person.

MR. MORTENSON: Well, connected with that then is, what about internal systems, HR systems and the like, that collect individuals working for the government?

MS. RICHARDS: So again, what we were saying about from an HR perspective is, from a policy perspective, major HR systems, Match HR, some of the headquarters different programs that they're doing, are doing PIAs because it is what we are recommended to do by OMB.

If you have a system that is a list of user names and passwords and it's at a component level, at this point we want to know about it through the PTA process. We are unlikely to require a PIA at this point.

MR. MORTENSON: A question about PIAs for systems that may have -- may not be a very simple system in terms of just being for one particular component. What about PIAs that are cross-service or there is cross-connection between other agencies? How might we view those particular types of systems for this process?

MS. RICHARDS: We want to sit down and think of -- there are a number of different systems within the components and we've had some conversations. These are the types of systems you want to sit down with us and have a conversation about what makes the most sense.

If we go back to remembering what the PIA document is, it's a document that is meant to have transparency so the public knows what we're doing with their information. So if we go back to that, you want to do the PIA in a way that makes sense. Sometimes the whole system as it's C and A'ed may actually have two PIAs. There's an example of that, because the PIA didn't make sense when you had so many different moving parts.

You want to talk about what that particular mission is for that if you have several PIAs. The Homeland Security Information Network Database, this is an example. It's a published PIA that provides you an example of a system that has many different functions. We worked with them very closely to make sure that the whole document made sense as sort of an umbrella, describing to the public what it is we're doing with their information.

MR. MORTENSON: Kind of in connection with that, there's been a number of questions that have looked at the Privacy Act of '74 and the exemptions under that particular act. Can you explain the connection between the e-Government Act PIA requirement and that in terms of those exemptions, and why would we require PIAs for

systems that would be exempt under the Privacy Act in terms of law enforcement, national security systems, and those sort of things?

MS. RICHARDS: So I think that it's both the e-Government Act and Homeland Security Act, for all of you DHS folks, would be the first answer to that. The Privacy Act is of 1974, exactly. In 1974 we had nice records and we would pull out the filing cabinet and there would be your records.

As we have moved into the electronic age, the e-Government Act was passed and the idea was we needed to capture what that meant from a privacy perspective and we needed to think about the impacts that were happening there. The PIA helps us determine what are we doing within the information technology or what are we doing from a system perspective with regards to personal information.

If you have, for example, an intelligence or a law enforcement sensitive system, we may not in fact actually choose to publish the PIA. But we as the Privacy Office and the Chief Privacy Officer as statutorily required needs to ensure that we understand what we as a Department are doing with personal information.

So there are laws that will tell us, you know, you need to publish this or you don't need to publish it, but our office still needs to know and understand so that we can -- so that she can stand up and ensure that she knows that we are in fact sustaining privacy within the Department.

MR. MORTENSON: Again, a number of questions have asked: When a system has personally identifiable information, how do we identify personally identifiable information? Does it deal with the input of the information, such as a query, or is it related to the information itself?

MS. RICHARDS: Okay. This is actually where you'll differentiate between -- where the PIA can help you differentiate between a needing a system of records notice and not needing a system of records notice. So if we go back to the example I gave earlier of I show up and I have a visitor badging system, my information is there and you've collected my name and you've collected the fact that I showed up at the GSA building on such and such a date.

If I'm not -- if I've collected that information, you're required to do the PIA. It's personally identifiable, it tells me -- it says something about me. But you're not required to do the system of records notice because you're not retrieving it by the individual or by the personal identifier.

MR. MORTENSON: How would this relate to a pilot project, particularly in the sense of dummy data collection? Will we still need to do a PTA, a PIA?

MS. RICHARDS: You still need to do the PTA. You still need to do the PIA, because again if you're developing a pilot you want to think about privacy early and often. How do you do it? You do it by thinking about it when you're developing the pilot. Again, it's much more effective, much more efficient, to think about privacy up front, think about how you're going to implement those access controls, think about what security is needed, if you do that up front.

If you've already developed the pilot and you're already on your way and then you say, well, wow, this really gave us everything we needed, and then we look at it and say, but you have these privacy concerns and these are not likely to be a problem for you, then you're going to sort of get stopped right in the middle of the road.

So you want to do the pilot -- you want to do the PIA for the pilot, or you need to do the PIA for the pilot. Not a lot of "want."

MR. MORTENSON: There's no such thing as a pilot program for privacy purposes.

MS. RICHARDS: Yes.

MR. MORTENSON: Some questions about exchange of information with other agencies or with non-governmental agencies. What should we be looking for in terms of the agreements with, memorandums of understand or what-not, to ensure that the PIA requirements, that is those, the duties placed upon the agency with the information that's exchanging information, are abided by by the recipient entity?

How will that -- how do we reflect that in the PIA?

MS. RICHARDS: Well, the PIA has two different sections or three different sections basically talking about sharing and use of that information. So you want to make sure

that you're clear and up-front about what you're doing with the information, who you're sharing with the information, how you're sharing it. When you do the PIA you're going to identify what risks are associated with it.

So for example, if you're sharing the information with an outside organization, one of the risks associated with that is that that organization is going to take that information and use it for a completely different purpose. So there's different ways that, depending on the nature of what the information-sharing is, that you can mitigate that risk. That's what you want to capture in the PIA.

Now, sort of downstream from that, from the PIA, is that it's likely you're going to have an information-sharing agreement or some type of MOU, and that should be captured. You want to write down so that everybody is clear what the information is being used for and when it's appropriate or not for that information.

You may, for example, decide that if the external organization decides they need to use that information to make a determination about benefits for somebody, that they have to come back to you. There may be different ways. But you want to think about it and you need to work with the partner that you're sharing the information with to make sure everybody is clear on what the rules are and you want to make sure then that it is clear in your PIA.

If we go back to the fact that the PIA is your transparency and accountability document, if you say, we are going to share information with X, Y, and Z for these purposes, but then for whatever reason something different happens, you want to make sure that privacy documentation is accurately and appropriately reflecting what you are doing.

MR. MORTENSON: Kind of a similar question to one before, but it's a little bit different in the sense of, in terms of the development process it's possible that during the process different components or parts of a system will be developed, and let's say that there was some PIAs done for earlier parts of the system. How would you deal with PIAs? Would you do new PIAs? Would you do updated PIAs, amended PIAs?

What would be the best process?

MS. RICHARDS: It's a great big "it depends." Some of these things are very fact-driven and so what I would say is we want to work with you so that it's clear what we're doing and we're not creating a whole lot of extra work for everybody just for the sake of doing extra work.

So if it makes the most sense after you're able to describe to us what you're changing that we make a few amendments to existing PIAs and then put a summary together, then that's what we'll do. If instead it sounds like we need to go back and revise some of those PIAs because what's going to happen is it's no longer clear what you're doing because of what's existing out there, then we also, we will work with you on that.

But unfortunately, it's very fact- specific to your different situations.

MR. COLEMAN: Let me add something a little bit onto that, to pick out one of the components, for example. CIS is doing a lot of modernization efforts. They deal with alien files and people applying for benefits in the country. They are going through -- through those modernization efforts, they are going through a tiered phase and certain implementations. We have worked with them hands-on and said: Okay, probably for phase one and phase two we could do a complete PIA because that's what makes the most sense. But by the time we get to phase three we should have a fully robust PIA and we'll just have the first part of the PIA in progress, because there are certain privacy implications that come in at each phase and each of those may need to be documented.

But like Becky said, it's very fact- driven and all it takes is a phone call or an email to us saying, you know, we need to sit down and talk abot the best way to do this, because we're not in it to make more work for people, but we're here to make sure that legitimate privacy protections are implemented.

MR. MORTENSON: I would add a couple things. For those of you who do system development, you know when you're doing system development how you have chosen to break out your system. You look at it in a modular sense in terms of understanding what are the different parts of that system? What you want to be able to recognize in that, are there differences in the way that personally identifiable information is handled as between those particular systems that you might want to reflect upon differently?

Remember, we want to look at privacy from the standpoint of that particular system, but we don't want to have to do -- if you do an overriding PIA, sometimes that

doesn't accurately reflect the differences in the way information is handled. It makes it a little bit more complicated, it might make it a little bit more difficult.

As Nathan was just talking about, one way of doing that is breaking it into separate parts. So you can think of aligning that with your systems development life cycle process, in which you've looked at the different parts and components of the system that you're developing. So if I have one big major system, but I have ten different areas where ten different types of personally identifiable information is handled, it might make sense to do ten different PIAs.

Again, as Becky said, it is an "it depends," which is my favorite answer in the world, being an attorney. But it certainly is one of those things where you can look at it and figure out, do I group certain things together because there are similarities and I can talk about them in the same way, or should I separate them out such that I can talk about it with specificity?

I think one of the things that we want to be clear about is the more specific you can be in talking about privacy concerns, the better off you're going to be, because then that lends to the better understanding of the purpose of the program as connected to the information. Thus it lends to the transparency to you understanding what the concerns are from a privacy standpoint.

A related question, in a sense: How do we deal with rulemaking procedures? That is, what if we have a PIA for an existing rule, but a new rule is going out? What sort of choices do we make and do we do a new PIA or do we not do a new PIA?

MS. RICHARDS: We want to make sure that the documentation matches whatever it is we're doing. So currently TWIC, the Transportation Worker Identification Credential, has a notice of proposed rulemaking out there. There's an associated PIA. When we go to the final rule we will have to assess at that point what were the changes that were made between the notice of proposed rulemaking and the final rule.

To be honest, it will depend on how many changes we made between those two systems. I just, I want to go back to the idea that this is a public document. You're writing it for the public. You want to explain to them what they're doing. I'll talk about in the next portion of this about the grandmother test. But that's important here, because you want your grandmother to understand what it is you're sort of talking about.

If you make a bunch of changes and you do a whole bunch of different things to the system, if it's not clear to the public or to your grandmother what you've just done then we haven't met that test and we haven't fulfilled our mandate of being transparent, accountable, and creating a trusting environment.

MR. MORTENSON: The next question is: What if a contractor is actually hosting a particular system that is performing a governmental function? Would that system require a PIA if it contains personally identifiable information?

MS. RICHARDS: Oh, absolutely. If you have a contractor who is doing something in the shoes of the government, and even if there's some question about exactly what that is, you want to do the PIA and you're likely to need a system of records notice. If you're acting on behalf of the government in some way, shape, or form and if the government is the one sort of telling you this is what needs to be in the system, you have a system and you meet the requirements under the Privacy Act, you definitely need a system of records notice and you definitely need a PIA.

You can't get around your privacy requirements by asking the contractor to do your work for you. You can ask them to do the PIA for you, but you're going to be held responsible for whatever that information is. So you want to keep that in mind.

That's particularly true -- and if there are questions about whether or not a PIA should be done, you want -- we're going to err on the side of you need the PIA, because it will look better from a public perspective. It doesn't look like we're trying to hide what we're doing. So you want to keep that in mind.

MR. MORTENSON: A question about the OMB-300 process and the connection between the requirements of having completed SORNs, completed PIAs. What's going to happen if you require either one of those and what's the deadlines, and are there waivers?

