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

PANEL II
COMPLYING WITH FEDERAL REQUIREMENTS FOR PRIVACY: SORNS, PIAS, C&A, AND OMB 300

Moderator:

Hugo Teufel

Panelists:
Eva Kleederman
Elizabeth Withnell
Bob West
Barbra Symonds

MR. TEUFEL: Good morning. If you could take your seats, we'll resume with Panel II: Complying with Federal Requirements for Privacy. I'm Hugo Teufel. I'm the Associate General Counsel for General Law at the Department of Homeland Security and I have the great honor and pleasure of being a moderator this morning. I say that because at least I'm not speaking, so I have very little to do and it's mostly not substantive, which is a great thing. But of course, being a lawyer, I've got plenty to say.

We have a distinguished panel of experts here to walk you through the privacy alphabet soup of SORN's, PIA's, CNA's, and OMB-300's. I've asked each presenter up here with me to provide about a ten-minute summary of his or her topic so that we can be sure to have plenty of time at the end of this hour for your questions.

I will of course introduce each of our speakers. Our first presenter, who leaves me at somewhat of a disadvantage, is Liz Withnell, who is counsel to the Privacy Office and a member of General Law within OGC. I say leaves me at a disadvantage because in preparing me for this morning she did a fabulous job of providing information on the other folks on the panel, but, being a very modest person, Liz did not provide me a whole lot about herself.

So I will tell you that Liz is one of the superstars, one of the true superstars in General Law and is a very senior, experienced attorney in the Federal Government dealing with information and privacy issues. Before she joined us at Homeland Security, Liz was over at OIP at the Department of Justice, where she was a superstar. And for some reason, and I'm not sure why, she decided that she would come over and work at the sweatshop that is DHS. You all are probably getting a feel of that today here in this room, the sweatshop part.

So, without any further ado, our first speaker, Liz Withnell.

MS. WITHNELL: That, Hugo.

Can you all hear me? I want to echo what Kip Hawley said this morning. When people introduce you as senior-level personnel in an agency, it just means you're old.

MR. TEUFEL: I didn't say that.

MS. WITHNELL: I'm happy to see all these people here. Not too long ago we would have organized a privacy workshop and we would have been lucky if 12 people showed up. Ten of them would have been perfectly capable of sitting at the table and providing the information because that's what they did all day

and they used the workshop as an excuse to get out of the office. Some of them are actually here today. We're glad you could join us.

When I found out how many people had enrolled in this seminar, I realized that what I had to say probably should step back a little bit and start from square one, because, despite the fact that there are lots of privacy experts here, I'm hoping that there are some people who are, if not totally clueless, then close to being clueless.

Last night it came to me how I should approach this little discussion about the Privacy Act and SORNs in particular. I thought, I'll just use a hypothetical, which is basically what's going to happen this afternoon with my colleagues, but I'm going to take a page from them and start you off with a hypothetical. For those people who are familiar with these kinds of things and with the Privacy Act itself, I apologize, but I thought this was the better way to start.

I should say that if I had had my act together I would have had this all done ahead of time and I'd have a hypothetical to give you and I'd have questions and so on and so forth. But this all came to me at about 1:00 o'clock in the morning, which is when I either do my best work or my worst depending on your point of view.

So in any event, Congress decides in its infinite wisdom to pass a statute that says to federal employees and to Metro: We want to encourage the use of public transportation, so we're going to give you money so that you can subsidize your employees using public transportation, Metrobus, Metrorail, whatever else you have.

Agencies are thrilled and, as is their wont and their responsibility, they decide to execute this law by setting up a program for transit subsidies. Someone in an office decides, in order to do this we need to find out from our employees who they are, where they live, how they come back and forth to work, if they use public transportation how much they spend on that particular piece.

So they develop a form and send it out to everybody in the agency and think: Hah, sit back, get the information; life is good.

Wrong. The Privacy Act requires that when you do that kind of thing you are in fact creating a system of records and you need to publish a public notice about it. A system of records is defined in the statute and it basically is a collection of information from which information is retrieved by name or personal identifier. So in my hypothetical example I am going to provide information and my agency's going to retrieve it by my name because when I show up every month to get my transit benefits, or every three months or whatever your program is, they want to see that in fact I still live in Rockville and I still take public transportation, and I have said that that's the case, and I'm still entitled to however much I'm entitled to.