MS. RICHARDS: So if you are part of an OMB-300 you probably have already spoken to Nathan and I and you know where you stand. If you're like 80 percent of them, you're failing. So what does that mean?

Most of you may be here so you can write your PIA. It has to be done. Most of -- the OMB- 300 is for major programs. Most of these programs have been in existence and

should have had the PIAs done two years ago, so you've sort of gotten your waiver. You were working on it, you were doing something.

This year, OMB has clamped down particularly. I think we're going to see a lot more because of the different breach issues. But you are expected to have your PIA and you're going to have to have a really good reason why your PIA is not completed and approved by August.

Remember, it takes iteration to do your PIA. So you need to get those to us now so that we can work with you to make sure they're approved and your funding is not in jeopardy.

MR. COLEMAN: Further on that point, OMB submissions, there are like 140 or something like that this year?

MS. RICHARDS: Yes.

MR. COLEMAN: You're not the only one that we have to review. So the sooner you get it to us, the sooner we can get you a substantive response. We're not -- if you send us your PIA on the day before your OMB is due, don't expect a response on that.

MR. MORTENSON: Expect a response --

MR. COLEMAN: You'll get a response, I guess.

MS. RICHARDS: You'll get a response and it's not going to be what you want. We don't want --

MR. COLEMAN: It'll be a short response.

MS. RICHARDS: We've been trying to work with the components and through the CPIC, the capital planning process. We have been very forthright with everybody as soon as we started training this last year in February, telling people. We've been working with all of you. If you have a program that you think is in question, you need to make sure that you are working with whoever is in your component.

We have components where the privacy documentation is officially provided to us through a different part than the one who's doing the CPIC process. If you guys -- you may need to be putting different pressure to make sure whoever it is in your component is the one who gives us the privacy documentation actually knows that we expect it and that your funding is at stake.

It's a serious situation. I've had a number of components sort of trying to figure out how they're going to deal with that situation. And I get phone calls and it's the CPIC person or it's the program manager going: I gave my PIA to this person over here; what's going on? I don't have control over the component program person who gives me the privacy documentation. That's within your component and you need to work on that.

MR. MORTENSON: A related question to that is more of a procedural one, which is: About how long does it take to do the review of the PIA from start to finish, including the approval?

MS. RICHARDS: I'm hoping less now that we're going through the training process after this.

Sometimes it doesn't take very long and sometimes it does. It depends on the complexity of your system. It depends on how well defined the system is when you start. Did you know what information you were collecting and what you were doing with it or are you still sort of working that out? Do you know who has access? Sometimes we get PIAs that come to us that are very broad.

In this afternoon's session after we finish the Q and A I'm going to give you some examples of what are answers that are helpful, what aren't helpful. Telling us what information you're collecting -- I'm collecting background information, that doesn't tell me what information you're collecting. I want to know name, date of birth, ten fingerprints. That's the sort of information we want to know.

So it depends on the state of the PIA that comes to us as much as that. Once our, the compliance department and legal counsel in the Privacy Office has reviewed and felt that the PIA is in good order, you will submit it to us officially. We will give it to Acting Chief Privacy Office Maureen Cooney, who takes anywhere from three to five days to review and do the final approval.

She may have some changes or questions as well, but generally that's the process.

MR. MORTENSON: Actually, the next question is one I'm going to take on, which is: Basically, there was a few people that asked and said: Listen, we're all out there working as hard as we can; we have limited resources, we have limited people, we have limited amounts of money to accomplish things. This seems like a very big thing to take on. How are we going to actually accomplish that?

My answer to you is a very simple one, which is: The folks who fund us are going to make us do this and they're going to make us do this more. If you haven't seen it already, I would really recommend you look at some of the bills that are sitting out there on the Hill, now that we've seen what's happened with the VA data breach.

Congress is very concerned about citizens' privacy. They're concerned about it both from the private sector viewpoint, but also from the public sector viewpoint. They consider us to be holders of something sacred that belongs to the citizens, and I would say that this particular process is going to be much more important.

Just as security through FISMA became a very important process, we're going to see privacy became a much more important part of what we need to do and consider when we're building systems. I think that to a certain extent what we're going to find is you're going to be given more resources to handle that because our leadership has recognized that. You heard Kip Hawley standing up here this morning how from a TSA standpoint that they have recognized that it is critical that they build a culture of privacy into the organization, and by doing that that means dedicating appropriate resources.

So if you feel you don't have appropriate resources, if you feel that you need more to accomplish what we're asking you to accomplish, I don't think it is a bad thing to talk to your management, to talk to your leadership, and say: We recognize this is something important, we recognize this is something that is critical to the development process, just as important as it is to look at the technology, to look at the security, it is to look at the privacy components.

I think that there will be resources available going forward.

MS. RICHARDS: I would add a couple of things. When we were talking about the risks and benefits of doing or not doing the PIA, the benefit is if you are as you're

developing your system documenting what you're doing and you're able to describe it, the PIA really shouldn't take you that long. Sometimes -- you should already know many of these questions as you're going through the system development life cycle.

It's often where we see a lot of the resource-heavy is because you haven't thought about it, we're now at the CNA process, and you want to turn the system on, and we're going back and saying: Yeah, you didn't think about this, this, this, this, or this. So that's why you want to think about these early and often.

The benefit side is and somewhat of the risk side to all of this is, again, everybody's starting to look for these documents. They want to know that privacy is being protected. They want to know what we're doing with the information. You could say: I don't have enough resources to do the PIA. Well, if you don't do the PIA you may not have any resources at all, so you've got to think about that.

MR. MORTENSON: One last thing to add to that. You all remember when system development life cycle became a real big thing. When I was a design engineer, the whole thing was system development life cycle, we needed to do that. Why did we do that? Well, we learned that if we just went ahead and did a design and at the end fixed it, gee, that was really expensive from a developmental standpoint.

This is no different than that. This is just a different concept to add to that. But we're still talking about doing it as part of the process. If you think about privacy, if you say, hey, you know what, we're going to have as an input we recognize some of our data is personally identifiable information, I should begin thinking about privacy now, the cost and the effort and the time is much less, much, much less than at the end having either you realize it or the Privacy Office realize it and say: Oops, we've got to go back and we actually have got to redesign, reengineer the system. That takes much more time, that takes much more resources, as well as trying to do the documentation behind that.

If you're doing it along the process, you will already have all the documentation written. It's just a matter of bringing it in and, if you will, cutting and pasting it into the appropriate places in the PIA.

MS. RICHARDS: One more.

MR. MORTENSON: Now, one more question. This is a pretty simple one: Does every "what if" have to be considered when doing a PIA in the sections that we're talking about doing privacy impacts? Do we have to consider absolutely every possibility under the sun?

MR. COLEMAN: Is it directed at what if we decided to do this?

MR. MORTENSON: I think the question -- and someone, thankfully -- whoever wrote this, thank you -- gave us an example of how the play this. What if an employee breaks the procedure and takes data out of a secure environment?

MS. RICHARDS: Oh, okay.

MR. MORTENSON: That will never happen, right?

MS. RICHARDS: Well, I think that you need to -- you need to think of the reasonable "what if's." So that's a pretty reasonable, what happens if you have an employee who goes rogue or something like that? You need to have things in place that catch that. So you need to have sort of some of the reasonable "what if's" should be addressed from both the privacy and security perspective.

So some of the privacy risks that are going to be associated are, what happens if my employee, if the employee goes rogue and decides to steal all the data? Well, you should probably have in place regular audit procedures, regular training for employees to understand what happens if they do this, and then disciplinary actions that occur.

I can't off the top of my head think of a really crazy "what if" that might not be addressed, but you sort of want to think about what are reasonable risks and how have we reasonably mitigated them. It's similar to what Secretary Chertoff was talking about, what are the risks and how are we going to mitigate it. If it's a very minor risk, then we're not going to worry about it as much as -- I think a rogue employee is something we definitely want to mitigate against.

MR. COLEMAN: I'm going to answer a couple of real quick questions. First off, where are or will be the PIAs published? They're going to be published on the Privacy Office section of the DHS website, which is the www.dhs.gov/privacy. There is a PIA section there. Right now there's just a chronological listing of the PIAs currently out, but

we're working on, as we get a whole bunch more obviously after this particular event, reorganizing that as well.
There is a question about: Will the materials and other slides be available? We will be putting them up onto the website, the same location, the www.dhs.gov/privacy.

MS. RICHARDS: So right now it's 1:50. All of you, there's coffee outside. Please be back here at 2:00 o'clock with your guidance, your hypothetical, your pen, and we'll start off with sort of some hands-on experience of how to write the PIA.

(Recess from 1:48 p.m. to 2:05 p.m.)

PIA TRAINING - SESSION II REBECCA J. RICHARDS and NATHAN COLEMAN

MS. RICHARDS: We have one question somebody asked about: In the TA-FISMA or TAF that has not yet been approved, do you need to use the new form? The answer is no, as long as it was the existing Privacy Office-approved form. If you have some funny Excel spreadsheet, that isn't okay. If you have a Privacy Office one that has a logo and everything, you're probably fine.

If everybody can take out their hypothetical, you will see on the front is two paragraphs, a disclaimer saying this is not a program at the Department. This is a hypothetical that we developed. This is hands-on. On the back side you see your worksheet. I'm going to have you all have your pens out so that you can write down the answers and see how your answers match with what we're looking for.

Again, if you have questions as we go along, we'll do the same format as we did at the end of the previous session, so just keep passing them on and we'll take them as we go along.

Again, our goal today is for you to be able to fill out that PIA comfortably when you leave here today and to have most of your questions answered. So that's why we've come up with the hypothetical, so you're actually doing something and not sleeping in the back of the room. I know where you are back there. I can see you. Or maybe they've all left.

All right, specific areas to review. Let me start with the grandmother test. I already talked a little bit about this. The document is for public reading. If your grandmother can't read it, your mother-in-law can't read it, you aren't doing your job well, we're not doing our job well. So remember that. Think about that as you're drafting the document: Does this make sense to you?

No trick questions. We're not trying to trick you when you ask the question, what information are you collecting? I keep bringing this question up because you would be surprised at how many bizarre answers we get to this, what I view a very simple question. I just want to know what are you collecting. I'm collecting names, I'm collecting date of birth, I'm collecting 4,000 pieces of information.

It's fine, but we want to know what it is you're collecting. Give us the nice big list.

Finally, use the template. On our website is the template. Use it. Don't change anything. Don't delete questions that you don't like. We notice. We wrote the template. We know. Don't change it. Don't change the font. It's there because DHS uses some really funny font and we have to use it to follow DHS. We chose the font type. The size of the font, same reason.

It just slows down the process. Use the template, answer the questions. If you don't know how to answer it, it's okay; call us, email us. If you've emailed us in the last week, we haven't responded. We know. But we were preparing for this. But on the whole we're going to respond to you. We want to help you go through this.

If you don't know how to write the privacy impact assessment section, that's what we're there to do to help you think through, help you think about the risks and how you're going to mitigate it. Don't delete the privacy impact assessment section.