So they have in fact created a system of records. The Privacy Act requires us to provide a public notice about the existence of these records, and the public notice requirements for the SORN are set out in the statute.

Now, the thing about statutes that I love and the things that keep lawyers in business is that people get nervous when there's a law involved, and so they come to their attorneys and say: Tell me what this says. Really the Privacy Act is a nice law and it's easy to read. If you haven't looked at it, it's on lots of public websites and I suggest you take a look, because if you are writing system notices the law itself tells you what they have to contain.

So you have to publish a notice that contains the name and location of the system. Well, that's easy. We're going to call this "Transit Benefits" and we're going to put it in DHS headquarters. Location used to be easy because it was where the paper records were kept or where you had your mainframe. Now in fact I think it's a little bit more difficult, and the tech people can tell me if I'm mistaken in this, but in fact systems could be everywhere.

So for purposes of where your system is located you really need to think about where the records are being used, because primarily we want the public to be able to know where this information is. In my case we want agency employees to know where we're keeping this information so in case they want to come and take a look at it they can.

The next thing that goes into a SORN is the category of individuals on whom records are maintained in the system. So in my example it would be agency employees primarily.

Then we have to put in what the categories of records are that are in the system. Well, basically I have this form that everybody's filled out and that's sort of the basic form that goes in there and that's what you're going to describe in your system notice.

Then there may be some other pieces of information, you know, what we get in terms of confirmation from the public transit authority as to yes, in fact these people are using the system, or what we get in terms of here's the amount of money that we'll give you, etcetera, etcetera. But basically we want to be as transparent as possible in terms of what is in the system in terms of records.

Then we have to talk about routine uses. Routine uses are interesting because under the Privacy Act records about an individual can be disclosed in 12 different ways, period, if you don't have consent. If someone gives you consent you can disclose the records any way that the consent covers. But if you don't have consent there are 12 ways that you can disclose records. One of them is for a routine use.

My biggest pest peeve with system notices is that there are lots of uses in the system notices that I've seen that aren't routine. It's supposed to be something that you would normally do. So for example, I might be sharing information from my Transit Benefits system with public transportation to let them know that I've provided benefits.

I might be sharing information with Congress to let them know that these are the employees who qualify, just in case they're interested. I probably need to share information from my system for some relatively routine things like with the National Archives because, even though some of you may think that these are your records and you can dispose of them as you see fit, in fact these are agency records and NARA controls the disposition of all agency records.

So you need to be listing the routine uses. One of the reasons -- or one of the requirements for a routine use is that the sharing that you engage in on a routine basis should be compatible with the purpose for which you collected the information in the first place.

I see Eva sort of sitting over there. It's hard when OMB is in the room because I might say something wrong. It's like I'm sure I'm going to hear about it, either publicly or otherwise. But as long as you're nodding I guess it's okay.

Compatibility I think is one of the issues that people tend to gloss over, particularly in the information-sharing environment in which we live. But it's something that I think all privacy professionals should think about in terms of writing system notices and in terms of actually sharing information: Is the sharing that you're envisioning compatible with the reason for which you collected the information in the first place?

If you want to share my Transit Benefits information with the CIA for some reason, there might be a compatibility issue because their mission is totally separate, it seems to me, from what the purposes of the system. So you might want to think about this and I would urge you to when you're putting these systems together make sure that you have routine uses that are truly routine for your system and that you're sharing for a purpose that's compatible with the reason that you've collected the information.

Then your system notice has to have policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposition. Some of those things, at least for people like me who are lawyers as opposed to technical folks, I'm hoping that the program people can take care of. I can understand retention and disposal and in fact I know a lot about it, but I don't know as much about storage, retrieval, and access controls, and it's the Bob West's of the world that you'll hear from, who I think can give us that information. So you need to be talking to your folks who are well-versed in those things.

Then we need to have the title and business address of the agency official who is responsible for the system of records. That's the system manager. That's

the go-to person when you want to know what's going on with the system. Those guys used to hide in the agencies and now really they've come into the fore because we have lots of systems of records.

The agency procedures whereby an individual can be notified at his request if the system contains a record pertaining to him is also a required part of the system notice. There are several aspects of a system notice that go to access and whether or not -- how you get access, who you contact, what the procedures are, and so on and so forth.

For most system notices, I would imagine that the access procedures are your FOIA procedures or your FOIA and Privacy Act procedures that you have at an agency. So this should be an easy part to write in your system notice.