Now we're going to get into: What is the PIA? What are we looking for? What are we trying to do? If you begin the second portion of the guidance, basically we're going to follow this through and call out some of the questions that we see, some of the questions that people have problems with, some of the things that we sometimes see issues with.

The introduction and overview, this is the context for what you are about to answer questions on. So tell us what it is you are looking -- tell us what it is you're doing. If you look at actually the hypothetical that we gave everyone, those two paragraphs,

that's a good first start. It describes to you what the system is: I'm collecting this information and it's for this purpose and this is what we're doing.

If you have a reason you're doing the system -- Congress mandated it, the President said you have to do it -- tell us this information up front. Anything that's relevant to your system is going to go here. Imagine that you're on an elevator with someone or you're at a dinner party and you describe in a minute or two what it is you do all day, what's the program that you're trying to build, so that that gives the context for the rest of the answers.

You shouldn't have any funny surprises way down in external sharing or access requirements that weren't sort of given in the beginning portion of the overview.

Have I missed anything there? Let me get my notes here.

(Pause.)

Another thing that actually is helpful in this introduction and overview section is to maybe give us an example of what a normal transaction might be in the situation. So for example, if you are a program where you're collecting the background information, you might say: We collect the information directly from the individual, we collect the following information for these purposes, and this is where the information then goes. We share the information with the FBI, we share the information with the commercial data person. That gives you a flow, so that again you're giving the context of what is going on.

Do you want to add anything?

MR. COLEMAN: No.

MS. RICHARDS: Section one, information collected and maintained. This is sort of the who, what, where, why question that begins: What information are you collecting, why are you collecting, what are you doing with it? If you have a specific law that you are actually required to do this, if Congress said in law X, Y, and Z you need to do this, this is the part, these are the questions that you're going to answer those.

So now, pull out your hypothetical. Question 1.1: What information is collected in our hypothetical? Look to the side and think about it. Okay, hmm. Well, it looks like I'm collecting some name, date of birth, social security number. These are the list of the information that you want collected, so write this down right now so that you can think about it. Okay, what's my system actually collecting? What are the things that I'm doing?

If you're collecting information from outside of the individual, how is that happening? So for example, in our background example I'm collecting information from the individual, but I'm also getting information back on the eligibility of that person to be part of the program, on address verification from the data aggregator, and the fingerprint check. So you have additional information that is being collected in your system.

Here's an incomplete answer: The agency will collect information for a background check. Thank you, okay. I don't know what they're collecting, so I can't help you decide whether you have personal information or not. I can pretty much imply from this statement, if you're doing a background check, you're probably collecting it from an individual.

A more helpful answer would be something along the lines of: The background check system will collect the following. List it out: name, date of birth, social security number, current address, phone number, your ten fingerprints, and the results from the commercial data verification, and the results of the background check from the FBI.

This gives you, us in the Privacy Office, it gives the public, an idea of what it is you are actually doing and what you're actually collecting. It's not a trick question. Sometimes we see people here who put all sorts of information into it and other times we see this very incomplete answer.

Okay, question 1.2. Again, this is one for your worksheet: From whom is the information to be collected? Again, you need to stop and think about the information flows, who gives the information and then where does it go and then where does it return to? Think about the data flows and you want to make sure that you're capturing that information.

In some cases you're going to be collecting the information, like ours, directly from the individual. In other cases, also from our example, we're going to be collecting the

information from the data aggregator, we're going to be collecting the information back from the FBI. So an incomplete answer might be: The agency will collect information directly from the individual. That's the obvious one. We know that's happening because I wanted to do my background check.

A more helpful answer is going to be that: The agency will collect, list what information you're going to collect, and then tell us what you're going to do here. The name and home address are going to be checked against the commercial aggregator and the verification will come back into the system, and fingerprint verification checks are going to be received back into the system. You now have provided the universe of where that information is coming and where it's going.

MR. COLEMAN: Just to note on this, one of the points to take away here is that, don't forget about the information that is coming back to you. That's one thing that we see specifically in the first section. People think, okay, well, I'm getting this information back, but they don't actually note data is going onto that person's record that you are retaining then: FBI okayed them, the commercial data aggregator verified their address. That's information you're now collecting as well, so make sure to note in 1.1 and 1.2, don't forget about the information that is coming back to you, not necessarily the information you got in its initial collection.

Becky talked about the what and the who or the from whom the information is collected, but this gets a little bit more sticky. This is the why you collect the information. Now, it gets sticky in the sense that it's not difficult, but people tend to overthink, overthink this question a lot.

What you want to do in question 1.3 is relate it back to the information you're actually collecting. So for example, so we sometimes get this response: The agency is collecting information to conduct a background check. Much like question 1.1, that really doesn't tell us anything as it's related to the data elements that you're using. We've learned in 1.1 and 1.2 we need some specificity about what you're collecting and the avenues through which it comes.

The more helpful answer is to outline why you need the biographical information, for example, then why do you need the fingerprint information, then why is it important to have the commercial data aggregator. Then ultimately, although this was your

ultimate conclusion, this information taken together allows the agency to conduct a full background check. That is the full robust type of answer we would be looking for.

Now, don't write that down and just plug that into your PIA, but that's the type of thing we're looking for. We're looking for you to associate a why with each set of data or data field that you happen to be collecting, depending on the system.

MS. RICHARDS: Now, just because we don't cover a specific question doesn't mean it's not important and that you can not answer or you can delete it. We're just highlighting ones that we often see questions or issues with.

MR. COLEMAN: So to carry on that point, section 1.1 -- section 1.0, privacy impact assessment section. As Becky said, and let me reiterate this, do not delete the section because you feel it's uncomfortable or you don't know how to respond to it. That's part of the reason we're holding this seminar, is to give you a better idea of how to conduct a critical analysis, because this is the heart of your PIA. This is what we're looking for.

Obviously, if you don't lay a proper foundation in the introduction and the substantive responses, you're going to have problems with the PIA. But what we're looking for is the critical analysis of the privacy risks and how you may have mitigated them.

You can go on. What we're talking about here for an impact analysis for section one is what risks did you identify. We want you to critically analyze what risks you identified and potentially how you mitigated them. So for example, if 1.1, during the development life cycle, which goes back to it's easier to identify risks and mitigate them once you know about them early on -- for example, you may have had -- you thought, okay, well, we should collect mother's maiden name as well. Well, okay, actually we got through that and FBI said they didn't need it, the commercial data aggregator said they didn't need it, so why does DHS need it then?

Okay. Well, that's a scope issue. We reduced the amount of information that we collected as a mitigation strategy. That's something you want to outline in the impact analysis section. That is the critical analysis that you did, a substantive privacy analysis on your system.

For example, the sources of the information collected. You got information back from FBI, you got information back from commercial data aggregators, and you collected information directly from the individual. Obviously, collecting information directly from the individual is optimal because they know who they are and where they live and things like that. So whenever you can do that, that's optimal.

That may not be applicable to your system, though. So you want to tailor that to what your system is actually doing. You may not have an opportunity, like if you're an intel system or law enforcement you may not be getting that information directly from that individual. However, that's a potential mitigation strategy for the hypothetical that we've outlined.

Additionally, when you look at the why, the reason for the collection, what processes and procedures did you build in to keep inaccurate information out? Well, in our hypothetical what have we done? The commercial data aggregator can verify an address, which helps us verify identity. That's something that has been put in place and is helpful to verify and get a complete background check done for the Department.

MS. RICHARDS: In that particular case, with the example as we went through, one of the ways that we could also mitigate is that if we find the commercial aggregator has a different address than what the individual gave us then we would want to go back to the individual. That particular system -- that particular situation or this particular system, that's a good way to mitigate that risk.

As Nathan said, for a law enforcement or an intel one, that's probably not going to make sense. But you may also set up different processes and procedures in place before you -- in order to mitigate the risk of having inaccurate information.

MR. COLEMAN: So that takes us to section two, which is the uses of the system and the information. Now, this section covers a few different topics, the first question being very direct: What are the uses of the information? Now, I want to make a distinction here that the uses of the information are not the why of the information. It's not the reason you have the information. The use is the practical use of the information.

So for example, we send to the commercial data aggregator an address and a name because we want that to come back verified as an address. That is the use of the

information. We send that and the commercial data aggregator says yes or no, we have a match on that. That is the practical use of that information. That's what you do with it.

In contrast, the reason you have that information is to verify the address. I hope that distinction sets in, so if it doesn't set in we can go over it again maybe in the question content. But the use is more practical, is directed at the practical uses; the reason is the why of it.

MS. RICHARDS: Let me just further that I think the why is I'm collecting this information, I'm using it in order to do the background check. It's a broader reason than the specific use associated with the final mission of whatever your program is. So just to reiterate what Nathan said, the use of the address and name by the commercial aggregator is to verify the address. The reason you're doing that is because it is helping you to do the background investigation. So you sort of have a broader mission in the why than the actual specific use.

Similarly, you're using the fingerprints in order to determine a criminal history check. All of that goes back to your bigger why I need to do a background check, for whatever the reason is.

MR. COLEMAN: If you're following along in your guidance, which I hope you a are, the other questions in this section are related to data mining, which I will get to in just a second, as well as accuracy. So that is generally what section two is getting at.

So can you flip forward.

So does the system analyze data to assist users in identifying previously unknown areas of known concern or pattern? A very strange-looking question if you do not engage in this activity. But for you data-mining people out there, this is your question and you should be responding yes to this question. This is exactly -- that is exactly what this question is getting at.

Let me go into a little bit more detail. The data-mining aspect and the use and the function that we're trying to get at in this question is at the tools you are using. Are you taking disparate parts of information and bringing them together to form information you would have not otherwise had?

Now, what that gets at is it can be reporting, so for some financial systems out there as well you would be encompassed in this system, or for example in some civil rights reporting requirements you need to know hiring practices and things like that. Although that would not be considered data-mining in the sense that maybe the press would use it, that's the type of information we want to know, because you're now getting information that you would have not otherwise had.

Now, let's see. Give me one second.

MS. RICHARDS: Just as an example, from our example of our background check, we're not doing any of these sort of analyzing this information. But as Nathan was saying, if you have an EEO or if you have financial documents or if you have HR systems that are aggregating information, all of that would answer yes. Similarly, if you are looking for patterns and then associating those patterns with individuals, again that might be -- I think that's partly what the definition is under the DHS lexicon of data- mining. That is where you want to discuss this.

So if you are doing anything where you're getting information you otherwise would not have known based on aggregating that information, you want to answer this question and you want to answer it robustly.

MR. COLEMAN: So just to carry on what Becky said, in the hypothetical your privacy is no: No, we do not engage in this activity. Then you can say, well, you know, maybe the agency in question could run reports on that. When you're conducting the background check it's a one to one relationship. You're trying to verify that this person is basically who they are and that they have the criminal record that you believe them to have. That's basically a one to one relationship.

Now, the hypothetical, you could say, okay, well, the agency has conducted 2,000 background checks and 1700 of them came back approved or whatever. That's not the type of analysis this question is getting at. This question is getting at basically is there an analysis being done, is there information being brought in to build a larger piece of the puzzle, for example. That's what this question is getting at. It's not necessarily getting at raw, I completed 200 PIAs or whatever last year, which is not true.