Then we're going to put in the categories of sources of records: Where is this information coming from? In my example, most of its' coming from the employees of the agency. But people like to know where it is you're getting this information. If I decided I wanted to verify everybody's address in my system of records by using a commercial database because I just want to make sure that no one's lying when they tell me they live in Rockville, but really they live just down the street, in your categories of sources of records you should be putting that you're using commercial data so that there's some transparency on that decision.

Now, the deal with Privacy Act notices is that in real life -- in theory anyway, you're supposed to publish them in the Federal Register for comment for 30 days. If you look at the statute, what the statute really says is before you use the information that you have pursuant to a routine use you're supposed to give folks 30-day comments or a 30-day comment period.

But in real life what that means is we're not going to operate a system until we have published it for 30 days, to give folks the opportunity to see what it is we're doing and why. My experience over time has been, once upon a time nobody read these things. They were published, they were compiled, and the Privacy Act folks knew where they were, and God forbid, there was a problem and you could point to it.

But now people are actually reading them, so it's important to get it right to begin with and also to publish them for 30-day comment.

30 days is not the only comment period, though. Actually OMB is supposed to have an additional ten days to look at these things, so really what you need to be doing is either ten days before you want to publish notify OMB or your comment period could be 40 days, which will include the ten days that OMB gets.

The other thing that happens with this system notice is that you need to do a new system report or when it's a new system of reports, when it's a substantially revised system. And that system report also has to go to OMB and the system report along with the system notice itself also has to go to Congress. The system report to my way of thinking really kind of looks like a privacy impact assessment, which is where I will stop because it's a nice segue to the next part of our presentation.

MS. KLEEDERMAN: Well, that was no notice.

(Laughter.)

MS. KLEEDERMAN: I was waiting for a graceful conclusion there.

MS. WITHNELL: We'll let Hugo introduce you and then you'll have it.

MR. TEUFEL: I'll get up, because I can.

Thank you very much, Liz, while I fumble through my notes here to introduce the next speaker. Barbra Symonds I believe is our next speaker. She is the Director of Office of Privacy in the Internal Revenue Service at the Department of Treasury. Prior to joining IRS, Ms. Symonds served as Director of Privacy Services with the Department of Veterans Affairs, where she was responsible for ensuring compliance with privacy rules and regulations. While she was there she did a number of wonderful things, including establishing the total privacy management framework, and a business plan to address health

insurance portability and accountability, eGovernment Act and other privacy-related laws to assure systemic agency compliance.

Barbra.

MS. SYMONDS: Thank you.

Good morning, everyone. I provided some handouts at the back of the room. I doubt that there were enough copies because I don't think I was planning on this type of turnout. But I'm only going to talk to a few parts, to stick with my ten minutes or so. But this is good information for you to have as a take-away. So those of you who are new to the PIA world can have some references of what requires it, what are the drivers, what are the interfaces or interconnections, and some things that you can think about.

So I'm going to focus on a little bit just specifically around how the IRS has implemented the privacy impact assessment and our approach of integrating with system development, security, business owners, those types of things.

(Slide.)

The one slide that one of my staff brought to my attention of kind of my standard talking points. A year ago I used to have to bring to people's attention these privacy breaches that were going on and now it's just, you read the paper and it's which is today's breach.

But going back and looking through, just since January 1 of 2006 approximately 21 percent of the population has been -- had -- well, has had their data breached or is suspected to have had their data breached. That comes out to somewhere around 63 million Americans, that their information has been lost or stolen. There's not a lot of -- how many people have gotten a notice from some company or the VA that your data has been lost or stolen?

(A show of hands.)

MS. SYMONDS: Yes. So I think that 21 percent of the population, I'm guessing that that number keeps going higher and higher, because these are the only breaches that have actually been identified and published. If you'll notice, what happened last year when ChoicePoint had their breach, all of a sudden there was this big flurry of activity of saying: Oh yeah, I did too; oh yeah, I did too, and the was several months ago and they were suddenly coming clean because it was a big deal.

You're now seeing the same thing in what happened with the VA breach. People are coming out and going: Oh, well, that happened to us, too. But you're looking at the dates of occurrence and it's back to September or October, November, and they're just now coming out with figuring out where things are going.

So I kind of look at this as a double- edged sword for the privacy program in that it's horrible that this is happening to the public and to the individuals who are impacted, but the good news is I'm now absolutely bombarded with questions from executives and program owners and trying to figure out what are we supposed to do, what do we do now, what's next, how am I supposed to get this into shape.

The dialogue between security and privacy has never been more integrated and understanding. We're no longer scratching at the door knocking and pleading and pulling on coattails, saying privacy's got to be at the table. Now privacy is instantly there. This now has occurred or this policy needs to be updated, or what should we be telling our staff and our contractors. So that's all very good news on that side.

(Slide.)

I'm going to flip to, if anybody's following along, onto slide 4, the privacy impact assessment. The way that we really approached the privacy impact assessment is that it's a tremendous source of a structured conversation. Any of you who have been -- if you're a program owner, you know what mission you need to accomplish. If you're a system owner, you talk in an entirely different

language of design requirements and technical specifications and you know what you need to build.

Then in the Privacy Office we try to bridge that gap and bring that triangle together of saying, do you really understand your mission and what the minimum data is that you need to accomplish it, so that your designers and technical staff are building that data minimization of only collecting or interfacing in or sharing the limited information that's necessary to accomplish the mission. Then we come in and look at it, saying, are there any unintended vulnerabilities or risks to the privacy of the individuals, to the privacy and protection of the data that you've collected, and where can we come in in advance of you going live and into a production stage of mitigating those risks.

One of the other things that's become very powerful for us is putting the accountability back to the business owner. So what we've done is wrap in -- the privacy impact assessment actually for us occurs in multiple avenues and multiple reasons. We do a privacy impact assessment on all of our legacy systems to catch them all up and see where they are.

But we also perform them when we have to do the E-300 submission. As a requirement it has to be done. So we're looking at things at the concept stage, what are you even proposing to do and what's the potential impact to privacy risk or vulnerability. But then we also are tying it into the certification and accreditation process. So now when a system has to go through their three-year cycle of C and A, talking about their security plan and all their security risks and all those controls and things, we're also looking at the privacy impact, so when it goes forward up to the DAA, which I always forget what it stands for -- I'm sure you can tell me.

MR. TEUFEL: Designated accrediting authority.

MS. SYMONDS: Yes, what he said.

(Laughter.)

MS. SYMONDS: That's the business owner, the system owner, has to sign on the dotted line and say: I accept putting this system into production and I accept the risks and vulnerabilities that are resident within that system. That is something that has been especially powerful for us in documenting the vulnerabilities and the risks that are there and putting kind of the system owner on notice to say, if something happens it's on you. You need to be aware of how can you continue to put management, technical, operational controls in place to mitigate those risks.

So we are doing a systematic evaluation of the data in the system, the purpose of the data. One of the things that we had a difficult time with the security office to understand -- how many people have heard "If you have good security you automatically have privacy"?

(A show of hands.)

MS. SYMONDS: Nobody else has heard that? You've got to be kidding.

There's often this chicken and egg syndrome or this argument of is it a pure relationship between security and privacy or is privacy a subset of security. What I would subscribe is that they're looking at the same problem with a different slice or a different focus. We're looking at do you even have the right reason to get the data in the first place, have you minimized the data that you need to get, do you have the right purposing of where it's coming from, how are you verifying the accuracy of what you're receiving, how do you know what's being transmitted out, who are you sharing it with, do you have the right authorities and controls, have you minimized the access once it gets into the system that it's not a one size fits all for your user base, have you minimized the access controls as to who sees those things?

So we're really focusing on the information contained before even what comes into the system, whereas the security folks, they're not questioning so much whether or not you have the right mission or purpose for the system to exist. They're looking at -- they're just kind of taking it as a given: All right, you have this system, you have the data; how are you protecting it? How are you shoring it up with your different layers of defense?

So we're coming at it with a common voice now so that when they come in and get their security certification or they're going through milestone development that it's specifically they're getting the slice with both eyes, so they're seeing the concerns that we have of, we think you're collecting too much information or you're drawing it in from other systems that are not accredited, you've got a vulnerability of the accuracy of the information that's coming in, and those types of things.

The other area that we've gotten very focused on -- I'm going to jump a little bit more. I'm now on my slide 6. One of the things that we're working on is, again because NIST has been very good to the security community in terms of publishing very prescribed, documented regulations -- thou shalt complete the 826, the 853, these documents must exist -- and they give all the parameters and protocols.