So in section two, just carrying on what we talked about with data-mining and the final question, I believe, of section two is the accuracy question. Now, one thing we get a

lot is people only address the accuracy question, like: I know my information is accurate. Okay, that's fine. Give us a little bit more discussion about the uses of the information and, if you are engaging in data-mining or an analytical tool, give us more information about that.

So the risk and the mitigation factors we can talk about in the impact analysis section for section two would be, is there a risk, did we identify a risk for use of information for undisclosed purposes? Well, it's possible, it's certainly possible. So what we want to do there is make sure that we have some auditing measures in place and a review of the privacy documentation we have already put forward or a system design plan.

In this section you can also -- it's okay in your PIA to refer someone, for example, to section 8, which is the technical access and security controls. You're going to have a robust discussion in that section about your auditing measures, user roles and access. It's fine in the analysis section to say we have implemented certain fantastic security procedures, please see section 8 for greater detail on those. But you want to make sure to mention that those are -- that is a mitigating factor, for example, for inappropriate use.

Regarding the data-mining question, it's already an awkward sort of question to begin with, but we want to make sure that people are still addressing that. So if you're doing data-mining and you say, okay, well, I found this one piece of information over here and I'm now going to put this on this person's file, if that's what your system does then that's what it does, but what you need to do is identify that as a privacy risk, because what we now have is a computer or a program making a decision about an individual, now placing information on an individual's file, as it were, and potentially making a decision about that person, whether it's benefits, whether it's being put on a watch list, whatever your system is designed to do.

So a mitigating factor for that could be an actual human review of the details of the attribution of that information, as well as direct collection of information where possible, and then follow-up if a decision appears to be inaccurate or unfair, frankly.

MS. RICHARDS: So if you look at your worksheet on the back, one of the ones was, how do we answer this question for our hypothetical. What you would want to start to -- the sort of impact analysis section would start with probably saying is: In doing this PIA, we found that the following risks are possible. The information may be used for

undisclosed purposes. That's a risk, and we have mitigated this risk by ensuring that we regularly review our privacy documentation and we also have ensured that we are training our employees to do that as well.

You might also indicate that one of the privacy risks in this particular example is that there's a risk that individuals will inappropriately use the information. So I decide that I want to go look up Nathan because I'm upset with him and I want to find out all the derogatory or all the negative information on Nathan so I can go and use it against him. That's a very -- that's an inappropriate, unofficial use and I need to -- we need to make sure that we've trained our employees to know that if you in fact are misusing that information or using it for inappropriate reasons, that there are serious and real consequences to doing that.

Then, going back a little bit on the data-mining, if you are doing automatic attribution based on the data-mining and then you are going to make an automatic decision, that's where you want to start thinking about how can -- that is a serious privacy risk because you may have the wrong person, you may not have all the information.

So you need to think about from your system how are we going to handle that. More often than not, some of the tools that are used is having a person, a human, look at all the information and make the final determination before whatever the decision is is made. This mitigates it to the extent possible.

MR. COLEMAN: Section three is very short, but it's very direct. All federal records have to be scheduled for disposition. You as a system owner or program manager, you do not get to unilaterally decide how long you get to keep information. The Federal Government, there are statutes in place that govern how long different types of data can be kept.

Now, probably the next question is, okay, how do I find that out. Kathy Shultz is the Department's records retention official. She schedules all -- she analyzes the system and schedules all records for disposition. There are general schedules, specific schedules can be crafted. It just depends on what type of information your system uses and collects.

After Kathy does a review and makes a suggestion, the National Archives and Records Administration, NARA, approves all federal records retention schedules. Our

understanding after talking with Kathy is this takes anywhere from three to six months to get your actual records retention schedule going.

So if you already have an idea of the data elements you're looking at, go talk to Kathy and say: I need to set up a schedule; let's get this done before going live. Because OMB, for example, and our office are getting much, much tighter on having your records retention schedule in place. So make sure that you talk to someone about, specifically Kathy's office, about getting this thing set up.

For example, some of the risks I guess associated with retention issues: The longer you keep something, the likelihood of that being accurate goes down. It's not going to be helpful to you 75 years on, some event that occurred way beyond. We're talking about obviously different types of information for different systems.

But it's not helpful to keep the information longer, because not only do you have an accuracy issue, you also have a misuse issue because, just as someone said earlier today, if you keep it you've got to protect it somehow, and that means resources, that means potential risks associated with just simply possessing the data.

So records retention is not simply just how long you keep it. It also has to do with accuracy, it also has to do with data misuse and things like that. So for example, in our hypothetical you could say, okay, we've outlined we need to keep this information for five years. Why? Why do we need to keep it for five years? To ensure that the individual can access the information if they're having a problem with their future background check. Why? Because that's fair to the individual, but it's not so long to be unfair to the individual to just hang onto their information without any great cause.

MS. RICHARDS: In a lot of cases there will be general schedules that already exist, so you won't have to actually go through the whole process of scheduling it, so the answer should be somewhat straightforward. Some of the different components also have records retention individuals who can answer these questions for you.

Internal sharing. Here we are asking you what are you -- what information are you sharing and with whom internally within the Department. Here we're really looking for routine internal sharing. So within the Department, if there's a clear need to know and it's relevant and necessary for the mission of the Department, then the information can and should be shared.

But what we're looking for in these questions are the regular routine sharing that may be occurring. So for example, if you are U.S. Coast Guard and you're collecting information about port workers and you are then giving that information to TSA in order for TSA to do the actual screening for threat assessment and then TSA is giving the information back to Coast Guard to say these people are cleared or these people aren't cleared, those are the types of routine sharing that we're interested in, as opposed to the one-off instance of, this might on the face of it it looks like we have a fraudulent situation.

We're looking for those routine, regular sharing that is already set up and is regularly occurring in these situations.

Now, in this section -- today we're spending a lot of time on the privacy impact sections because those are the ones that are the most difficult. Those are the ones that we get the most questions about from folks. Much of these questions should be fairly straightforward for you to be able to answer as you're going through it, but you may not be able to -- you may not be able to identify what are the privacy risks and how have you mitigated them.

But when you're setting up and you're developing your system, you should already have thought through: Okay, this is the information I'm collecting, this is what I'm going to use the information for, this is where it's going to -- this is how long I'm retaining it for, and this is where the information flow: I'm sharing it from A to B to C to D.

Now, the question we're looking and the reason we're spending as much time on the impact section is that's the harder part. What's the impact to privacy? I know I need this piece of information to do X, Y, and Z, but we need to think about whether you really need that piece of information and, if you do or don't have it, what's the impact on privacy.

So from a privacy, from internal sharing, some of the privacy risks are going to be similar to the ones that we saw under use. So use of the information for undisclosed purposes. You share the information with another component, the component goes, oh, this is really good information, I'm going to use it for X, Y, and Z. It may be perfectly acceptable for them to use it for X, Y, and Z, but if you have never disclosed the fact that that's what it's being used for, that's where you start to have privacy problems because

you weren't transparent and you weren't accountable for how the information was used. So now you have these big worries.

This is why agencies as a whole get in trouble: they haven't disclosed what they were doing with the information. What happens is people begin to think the worst: Oh, we're doing all these horrible, evil things. We're probably not, but it was that we weren't straightforward and we weren't telling people what we were doing with the information.

So if you're using the information -- there was a question from this morning or from this afternoon in the first session saying: When I'm doing sharing, what sort of documentation or what do I do? You want to be clear with whomever you're sharing, what are the rules around the information-sharing, so everybody knows. People don't like surprises. So if your component number two wants to use it for X, Y, and Z, review your public documentation and make sure you can do that. If you're component number two in this instance, make sure you ask whether you can actually use the information for that.

Inappropriate or misuse of information, so again if you share it -- there's always this concern that you will have a rogue employee, as was asked earlier. You want to make sure that you're putting in some basic access and security and auditing procedures. This is where we begin to connect back to the FISMA conversations and the CIO conversations. Make sure you have those things in place so that the information is secure, not only against just losing the data, but also misuse of the data.

Then finally there's misconstrued data. This is where, if the information was collected in one particular context -- perhaps it was collected in an immigration context and now it is being moved over to some other context. You want to make sure that the people who are using the information understand the context of the information. You want to make sure -- and this can be mitigated by training the individuals on what that information means.

It may mean, immigration information may mean one thing here and it may mean something completely different in a Customs and Border Protection scenario. So we want to be very clear when we're using and sharing that information, particularly because DHS has many different components that are doing many very different things. So you don't want to have FEMA information being used in one way and not another. It comes back to the idea, is it relevant, necessary, and appropriate for the use.

MR. COLEMAN: Just to hammer home a point about internal sharing and external sharing, which will come up in the next section. Becky described about the introduction: Describe the typical transaction that occurs on your system. If you're engaging in internal sharing or external sharing, please give that as part of your introduction, basically describing what the typical transaction is with internal and external sharing partners, because if we get to the internal sharing and external sharing and, bam, all of a sudden you're sharing it with FBI, CIA, and someone else, and we didn't know that in the introduction, that's not helpful to us because now we have to backtrack and make sure everything else in the PIA matches up with the information you get back from CIA or you get back from FBI.

So this really is helpful in that it outlines specifically who you're sharing, whether it's authorized, whether you have an understanding with them. But also make sure to mention this type of thing in the introduction because this gives a whole picture of what the typical transaction and basically what your system is doing.

MS. RICHARDS: External sharing. First a word of caution. If you have a system of records notice or you're developing a system of records notice, do not list the routine uses in this section. I am interested in -- if you really feel the need to, then summarize them. But don't list everything that's already in your Federal Register. Give us basically the high level answers to those. Don't just list those routine uses.

Now, information can be -- you want to simplify the routine uses. You want to be clear with them. So for example, if you're sharing the information in our example with the FBI, let's just say we're sharing the information with the FBI. Your routine uses may also have other things that are routinely done, but the majority of what you're doing is you're sharing information with the FBI to do the background check and the commercial data aggregator for the address verification in our example. Those are what you're using the information for, so that's what you want to really spend your time on.

The system of records notice can deal with the specifics of the routine use. Simplify it and parse it.

Similarly, if for example you have a screening system and you're sharing the information with the Terrorist Screening Center, this is where you want to describe it here and you want to make sure, as Nathan said, that in the overview you actually said that

and that you've collected, you've stated that up when you asked what information was being collected. I'm collecting information back from the Terrorist Screening Center. You want to go back. You want to make sure that all of those are in there.

Now, if you go to your worksheet, one of the questions we get is: With which external organization is the information shared? Well, in our case you want to make sure that you're -- just answer the question. Still, it's not a trick question. It's a very simple answer: I'm sharing it with the FBI and commercial data vendors. Straightforward, not a lot of question. It's not a trick question. Be straightforward and we'll all be a lot happier for it.

The next question is what information is shared and for what purposes. This is question 5.2. Again, you want to think about what are we sharing and with whom. You can just do it, fairly straightforward: FBI, I'm sharing name, data of birth, and fingerprints for criminal history check. Simple sentence, very clear; we're good to go.