I think that the privacy world needs to catch up to that, and I think that -- so what we've been seeing is, we started out with the premise of the OMB E-Gov Act memo and guidance of, here are the seven or eight main categories that you need to address. Some departments said: Great, I'm going to answer eight questions and I have completed my PIA and I'm done; check the box, we're done.

Others have gone into a different -- everybody's taken a different tack on how they approach the analysis. What we are looking at doing, and I hope to have it to go live in the fall time frame, we're building what we consider our next generation of the PIA, which will be much more of a system-driven decision support system that will take you through a series of questions; that the system owner and the business owner don't need to understand privacy requirements, the rules around system of record notices, Privacy Act statements, those types of things.

We're having a dialogue. We're saying: What's your purpose? What authority do you have to conduct this mission? Tell us about the data that you're collecting? So we're framing the PIA around the combination of the data elements that you're collecting, down to the specific data elements, and that's

going to really help us along with this data classification and categorization because we haven't gone that far yet.

There's a FIPS-199 document that requires you to categorize and classify your data. A lot of people say, well, that's just too hard, there's just too much data in the system; you want me to tell you about every single data element? The answer is yes, we do. We need to know all of the data elements.

Then we're taking that actually across the information life cycle. So we're saying, when you collect it what's the source? Does it come from the primary source, a third party, from another system? How are you storing it, maintaining it, disposing of it? So we're taking it all the way across.

So we kind of have a double matrix of, first of all that you collect it and then at what points are you using it or when are you disposing of it and retaining it? So that's going to get us a lot further along. The raw data collection has been, we spend a lot of time back and forth with the system and business owners, that they kind of guess at our narrative of what we're looking for. So we're going back: No, we really need to know this part as well. And they say: Well, why didn't you tell me that?

So we're looking at doing that. So we're doing a lot of raw data collection up front. The fact is that's a much more powerful analysis capability to really understand the vulnerabilities or privacy risks that may be introduced and how we can go around mitigating those. We mitigate those at the earliest point possible.

The other page that, if you have the handout, I would draw your attention to is Slide 10. One of the other things that the IRS has done for several years now is embed the privacy impact assessment throughout the enterprise life cycle of system development. So we use a milestone 0 through 5 approach of a system development life cycle. We conduct a PIA at every stage of milestone development.

So we don't wait until it's ready to go into production. If we wait until that long we've got no chance of influencing the design or the development. If

you look at the cost of implementing a new system, and especially on the magnitude of the IRS modernization planning, it's multi-millions of dollars. A little squeaky Privacy Office privacy impact assessment says: Excuse me, I think you should have done this instead. They say: It's too late; we've paid the contractor, we've closed out the deliverable; we're going to production.

So what we do is we get in again at the concept stage, in at milestone 0, to look at what are they proposing to do at the highest level of concept, that we can have some suggestions and concerns right up front, so that then when they get into the design requirements, the technical requirements, into development, into prototype, into their system test and evaluation, so that we're actually building a requirements document for them to consider, say, here are the privacy requirements that then we need to have documented test cases, privacy test cases, for you to prove that you've embedded these privacy requirements into the system.

So again it's to complement what security test cases go through with a different look at the privacy vulnerabilities and risks that go through. So the notion is that by the time we all get to milestone 5 and the system is ready to deploy into full production, security and privacy and system owners can all nod their head and sign on the dotted line and say: we're comfortable that this has satisfied all of the concerns and requirements and is going to satisfy the mission and the purpose for the system to exist at all.

So what we have on Slide 10 are the different types of things that we look at throughout the milestone development stage. We're suggesting that there's not a one size fits all PIA. One of the things that we're doing with this to support the PIA is, tell us first of all who you are. I'm a system, I'm a survey, I'm a website, I'm a proposed rule, I'm a contract, I'm in production, I'm in development.

Those types of qualifying questions that tell me what you are first will take you down a different path and a different series of questions that need to be answered. Some of the pushback that we get is: You're asking me things that all I'm saying is NA, NA, NA, NA, and we don't want to -- we have to make it a

value-added exercise and not perceived as just another bureaucratic piece of red tape to complete.

That's all I'm going to say for now. So now you're up.

MR. TEUFEL: That was quick. Thank you, thank you very much.