Similarly, commercial data vendors; sharing full name and address for address verification. You've clearly stated what you're sharing and for what purposes. We're not looking for a whole long -- we're looking for it to be concise and we're looking for it to be specific to what you're doing.

Now you get back to our privacy impact analysis section. We're going to have -- and it's okay. You're going to have some overlap in these privacy impact analysis sections and that's normal. Section 2.0, section 4.0 -- 2.0 is uses, 4 is internal sharing, and 5 is external sharing. These are all going to start to -- you're going to have some more ones and you're going to want to take mitigation strategies that are similar.

You also, if you for example say one of the privacy risks that we had was inappropriate use of the information and you go into the access and security requirements, you can absolutely reference those. Nathan mentioned those, but each of these sections is meant to work together. You need to think about them together.

So what are the risks from internal sharing? The first would be the information isn't secured by our external partner, so we've given the data over to the FBI and the FBI for whatever reason decides not to secure it. That is a serious situation. Mitigation would be that you have written assurance from your external partner that they are securing the information.

Another way to mitigate that is to actually have the organization not maintain the information. So you send over a query and they send back an answer and they don't maintain the query. This mitigates quite a few risks in this case. The FBI can't -- doesn't need to secure it except for whatever the transmission line was. You don't have to worry about them using it for some purpose that it was not intended for when you did the original collection. And you're also stopping them from having the ability to inappropriately use or misconstrue the information.

So you want to think about, when you're developing these sharing agreements, what makes the most sense. There are other instances where the FBI may need and you may want them to have that and maintain that information. But you want to think about what makes the most sense as you design the system and think about how you can mitigate the privacy risks.

Again, the privacy risk with external sharing is your partner loses the information, your partner doesn't secure the information, they decide to start using it for some other purpose. That could be rather serious. Or they have inappropriate use by that one, so again it was collected under an immigration, FBI is now looking at it from a different perspective; it now has two different meanings because certain words may mean different things to different people. So those are the things.

You also want to, if you're doing external sharing, you want to have some sort of written agreement so that everybody knows how the information is being used, so party A and party B all agree this is what we're doing, so party A can't say, oh, oh, you can't use that, and they always were using it.

We want to be clear, we want to be transparent, and we want to be accountable. The way we do that is we write these in the documents, we make sure all of our partners are clear.

MR. COLEMAN: Additionally, an extra note on the MOUs. It is up to you as a DHS employee and the system owner to make sure that your sharing partner, external sharing partner specifically, is living up to its end of the bargain. So as an auditing measure or as part of the contract or whatever MOU or agreement that you have with that person, it is up to you as the system owner in the Department to make sure that information, what the MOU says is what's actually going on. That's a very serious thing.

MS. RICHARDS: I'll just go back to, you want to make sure everything is the same all the way across. So whether it's your sharing, your SORN, your PIA, your PTA, your OMB-300 submission, all these documents need to say the same thing because that's where we get in trouble or that's where we begin to see problems with privacy, because you said you were just collecting information to do a background check and the next thing you know all that information is going somewhere else and doing something.

That may be fine, but if you haven't documented it the public doesn't know and we are held accountable for whatever is in your PIA and whatever is in your system of records notice and any other public documentation.

MR. COLEMAN: Notice. The section on notice basically -- it basically describes itself, but I want to be a little bit clear about what some of the questions are actually saying. What type of notice are you providing? Is it written notice on the actual application, for example, or the background check paperwork?

Does that notice clearly define what information is being used, by whom it's being used? For example, does it define all the uses? Does it define who that information is going to? The individual who is giving you the information or the organization from which you receive that information needs to know what you are going to do with the information.

Going back to the MOU issue, you need to outline and have an idea and have something to say to the individual who's information you're collecting. That is the primary privacy and oftentimes very initial privacy concern, does the person know that you're collecting their information? If not, you may have a serious issue if you're not giving the particular notice.

For example, if your system has a SORN that's one particular form of notice through the Privacy Act. Also you can have a Privacy Act statement on the actual form that the person is providing information on. Additionally or furthermore, if your system does not have a SORN or doesn't need a SORN, the PIA itself may serve as that notice.

Ideally you would have notice if you are collecting information, but the PIA itself, being publicly published, that PIA serves as notice right there that this is what we're

doing and this is what we're sharing and this is what we're collecting and this is why we're doing it.

Just a notice on the system of records notice, some systems out there are functioning under legacy system of records notices. Make sure that you as a system or you as a program, make sure that that system of records notice outlines exactly what you are doing today, because when that system of records notice was drafted it was most likely accurate, but today ensure that it is accurate because it's a serious, serious issue if your system of records notice does not reflect exactly what you were doing and exactly what information you're collecting.

So for example, other issues in notice: Does an individual have the right to decline to provide information? Okay, now I know what you want to do with it; can I say no to providing that information? It's quite possible you could have a situation where, no, you don't really have the right to decline to provide information. There be criminal -- in a law enforcement environment or an intelligence environment, no, there is no right to decline. Maybe there's not even notice given to the person.

It depends on the type of system that you conduct. But if you're dealing with the public on a regular basis it's quite likely that you're going to have formal notice procedure given.

Furthering the notice issue, and I think I mentioned this before, if they have a right to decline or whether or not they have a right to decline, does the individual know exactly what uses the individual -- that the DHS is going to be using it for? So for example, when we look at the privacy impact section, you want to talk about the notice you provided and why it is sufficient, the critical analysis of why it's sufficient.

For example, parts of DHS -- CIS for example deals a lot with the public, so they, ideally they're giving robust notice each time they're collecting information. Now, what they want to say in this section -- you see: "In some cases your organization may choose to provide notice beyond the PIA" --

MS. RICHARDS: Slow down.

MR. COLEMAN: Sorry.

In order to help individuals understand maybe how they could correct the information that's collected or to make sure to give the proper information straight up front. Basically, we want to make sure that they know.

So a typical impact analysis would be helpful to read: During this review we identified that, yes, we needed a system of records notice under the Privacy Act. Additionally, by conducting this PIA we found that the system of records notice wasn't quite adequate to capture all the uses that we were using the information for. So we decided to give more robust notice directly prior to collection.

MS. RICHARDS: You may also in this section -- this is the section that also deals to a certain extent with some of the redress processes. So this mixed with this next section having to do with individual access, these two are going to work together. So you may have -- TSA has a more robust redress process and so they refer to that in the notice section to say: There's additional notice about -- we've provided additional notice about redress. You can find it on our website. We've also outlined it in the redress process.

Part of the notice process is not only the fact that you are collecting the information, but what if any redress processes an individual has based on the information collected.

MR. COLEMAN: Just dovetailing off what Becky said, section 6 and section 7 work very well together, in that if an individual knows about the collection they can ensure that their information that you have collected is correct. So an individual, they have a right to access -- if they have a right to access the personal information, regardless of whether you as a component directly collected it, whether you got it from a commercial data aggregator -- maybe they don't have the actual right to access your system, but they do -- it is important to note whether or not they can correct their information, what procedures they should take for that.

There's two specific statutes that come to mind. The Privacy Act allows for an individual to see what types of records the Department maintains on them, as well as the Freedom of Information Act is a very powerful disclosure tool.

In this section what you want to do is outline what your procedures are, who to contact, who is your FOIA component specialist, what is your FOIA document request procedure.

Becky, can you go to the next one.

There you go. A typical, you want a name. I am CIS, I am CVP. Here's our FOIA division and here's how to contact them.

The FOIA statute applies to all the Federal Government. So it doesn't matter what you think of your system, the FOIA applies. FOIA has its own specific exemptions and things that you are allowed to retrieve by yourself, but this is a very direct access measure to your records or to another person's records.

MS. RICHARDS: In most cases we're not necessarily giving -- we're not giving you the answer to the question. This is the only one. We're giving you the answer to the question. What are the procedures? FOIA and Privacy Act. You may have additional information that you want to add. You may have exemptions, as was noted I think sort of very much in passing, but by Eva Kleederman earlier today. If you have a Privacy Act system of records notice and you have law enforcement or intelligence information in them, you may need to do a notice of proposed rulemaking to exempt those systems from being FOIA'ed or from the access provisions of the Privacy Act.

But everybody has the right to FOIA. You can then in turn say: We've exempted the system, you don't get the information, or whatever the appropriate response is. But this one, pretty much most PIAs are going to have the same answer.

MR. COLEMAN: Just to carry on, if you have additional procedures, as Becky just said, make sure to mention them. Like for example, if you provide web access for people to alter their information to make sure it's up to date, like if you're a first responder for FEMA or something like that, you want to make sure that they have your most appropriate information and there should be measures in there so people can access their information, make sure it's accurate and things like that. That's mission-critical type information.

MS. RICHARDS: The privacy impact section of this is basically going to say something along the lines of: Individuals may be provided access under the provisions of the Privacy Act of 1974 and FOIA and individuals seeking information should go through this process. Then again, I'll use TSA as the example. U.S. VISIT is another one. They have redress processes in place that are additional to these particular ones to help people go through that process.

Part of your analysis in this section should be, do I need additional redress processes? Is what I am doing -- am I determining whether or not there's a benefit applied based on this? Do I need to have additional ways in which can seek redress because the Department is making perhaps a decision about them?

You need to think about that. You'll work with our office and we'll work to come up with what's the appropriate level of redress or access that's provided based on what your program is doing.

MR. COLEMAN: Technical access and security. Some of you in this room are security officials. Some of you maybe are financial officials that have been tasked in OMB-300 to get the PIA done. This is a major section as far as privacy concerns go. You want to make sure that, if you're the program manager, for example, that your security official is directly answering these questions.

These answers need to be specific and they need to be well documented. So in this section, if you're following along in your guidance, we're talking about roles, the privileges associated with those roles, are those roles and privileges documented in some formal procedural manual or something like that. What are the auditing procedures is a major question. Can you go back and make sure that people are not violating the privileges or stepping outside of what they are? What technical solutions have you implemented to make sure that those things are done and they are done on a regular basis?

This is just with the VA issue and several issues that have gone on in the last two or three years, making sure these policies are in place, dotting these i's and crossing these t's is a major, major issue. Now, I know through the C and A process a lot of security officials are already addressing these issues and we've gotten some fine responses on PIAs. But I want to make sure that it gets hammered home. This is really important.

This is where Mr. Hawley was talking about this morning, security and privacy are not diametric opposites. They are in fact a partnership. You cannot have good privacy without security and you cannot have good security without some privacy protection.

So this section and the proper analysis section, in the analysis section, you want to document: We defined these roles for specific purposes because this is how we designed

our system and this is what we envisioned the system to do. In addition to that, we do a regular audit every three months to make sure. If a breach occurs, we have this sort of plan in place. We want to critically analyze where you saw the risks in your security plan and how you mitigated those risks for future breaches or for future misconduct by employees or contractors.

MS. RICHARDS: Now, in this section you want to remember that this is related again to, you're going to have probably referenced these sections in your discussions earlier regarding the use and sharing, because that's where you're going to have the -- you're going to be able to control both use and sharing by having good security controls put in place.