Moving to our next speaker, Robert West is the Chief Information Security Officer for the Department of Homeland Security. Prior to being appointed to this position, Mr. West was in the Office of the CIO, Homeland Security Transition Planning Office, at the White House, where he was responsible for developing a strategic plan for implementing an information security program for the Department.

Prior to the formation of the Department, Mr. West served as a Senior Policy Analyst with the Critical Infrastructure Assurance Office at the U.S. Department of Commerce, where he was a major contributor in the development of the national strategy to secure cyberspace, a White House initiative.

Also I will mention that prior to joining the Department of Commerce Mr. West was a career naval officer. With that, Robert.

MR. WEST: Thank you for allowing me to come and join you today.

I want to begin going back to something that Barbra said because she really I think hit a key point. When we think about security and privacy and sort of this, it seems like we're more and more joined at the hip today than we ever have been in the past. From my perspective as the IT security guy, when I think of privacy data I think of privacy data as a subset of all data. From my perspective, it's really that simple.

But the problem is for people like me it really isn't that simple and we tend to try and make it more simple than it is. Security and privacy really, the way she said it, to paraphrase, that we're really looking at common issues from different perspectives. I think we need to keep that in mind as we move forward. It really is a complex subject and there are things that we certainly need

to learn about privacy from a requirements perspective, from an issues perspective, so that we can better engage.

But I would add, and I'll talk about this in a minute, there are things that we do that you should be aware of that I think will help you, help the privacy team, if you will, in implementing an effective privacy program.

To illustrate sort of this different perspective, right off the bat we've had some great conversations between my office and the Office of Privacy about how do we better work together, what kinds of things can we do moving forward. Right off the bat we kind of went into this tailspin, if you will, about what is a system.

From a privacy perspective, a system of records is one thing. From my perspective, an IT system is a bunch of chips and printers and things like that with an accreditation boundary where we're going to have someone accept risk. So they're different things. So now we're working together to figure out, how do we map the two together and make sense out of them, so that when we say that this system, this IT system from my perspective, that we've built appropriate privacy controls around that, that in fact that's consistent with all of the notice requirements and the things that we're doing in the broader sense in addressing privacy.

So from this point forward as I speak, when I talk about a system I'm referring to an IT system, a set of boxes, chips, transistors, the technical, the geek stuff, not a system of records, but understanding that there is a difference.

The other thing I want to say too up front is that DHS is somewhat of a different duck. It's a different dynamic for us than with other federal agencies. Our history is rather short. We became a Department in early 2003. We brought together 22 agencies, disparate, divergent, different agencies, radically different agencies.

The Secret Service has their mission. I didn't know until recently the U.S. Customs, now our Customs and Border Protection Directorate, I guess, that one of their missions is that they generate revenue for the federal government. They

are the second largest revenue generator for the Federal Government behind the IRS. They generate like billions and billions of dollars of revenue every year. So when you talk about their security requirements, they have a financial component to that that other components don't necessarily have. So it's just a different -- from my perspective it's just a different set of requirements, if you will.

So we really are somewhat different, and bringing all those agencies together, we've been working real hard the last few years to try and make sense out of that and to kind of rationalize into a common program.

Now getting into specifically what I do, we have our own statute, the Federal Information Security Management Act of 2002. Interestingly enough, FISMA was actually signed into law originally as a title of the Homeland Security Act that created this Department. That was in November of 2002.

The FISMA statute was reenacted as part of the EGov Act of 2002 in December of the same year. I think Congress had originally intended it to be there, but they wanted to get it in front of folks and kind of get it on the street, so they went ahead and attached it to the Homeland Security Act.

But I think there was also sort of a growing awareness that as this new Department was created that IT security was -- when we talk about - how do we protect the nation, part of it is protecting our critical infrastructure and resources, and a lot of that involves technology.

So with that, we have a statute, the Federal Information Security Act, Information Security Management Act. I'm the guy in the Department who is assigned the responsibility of implementing a FISMA-compliant program across the Department. The Act puts the program under the office of the CIO and so I work for -- I'm a direct report to the Department CIO.

The way that we have approached this, as I said, the first year or two it was kind of getting to know folks and we sort of left the components free to do what they needed to do to kind of maintain the status quo. But we learned after

the first couple of years that the status quo wasn't going to continue to get us -- continue to be the right way in every case.

We had a couple of IG reports, for example, where by the end of the second year we were already in a sense governing an inventory of IT systems, and we had components that were reporting, the CIOs were reporting to me: We've got these five major systems or these 16 major systems.

Then we started getting IG reports that say: Well, you're doing really well on those five; what about, quote unquote, "the other 450." Or another component: We're doing great on those 16 that you're governing, but what about the other 900? I won't tell you which component, but it was pretty much across the board.

So we realized that right off the bat we didn't even have any idea how much IT we had in the Department. So last year I actually hired an audit firm, PWC, PriceWaterhouseCoopers. I wanted to use a firm that had a sort of compliance audit flavor to it. We branded this and we set out to conduct a Department-wide inventory.

Some of you may have heard of this. I branded it as a boarding party. I did that intentionally. I wanted the components to know we're not coming to ask; we're coming to learn and we're coming to engage, and we're going to get to an accurate inventory. The mantra of all year last year was: No computer gets left behind. We really made great strides in getting to an accurate inventory.

We now have about 700 major systems and applications in our inventory today. That was the accountability part. FISMA is all about, and privacy too, the Privacy Act and all of this, is really about accountability. It's about people and making sure that they do the right things.

So first and foremost for me and the inventory effort, it was about making sure that we could hold folks accountable to do the right thing for every system. But sort of coupled with that is the notion that when you start holding folks accountable you also have got to reach out the hand and help them. So we also wanted to be the easy button, and we've implemented some automated tools. We've necked the policy, all the NIST things that Barbra talked about, down to

an architected subset of that with compensating controls, and we're now implementing those system tools.

Is that the button?

(Laughter.)

Then, with automated tools in place and a streamlined way to determine what controls are required for each system and a detailed set of remediation metrics, this year we launched a remediation project to get every system accredited by the end of this fiscal year, and we're well into that. We have completed about 80 percent of the documentation for accrediting systems, which is about 11 different artifacts that we require, and we're at about 60-some odd percent of systems actually accredited. That's up from 23 percent when we started, so we are making good progress with that.

So what does that have to do with privacy? One of the things we're learning is that -- let me say it a different way. What we've done is we now have the processes in place to implement controls the right way for systems, with accountability. We need to make sure that as we do that -- and we want to take this on -- that when we talk about privacy and specific privacy- related controls, technical controls, not all controls, that we need to implement at the system level.

Let us do that. Tell us what the controls are, tell us what the requirements are, and then work with us to get that done. And we really are going to do that.

My fear is that, because we're a new Department and we have so many requirements that at the system level a system owner or a program manager is going to be bombarded with all these different requirements and it's going to be so difficult that they're not going to be able to get it done. What we want to do is neck that down and say: Here is your requirements, and our tools will allow you to tailor, based on answering some questions, and get a specific set of requirements and controls that need to be implemented, and we want to build privacy controls into that as well.

The last thing I want to say, as I'm getting the axe here, is that the other thing that I think is going to be, we're going to probably see even legislation about this, is there is concern now about how we report privacy disclosures. We need to ensure that we have a process in place to do that. We today have an incident -- an IT security incident handling capability in the Department, with network ops center, security ops centers, computer emergency response centers. We report to the U.S. CERT, which is the federal CERT, in DHS.

We have a process in place. We're still kind of maturing it, but at least we have a process in place, and I hope we can leverage that to ensure that we report privacy disclosures as well.

The last thing, what you can do more than anything else to help us, and hopefully how we can help you is, in the component level I have counterparts that are called information system security managers and they report to your, the component, CIO. If you don't know who that individual is, you need to go introduce yourself and meet them and start working with them.

I've tasked them to do the same thing to you. So hopefully at some point in the near future you're going to be walking down the hall looking to meet somebody and you're going to see somebody's head bobbing who's looking to meet you, and you all will meet and that will be good.

Thank you.

MR. TEUFEL: Thank you very much.

Our last speaker is Eva Kleederman. Eva joined the Office of Management in October 2001 as the analyst for privacy policy in the Information Policy and Technology Branch, Office of Information and Regulatory Affairs. Since enactment of the E-Government Act of 2002, she also serves as the new statutory -- hold on here. Yes, sometimes I get lost. She serves as the new statutory Office of Information, Technology, and E-Government established within OMB.

Her work involves issues relating broadly to federal privacy policy, but she also carries responsibility relating specifically to federal agency implementation of the Privacy Act of 1974.