So you want to think about-- when you're answering these questions, you want to make sure that you're thinking back to, did I actually put in roles that made sense based on the appropriate uses of this information? Do I have appropriate auditing based on that?

The other is, you want to make sure you're actually doing this. So it's one thing to answer, oh, yes, I have role-based access. Make sure you actually have role-based access. Make sure that you're actually integrating it into the program. If you're a security official -- if you're a security manager, make sure you're working with the program manager to show that, for example, you have access to X number of information for 100 employees, but when it gets more sensitive only 25 have it, because if you say you have role-based access and somebody comes back in to audit it and everybody has roles and everybody has access to the same information, then you haven't actually implemented the privacy and security requirements that you need to to secure the information.

So you want to make sure -- this is where the rubber meets the road -- that you're doing what you're saying you're doing and that the security is actually matching what the privacy requirements are.

MR. COLEMAN: In addition, just to add onto that, going through the security measures, the risks are sometimes quite easy to identify because programs or -- or they're easy to spot because if that is your area of expertise you know where the risks are and you're used to identifying them in the business plan or system security plan.

I would consider this one of the easier ones to write if that is your area of expertise, because, okay, well, we identified these risks and here are the policies we have in place, here are the procedures that stem from those policies, here are the technical measures that we have implemented to mitigate the potential security risks.

MS. RICHARDS: Section 9, how did you make your technology decisions in light of privacy protection? In some cases this, like the privacy impact assessment section, are the most difficult. But they also should stem from the fact that you began this process as you were developing the system. So you made certain choices and some of those choices should have and were based on the privacy decisions that you made.

This last question, you need to describe how you made those decisions. So in this last question, this is basically the conclusion of your PIA. This is what we're doing with our system, this is how the technology supports the system and the program, and this is why we're doing it.

Then this is slightly different, though, than your conclusion for the entire PIA. This is just talking about the technology and the conclusion for your PIA is more about how the technology is supporting the entire program.

From here we get to our conclusion. Now you've written your PIA, you have a short description here of what were the privacy risks you took and how were the mitigation strategies. It's broader than the question previous about technology. Here it is about what did you do from the program perspective. This is how the technology was put in place and these are maybe the policies and procedures you decided to put in place, and this is the training you decided to include.

So from a technology perspective, you're looking in part at what you've said in answer 8, which is that we decided to employ this type of technology with this type of backbone, it had encryption, it had security and access controls, etcetera. Then you get to your conclusion and you say: In addition to the technology we chose, we also have put in place the following redress processes, we've put in the following policies and procedures to ensure that our employees are well trained, they know not to misuse the information, that there are penalties associated with it.

At that point you are done with your PIA, and now all of you are very happy.

What's the review process? This was asked earlier. If you have questions, we're going to -- if you have more questions, just pass them. I know we've been collecting them.

The PIA review and approval process. Send them to pia@dhs.gov. You can send them directly to Nathan or myself. We will review and provide comments. An important part: No response does not equal approval. So if you have a PTA, you uploaded it into TAP and it has no comments in it from us, that doesn't mean we liked it. It just means we haven't looked at it. Feel free to call us. We are, similar to you, we are all resource-constrained, but we are working very hard to make sure we're reviewing this.

So if you need something, call us, email us. We're there to help you guys. It's a multiple collaborative iteration. Your PIA isn't going to get approved the first time you send it to us. At least it hasn't happened yet. Maybe after today's training it will happen. I would love it. The reality, though, is sometimes it just helps to have a second set of eyes look at what you're doing and ask you, well, do you really need that piece of information, or what are the real uses, or have you put this in place?

Once the PIA is -- once the compliance department and the legal department within the Privacy Office feel comfortable with the PIA, we will ask you to submit it to us formally. What that means from your side is that if we were working with the program level people, you may have approval processes on your side that you need to go through before you're ready to send it to us officially, because the final process is Maureen Cooney, our Acting Chief Privacy Officer, will review the PIA and she will approve it, and then 98 percent of these are published on the website, www.dhs.gov/privacy.

Most of these are going to be made public because, again, what is the PIA? It's a transparency document, it's an accountability document, it's a way we begin to build trust with the public. So most will be published on our website.

MR. COLEMAN: A quick note. In the beginning of this process it's important to let us know what your timelines are. If you plan to begin your pilot and then 30 days later you plan to go live if everything's kosher with the pilot, we need to know that, because if you're sending us a document the day before you go live with your pilot at least, that's not going to work.

Just because it came out of your office, we also have to have some review time as well. So let us know your timelines beforehand because it will only help us all in knowing what expectations to have of timelines, of product, of productivity in general.

MS. RICHARDS: It's a collaborative effort to finalize, to write and finalize your PIA, to ensure that privacy is integrated into your system. We're here to work with you, but we also -- we need some time to review it. We have the entire Department we're doing this for. So just keep that in mind.

You also all have some type of privacy person in your component. If you are a component, whether it's CVP or CIS or the other ones, you need to work with your privacy officials before you send us the documents.

With that, Ken's back to ask us questions.

MR. MORTENSON: Some technical questions now, surprise surprise. The first question is: Section 1.4 asks what specific legal authorities, arrangements, and-or agreements define the collection of information. Can you describe how one would answer that? What would be an answer that one could use, and some examples?

MR. COLEMAN: There's a couple of different ways you could approach that question. For example, in a rulemaking, Congress has said to do this and this is what we're doing. That's pretty darn specific. We have been specifically asked to do this.

MS. RICHARDS: And you give the law. ITSA. I don't know what "ITSA" stands for.

MR. MORTENSON: ITSA?

MS. RICHARDS: ITSA, one of those. There is a specific law. There are a variety of specific laws. It could just be the Homeland Security Act, section blah, blah, blah says.

MR. COLEMAN: If it's a little more vague than that, if you have not been given specific authority to do this, you know, person X, go do activity Y, you would want to cite your enabling statutes -- the Homeland Security Act, statutes that predate the Homeland Security Act before the merger occurred. Those are the types of things that enable you to

do what you're doing. You're not just doing what you're doing willy- nilly. There's a statute, statutory authority that came from Congress for you to conduct this activity.

MS. RICHARDS: Your activity -- the mission of the Department is to do X, Y, and Z, and you better be building your technology or you better be doing your rulemaking to further that mission. If you can't find that, then we probably should all have a little more conversation.

MR. COLEMAN: It could be a treaty.

MS. RICHARDS: Yes.

MR. COLEMAN: It could be anything like that. We deal a lot with international partners. It could be a treaty and that according to the terms of that treaty you have initiated this system to comply with DHS's and United States' portion of that treaty. That's what you say.

MR. MORTENSON: A drafting question: You have emphasized that you should not omit any sections. However, what if there is a need or it seems appropriate by the drafter to condense the answers all into kind of one thing?

MS. RICHARDS: Don't do it.

MR. MORTENSON: Okay.

MS. RICHARDS: Don't change the template. We put the question there for a reason. If your answer is "not applicable," that is okay and we understand that. But if you start to moosh this together it makes it more difficult for us, it makes it more difficult for people in the public who may be reading these. It's easier if everybody has the same template and we go through the same process.

It's a systematic process. If instead we're just randomly choosing not to answer some question because it didn't seem to quite match your program -- if you have an honest question about, I don't know how to answer this question, or here's sort of my answer, how do you think this would best fit in, that's when you want to contact us. Or you can put a note in the PIA as you're drafting it: Privacy Office, look at this; this is sort of what I want to say, but I'm not sure if it answers this question or that question.

MR. COLEMAN: On top of that, your responses are going to be redundant and they are also going to link to other sections. It's a comprehensive analysis. It's not intended for each section to be on an island. You're going to say things over. You're going to cite your technical access and security measures probably two or three times at least. That's okay. Being redundant is okay. We would rather you be bored than stymied, I guess.

MR. COLEMAN: Actually, from a process standpoint I would like to emphasize, do not change the template. They call me "Font Man" in the office because I'm the guy who looks at the templates and looks at somebody who has cut and pasted something in in a different font.

The reason why I'm so crazy about that is, one, DHS has specified -- not us, not the Privacy Office, but DHS headquarters has specified -- a particular format for publishing these sort of documents. We have to follow that format just like everybody else has to. If you change the template you're adding a lot of processing time on our end to make it available to go onto the web. So that makes Nathan and Becky not happy people.

The other thing is that the things are put together in a particular way so that you can put the answers in much more simply than having to just cut and paste things in. It really makes life easier just using the template straight up.

MS. RICHARDS: The other is, don't read too much into these questions. A simple answer is fine. Two sentences that answer the question, what information you are sharing, is fine. You don't need to rewrite the entire book. You will repeat, but it's okay.

MR. COLEMAN: I guess another thing is don't be afraid of what your system does. Just say it. If it's sensitive, we obviously already know that and we're working with you on how to develop the PIA appropriately. But don't be afraid to just frankly say what exactly your system does.

I guess it goes back to 1.1 we discussed. You'd be surprised what kind of answers we get because people aren't really comfortable, it seems, saying exactly what they collect, this is exactly what we collect. So don't be afraid.

MS. RICHARDS: Somewhere there's a form that somebody filled out that says: We needed these 12 pieces of information.

MR. MORTENSON: There's a next series of questions that I'm going to kind of group into one thing, which is trying to distinguish a PIA from a SORN. I'll kind of begin this and let Becky kind of talk about the details of it.

They are two different beasts. Just because you have a SORN does not necessarily mean you have a PIA. Just because you have a PIA does not mean you have a SORN. The rules and procedures under each set, that is the rules for how you go about it, what do you have to provide in a SORN, what do you have to disclose in a SORN, as opposed to what you have to do or disclose on a PIA, are very different.

So you may have certain redundancies between the two. There may be certain answers that you can do in a SORN that you will also use in your PIA. But they are not necessarily the same. So think of them in some ways of being independent. However, they are a connected process because we're talking about personal information. Just in one set we're looking at how is it put into a particular system, in the other set in terms of the privacy impact what is the impact of having that information.

I'll let Becky continue.

MS. RICHARDS: If you remember from the afternoon -- from the previous one where I had sort of the map of the different documents, the PTA, the C and A, the system, the PIA, and the SORN, remember, the SORN is somewhat more of an umbrella situation. The SORN is almost always -- it's going to at some point in its existence have a PIA associated with it. It may not be at the same time because you may still be developing the system, but the system of records notice is such that you need to, if you remember from OMB, you need to have that out at least 40 days before you're ready to go live.

So you may still be writing the PIA. The PIA needs to be done -- it needs to be done before you go live. The SORN needs to be out 40 days. Nonetheless, those two documents are going to at some point come together. There.

MR. MORTENSON: A question about personally identifiable information: Would that include derived information, that is information that came from other information

that was an analysis of the report, such as basically some sort of determination that was stored in a system by a component, for example a naturalization decision?

MS. RICHARDS: Yes.

MR. COLEMAN: Absolutely.

MS. RICHARDS: Absolutely. Any information that you're -- remember, if you just have an answer and it's not associated with anything, it just says yes, that's not personally identifiable. But if it's connected to me that, yes, I can now be a citizen or yes, I can now do something, or the green light has shown up on my address verification, or any of those things that come back into it and are associated with me, it now becomes personally identifiable information.

MR. COLEMAN: Think back to the data- mining question and the uses question. Have you enabled the tool to make a decision or make an analysis about someone and it is applied, just like Becky said, to that person? Well, yes, you have, and what you want to do is outline in the summary and introduction that this is the basic function of the system or this is part of the functions of the system and outline that in section two and the other relevant questions, this is a data element that we collect and this is why we collect it.

Whether you've produced it through your own system or not is not particularly important to that aspect. You've now produced a new piece of information about someone. It doesn't exist in a vacuum. It exists in your system.

MS. RICHARDS: The other thing I would add is if you have commercial data coming in or if you are working with a commercial data vendor of any sort, that information, whether it's a query that goes out and comes back with the answer or if it's just a query that goes out, you need to make sure that that's being described in your PIA, and it likely, if you need to do a system of records notice, should also be part of that discussion.

MR. MORTENSON: A couple questions here asking the question: When should we do a PIA? The first one is: Should we do PIAs for non-IT systems?

MS. RICHARDS: I'll go back to my answer from this morning. It depends. You probably -- most programs are going to have some sort of IT system that's underlying

whatever it is they are doing. There will be some type of technology associated with it. But if you're sort of thinking about it from a budget process, OMB-300s have IT submissions and non-IT submissions.

Your non-IT submissions probably still have some sort of backbone technology, but the technology portion was not high enough to rise to a certain level that takes it to an IT one. Those subsystems or systems that are existing in that particular class are still systems, according to Bob West and according to us, and still need to go through the PIA process -- the PTA process at a minimum, and then a PIA process.

The areas where that isn't necessarily true and you can do -- we can discuss that, but if you have like a radio, you're buying a bunch of radios for FEMA or you have a phone, those are the things that, hardware that's physically -- servers -- those are the things that I actually don't care about.

MR. MORTENSON: Let me just answer that real quick. From the Privacy Office's standpoint of looking at privacy in a holistic sense, you might still want to come and talk to us. You might not have to do a PIA, but we might want to think about perhaps putting together procedures -- the radio example is a very good one -- of making sure that when we have training for the employees or the contractors that we make them aware that, okay, you're using a radio, this information is not going to be encrypted, it's going to be transmitted over a radio frequency, which can be picked up by anyone; you should not be talking about personally identifiable information. I shouldn't be saying over a radio: Oh, the person's social security number is X.

Those sort of things, while not necessarily requiring a PIA, might be a good time to think about appropriate usage, acceptable usage, implementation standards that impact privacy. That's one thing we would definitely be very happy to work with you on.

MS. RICHARDS: Because you may also want just to develop training around those particular items. What we want to avoid is the Department looking like we aren't sensitive about privacy. So the exact example of somebody sort of over the radio saying, I have this person here and their social security number is X, Y, and Z, do you have their documentation over there -- there may be a reason you want to do that, but we want to think about it, because the last thing you want is for someone to show up and say: Hey, DHS is screaming people's over unencrypted things over their walkie-talkies, this information.

MR. MORTENSON: Another question of when is: Are PIAs only necessary for programs that are reporting under Exhibit 300 or Exhibit 53?

MS. RICHARDS: Those theoretically should capture most everything. The exceptions would be --

MR. COLEMAN: Wait. Is the question directed at are OMB-300s and 53s the only ones who have to do?

MS. RICHARDS: Yes.

MR. COLEMAN: No.

MS. RICHARDS: No, you're right. So you may have a program that isn't -- you may have a specific program that you're setting up that isn't a 300, isn't a 53. Some of the things that we did -- TSA did a number of different threat assessment programs that they didn't have necessarily a 53 or a 300. It was they were screening this group of people, these port workers, for an interim period of time. That needs a PIA. It's not a 300, it's not a 53. It's a specific program.

MR. COLEMAN: Said more explicitly, there are 140-some odd OMB-300s we expect this year. Bob West's system inventory has high 600s, 701 or something like that, systems. Subtract the OMB-300s from that and that's how many systems might need a PIA as well, 550 or whatever.

MR. MORTENSON: Then in a previous question we were talking about whether non-IT systems require PIAs and you were mentioning how the backbone systems in terms of the client computers, the networks, the general systems that are there -- would those systems, just if it's a general system, the LAN, a WAN, would they require a PIA?

MS. RICHARDS: Those are examples of ones that need the PTA. So if you remember my -- and actually I think I'll just see if I can find this picture.

Those are the systems that need -- you'll go through a C and A. You need to do the privacy threshold analysis. But Nathan and I particularly like those, and Rachel does as

well, because it takes about two seconds to go: We don't have any personal information here; you're all set.

There we go. So here, that particular, the WANs, the LANs, the infrastructure network, those fall into this group. You do your C and A, you do your PTA, it's about three or five questions at this point, and boom, you're done, see you later, until you decide to make any changes to your system. And I'm guessing the WANs and the LANs aren't going to be changing systems to start taking in that information.

MR. MORTENSON: How would including log- in information affect your answer?

MS. RICHARDS: At this point in time, given all of the systems that need PIAs, we are not necessarily going to require a PIA at this time. However, we will capture your system in the TA-FISMA system as having employee-contractor information, and some day when all of us have finished all our PIAs then we can go back and do those ones.

MR. COLEMAN: Let me clarify. Just because your system may be associated with a backbone system and that backbone system relates to several systems that are within your component, what we are most interested in are the systems that utilize the personally identifiable information. So just because your system is supported by a LAN doesn't mean that the LAN needs a PIA. It means the systems that are associated with that backbone may potentially need a PIA.

The LAN is there for a foundation, but the other systems that are manipulating the data and generally intake-outtake, that's where our concern lies.

MS. RICHARDS: Some of the different components are doing modernization at this point in different ways. So some folks are deciding to do a -- have decided to build basically a backbone that provides security and access on the bottom, and they've a PIA on the security access that they are implementing, and then the information -- so we know that the information will be controlled and secured in this particular fashion.

But then the particular programs actually talk about their uses, their sharing, their collection. But then they refer back to the general PIA that's been done on the securing and accessing of the information. There's different ways that the components at this point are doing their modernization efforts and so that's just one example of different ways you might see that.

MR. MORTENSON: One section, section 9, question 9.3 says: What design choices are made to enhance privacy? Can you describe some of the ways that components or programs might look at things with regard to enhancing privacy from an IT perspective?

MR. COLEMAN: I'll talk about it for a second. You have a technical background, so maybe you can provide a little, flesh out the details.

For example, the first question, question 1, 9.1, says "What competing technologies did you evaluate?" Okay, well, we took a commercial off-the-shelf system, or we built the system from the ground up because these are the requirements we needed.

Okay, well, you've just told us what decisions you made to build the system. Now, in the last question you want to analyze that: Okay, well, this is the reason we did this. We built the system from the ground up because we couldn't find anything that was commercial that would really implement the security measures and the privacy protections that we outlined we needed in our basic system design.

I don't know if you could fill in some technical aspects.

MS. RICHARDS: You would also -- you may have decided that you wanted -- you may have had to make a choice between whether you wanted to spend the money on encrypting the information or not encrypting the information. If you had, for example, social security numbers, you probably want to have that information encrypted. So that would be something that you would describe and say: We made the decision to encrypt the following information in these instances.

You also will want to discuss, if you made decisions -- if for example the access, if the commercial off the wall -- "off the wall" -- off-the-shelf program didn't provide granular enough access rules, you may have decided from an access perspective that you needed to build some additional access requirements in. You may also have decided that perhaps you weren't able to give access through the web in a certain way and so you needed to make specific changes based on that.

You may also have decided that, for example, rather than using somebody's social security number as a user ID, you decided to use some number that was randomly generated. You would talk about how that works.

MR. MORTENSON: One small thing I would add to this. Actually, what Becky was talking about reminded me of a conference I was at back in April. I was talking with Jim Dempsey from CVT, who was on the panel, and he said that the Privacy Office shouldn't be Dr. No. If you come to us and say, listen, we have this mission requirement, we need to get this accomplished, this is important because of these purposes, we have provided the authorities under 1.4l, yes, there may be some issues with regard to privacy; we're not expecting things to be 100 percent.

We want you to do best efforts with regard to privacy. We want to make sure that the privacy protections are there. But this is not a situation where it's a balancing act. It is a situation in which we must maximize privacy while accomplishing the mission. So you can come to us and talk to us about it and we'll be able to work -- we're not expecting you to have all the answers.

We are here also to provide you with help from a technical standpoint. Actually, Peter Sand is standing in the back. Peter is our Director of Privacy Technology. Peter's job is to look at these things, to help you all out to understand what is available in terms of the technological solutions that can happen, or rather that can exist, what we might be able to employ, because you may look at things that you haven't had that presented to you.

Also in addition, there are certain technologies that even of themselves cry out with certain types of privacy concerns, things such as radio frequency identifiers, things such as biometrics, things such as identity management systems. There are natural issues of privacy concerning those systems, geospatial, other types of technologies that are there.

We've looked at those things. We've spent time examining those particular technologies. There will be new technologies out there. We're more than happy to sit down and talk to you. Please be free, feel free to call us, to bring us in. Certainly at the design stage is the best time.

I don't know who is left from Secure Flight, but I'd like to hold them up as an example of saying they have done that. They have made sure that we're sitting at the table with them as they're designing things so that we can say, hey, we've seen this particular technology, we think this is interesting, we think this will have privacy-

enhancing effects that you can accomplish with your security mission to the fullest extent while maximizing privacy for the citizens.

I just wanted to bring that forward.

Another question here. Basically it's a definitional question, which is: What does require a PIA? Is it a program or is it a system? Under the e-Gov it's a system. Under OMB-300 we talk about programs. Which is which?

MR. COLEMAN: Yes.

MS. RICHARDS: Yes.

MR. COLEMAN: For example, we have one, two, three systems that are building up this vein here, I guess. At this level we would look at the program level, so at this point we would talk to you and say: Okay -- there are people in the room where we've actually had this conversation with them. It makes more sense to have a single PIA for these several systems and basically on a program level and say, all your systems are essentially doing the same function in the sense that the output is the same or the product is the same from the privacy perspective. So this would be the program level and we did a single PIA on this program, but it encompasses these three systems.

In your introduction you would say: These three systems are encompassed in what we call this general program.

So yes, the answer is yes.

MS. RICHARDS: You should remember, at DHS we have the Homeland Security Act. So don't just look at the requirements of e-Government Act. Look also at the Homeland Security Act to sort of go back.

The other is, be careful about trying to sort of go on technicalities of getting yourself out of a PIA. If you're to the point where you're trying to say, well, I just don't want to do it because this particular definition doesn't work, go back to what probably in the long run is the best for your program and for your office and for the Department. Is it to do the PIA up front and think it through or is it to have somebody come -- or is it to be called up to Congress and say or have some staffer say, well, why didn't you do this PIA

on the system, and say: Well, when we were designing the system we thought that it was really a national security system and so we didn't do the PIA, but after we really got developing it in the system development life cycle we realized it wasn't.

You end up putting yourself into a much more difficult situation and it's not good for any of us. At the same time, I'm not looking for more PIAs to review. I mean, we have more than enough. So we're looking to come up with the most effective and efficient way to describe what we're doing within the Department and how we're dealing with the privacy risks.

MR. MORTENSON: I might mention that the one item or the one tool that exists is the PTA. The privacy threshold analysis is a very simple tool. In there, the current version has a definition of what is an information system and what is information technology. Those are guidance, but I would say that you might want to be expansive, because the privacy threshold analysis, you might want to read it and say, well, okay, let me just think that I have a system or I have it, it falls under this, and just answer the questions and see where I fall. Then if you have any additional questions or you're not sure, you can certainly speak to us.

As Becky said, just because you call us up doesn't mean we're automatically going to rope you into doing a PIA. We want to do a PIA when it is appropriate. We don't feel that a PIA is necessary on absolutely every system.

The next comment I have is: Becky had said, for those of you from DHS, we look at section 222 of the Homeland Security Act, that it gives -- the Privacy Officer looks at more systems than just those required under the e-Gov Act. I would also say, for those of you from other agencies, you might want to look at the enabling sections of the statutes for your privacy officer.

For example, for those of you from the Department of Justice, if you look at the enabling statute for your chief, the Chief Privacy and Civil Liberties Protection Officer, you'll note that there is similar language that expands upon what PIAs would be done on.

So that's why many other agencies, not just DHS, would be also looking at PIAs beyond necessarily what the e-Gov Act says.

Does anybody else have any questions at this time? Do you have any cards for us to pick up?

VOICE: I have a question. Aren't the risks the same for all the personal information systems?

MS. RICHARDS: The question is: Aren't the risks for all the information systems the same? The answer is there are going to be similar risks, but depending upon the particulars of your system it's going to differ. So a system that -- a system that is taking in information for a background check is going to have a certain level where the risks associated with that particular information coming in and the uses may be different than, for example, a system that is doing a -- is an intel or a law enforcement system that is bringing in different types of information.

You will have similar risks and you will have to -- as we discussed with you, when you weigh how to best mitigate it you will have to make a decision. So you may have with a law enforcement database, you may not have purely accurate information. But that may be less of an issue in that particular context than in the context of a background check about me and whether my employment is occurring.

MR. COLEMAN: So I guess, said another way, a risk by definition, yes. A risk by degree, no.

MS. RICHARDS: That's good, yes.

MR. MORTENSON: Actually, to build upon that, one thing I would say is there's another tool in our arsenal, if you will, for certain programs we've worked with. I would bring out U.S. VISIT. Steve Yonkers is the privacy officer there, and we've worked with him, that when we get to certain decision points within the system development life cycle we will do a privacy risk assessment.

Essentially what we're doing is we're stepping back and we're looking at the choices that we've made at that particular point. Now, this is something you could do. It doesn't have to be formalized. It's just something, you can sit down and get the team together and say: Okay, let's look at the technology choices, let's look at the program choices, let's look at the process choices that we've made. What impact, what risks from a privacy standpoint, from the use of information, from the flow of information, from the

exchange of information, what are those particular risks and what are the mitigations that could exist for those things?

So they help guide what's the next step, how should we change, how should we develop, how should we move forward with this particular program? So it's going to be dependent upon what the operation is that you're doing, what the mission is that you're trying to accomplish, where are you in the process, what particular information you're dealing with, and put those all together. You should be able to define what are the risks and what are the mitigations that go with those particular risks? How can you mitigate those things?

Obviously, the goal would be to reduce the risks as much as possible so that you have a highest level of mitigation at the end. So this privacy risk assessment is an opportunity to evaluate at checkpoints. But you can make up your own. It is not a formal process, but it's a point at which you say, hey, we're going to choose a particular technology. Do we want to go with iris prints, do we want to go with fingerprints, do we want to go with some other biometric? Let's sit down and let's look at each one of those and what the impacts would be and understand what the risks will be from a privacy standpoint.

Yes, sir.

VOICE: (inaudible).

MR. MORTENSON: Well, some of them I was going through and obviously I was trying to consolidate them into single questions. I apologize if -- if there was one I didn't answer or ask specifically and you feel it wasn't answered, feel free to ask it right now.

VOICE: (inaudible).

MR. MORTENSON: One comment I would --

MS. LEVIN: Re-ask the question.

MR. MORTENSON: -- make to that is that that is a different process, because what you're talking about there is a system of records --

MS. LEVIN: Can you re-ask the question?

MR. MORTENSON: I'm sorry. The question basically was -- and correct me if I get it wrong -- in the PIA analysis there is no requirement or there doesn't appear to be a requirement dealing with providing notice as to the disclosures of information made about individuals, to let individuals know who the agency has disclosed information to or about whom they've disclosed information, as there is under the Privacy Act of 1974.

I would say the simple answer is the Privacy Act of 1974 took care of that. If I have a system under which information is retrieved by some identifier, I must have all that in there as well. Part of the evaluation of the PIA may also look at those particular processes if required, if the system does need a system of records notice.

The PIA itself isn't looking at the same, if you will, issues as the Privacy Act. Rather it's looking at the particular impact. So we want to evaluate that from a more developmental standpoint to understand what the system is doing and how does that impact the privacy system.

Now, it may be that the impact comes back and says we should have a system of records notice and we should put in place those particular processes such that we do have a disclosure operation. That is a result that could occur from the PIA process. But it's not an inherent component of the PIA process.

VOICE: This is like the -- the example you brought up earlier several times was, don't wait until the day before you go to bring up an issue. If you don't -- if the law requires you to be able to account for disclosures and you know you're disclosing information to other agencies, and you wait and you don't even discuss it in your privacy impact assessment, you're not thinking about it, and you're therefore not thinking about how you design that into the system as something that has to perform.

MS. RICHARDS: In the PIA you do actually describe who you're disclosing the information to for external and internal. That is one of the aspects of the questions that you would ask.

VOICE: But in a general way. The question is for each particular individual's information. How are you keeping track of the fact that my information, as opposed to 15 gigabytes of information, were provided to another agency? There's a difference between

15 gigabytes and my information. When I ask, when I come to you and say, who did you share the information with, I don't want to know you shared 15 gigabytes with something, with another agency. I want to know that you shared my information with another agency.

MR. MORTENSON: My answer to that would be if we do have a system like that and it's sharing your information which is being retrieved by an identifier, we should have a system of records notice. That should exist, so therefore --

MS. RICHARDS: And you have --

MR. MORTENSON: I'm sorry, Becky.

But that process should be there. The PIA should call out to us, and it has on occasion when we've looked at it, and said, hey, we have a system here that is collecting this information and we're retrieving it by an identifier and we're exchanging that information, therefore we need a system of records notice, we need to put in place all the Privacy Act system parts of it as well.

So it provides us with the front end notice to do that particular activity.

MS. RICHARDS: You also have the auditing portions of the questions asked here in terms of the security and access requirements. So you want to -- if you identify that the system of records notice is needed, then you need to think about some of the risks that are going to be associated with it. To a certain extent, are you able to meet these requirements as related to the Privacy Act, and this is how you've handled those.

MR. MORTENSON: A PIA, just because we say you've got to do a PIA and you do a PIA, does not mean you have satisfied all privacy requirements. There still is the Privacy Act out there. What I'm saying is they are independent, though, that the privacy -- the e-Government Act does not drive Privacy Act systems, just as Privacy Act of '74 does not drive PIAs.

But there is a very close connection and certainly if I have a system that I'm transferring your information out of that very likely will need a system of records notice and I will have to set up all the requirements under the Privacy Act. I agree with you absolutely.

MR. COLEMAN: The PIA is an assessment tool. It's not necessarily a panacea for all your privacy issues.

VOICE: I terms of writability, I guess, an expansive reading of section 8 would lead me to regurgitate my entire technical control section from the SSP. Conversely, I don't really want, since the PIA is a publicly accessible document, I really don't want to tell the public everything I'm doing to protect my system.

MS. RICHARDS: Absolutely. I don't want you to regurgitate everything that's in your C and A. So let's go back to, a sentence or two or three is likely to answer the question. So thank you for bringing that up. I don't want to see your whole C and A. I don't want to see all your routine uses. Those are already covered in another document. You do need to refer to them.

One of the specific questions under the PIA is: Do you have an authority to operate under FISMA and, if so, what's the date, and all those good things. So that's sort of part and parcel of it.

MR. MORTENSON: One thing I would add to that: There may be certain types of systems where the information we don't want to disclose, but it's necessary to answer the questions. We don't have to disclose all that. If there is a security reason, if we don't want to tell people how a particular security system works, then obviously that might need to be reported to the Privacy Office for evaluation for the PIA, but it might be redacted from the published version.

One more question and then we're going to finish for the afternoon.

VOICE: Thank you. This is a follow-up to that and an upstream-downstream question. A program that uses data in the upstream files for the PIA and files the SORN and then gives more information to downstream agencies -- in the case of Secure Flight, we will use watch lists, compare passenger information, and then we will forward the results to TSE, for instance, who owns the TSDB, makes the adjudication, and then they go ahead and dispatch law enforcement.

So everyone is touching passenger information. Secure Flight, TSA, files for a PIA and SORN. But is it true that we cannot go operational until TSC and all the other law enforcement agencies also finishes their PIA and SORN?

MS. RICHARDS: No.

VOICE: That's not true?

MS. RICHARDS: No.

MR. MORTENSON: From a policy standpoint, the requirement doesn't exist. However, from a practice standpoint you want to make sure everybody that is part of this entire process is thinking privacy. So if your partner that's outside the agency -- we can't adjudicate TSC. We have no authority over TSC. So we can only adjudicate a DHS program.

There will be points at which, though, DHS programs touch other programs, very, very, common, especially in the information-sharing environment. Those sort of things are going to occur. Part of that I will say will be solved. The President has tasked some groups to look at these particular issues so we can figure out how do you do privacy as between systems that are sharing.

I think it would be a good practice and certainly we in the Privacy Office will work with you to get your partners to be aboard with that. I would certainly say in working with private sector partners -- I can't think of an example off the top of my head right now -- but where we are exchanging information now, we want to make sure that the private sector folks are abiding by rules as strict as what we have to abide by.

Going back to what Becky said a little bit earlier, just because you use a contractor doesn't mean that they necessarily get out of the requirements. But likewise, even if we're sharing information now, we want to make sure as we share that information that the protections and the controls on that information do flow with it. That's from an information-sharing arrangement probably what you would probably want to do in that situation. I can't imagine that the OCC is going to allow you to exchange information without having an MOU that has built into it privacy protections that will say you will abide by the same level of protections.

So from a simple answer, no, we can't enforce it onto them because we don't have authority over them. However, from a process standpoint very likely that's going to exist because we're going to have some sort of agreement with the partner that puts those protections in place to ensure that they have that.

All right, we're going to finish this up for this afternoon. If anyone has any other questions, I certainly invite you to email us at pia@dhs.gov. Also indeed, you can call us at the Privacy Office. The main number is 571-227-3813.

I want to thank everybody for coming today and staying through a very long and hot session. I certainly appreciate your time and thank you very much.