The reason why I was pausing is because, why, something else that Eva had done in her professional career. When I read that I thought, why would you ever want to leave? It's the best job anywhere in government. For ten years prior to coming to OMB, Ms. Kleederman worked as an attorney in the General Law Division, and that's what I was referring to, of the Office of General Counsel at the Federal Emergency Management Agency. Her numerous responsibilities at FEMA included information access and disclosure issues.

Before coming to the government, Ms. Kleederman worked in private legal practice, primarily in the field of government contracts and regulatory counseling, both things that I can relate to.

Eva.

MS. KLEEDERMAN: The ten years I was at FEMA, it was a great job.

I don't think my remarks are going to be as smooth as those of my colleagues because I'm kind of just commenting on their remarks and filling in the gaps. So bear with me.

But Liz, thank you for your description of SORNs. The Privacy Act, as you know, was enacted in reaction to the excesses of the Nixon administration. The purpose is to avoid having any secret records. So the purpose of a system of records notice is to tell the public what information agencies are collecting, how it's used, and how they can find out what information an agency has about them.

The system of records notice should accurately reflect what's being done programmatically, as Liz said, in terms of the information collected and the use. In many cases this programmatic aspect will have been hammered out during the ICR process, and that is the process by which an agency comes to OMB with a request to collect information from members of the public. OMB will review it in terms of the purpose and say, well, do you really need this item, how does this

item of information that you propose to collect go towards the purpose? So that the collection of information becomes narrowed.

This is not necessarily true when the information collection is targeting federal employees since that doesn't go through the ICR process. So agencies developing such systems as the one that Liz mentioned, having to do with the transit subsidy, the agencies will need to closely scrutinize those systems of records to determine, is the minimum necessary being collected for the purpose, are the routine uses compatible, does the agency accurately reflect what is going on.

I'm really delighted that Liz specifically mentioned the issue about data obtained from commercial data aggregators and resellers because this is particularly important these days when so many of the agencies do obtain commercial data that should absolutely be reflected in the system of records notice.

I would caution -- Liz asked me to speak from the OMB perspective about the kinds of things I see in systems reports that are submitted to OMB. I would caution agencies not to try to do too much in a single system of records notice. A single SORN can have multiple purposes, but they shouldn't be too disparate. They should use the same kinds of data.

Again, routine uses should be narrowly tailored. Don't try to get too many uses all condensed together because it becomes confusing and meaningless. The routine use should include what information is being released, to whom, and for what purpose.

The purpose of the system of records notice is notice, and if the routine use is indecipherable then it's really not providing notice.

Routine uses I believe should be itemized with the notice. If an agency is publishing all of its SORNs at once, it can certainly have an appendix of all the common routine uses or all of the routine uses and then in the body of the notice reflect by number which routine use is applicable to that particular system.

But the practice of publishing blanket routine uses in one year and then having subsequent systems published that refer to a prior Federal Register publication without actually reprinting the routine use is deficient notice, I believe. I think it's too hard for the reader to go back and forth. If the system is up electronically on the agency's website and there's a link to the blanket routine uses, that's fine. But requiring readers to go back to prior Federal Register publications is just too much work and I believe deficient notice.

Major changes to a system of records notice should be made immediately. Otherwise agencies should review their systems notices every two years to ensure that they continue to be accurate. Minor changes can be published as they come up or all at once annually, but the important thing is that major changes as to the purpose of the system or the individuals covered by the system for significant routine uses really do need to be made immediately.

Kind of an esoteric area has to do with exempting a system of records from the access -- amendment provisions of the Act or other provisions of the Privacy Act. That's rather technical, but my point is that that action requires a rulemaking. That is, publication of a proposed notice to invoke an exemption and 30 days notice and then publication of a final notice. So that's your basic rulemaking activity. Other kinds of privacy notices are simply notices, that don't need to be finalized formally in the Federal Register.

Finally on SORNs, I would say that existing guidance is still good, the 1975 guidance, and A-130, particularly Appendix 4, both on the OMB website.

With respect to PIAs, as Barbra said, PIAs are a creature of the E-Government Act of 2002, section 208, which is the privacy provision of the E-Gov Act. It kind of picks up where the Privacy Act leaves off insofar as it requires the agencies to scrutinize how they are handling information, identifiable information about individuals, or information about individuals that can be made identifiable through matching or other techniques. It makes agencies scrutinize the handling of this kind of information that may not -- that is not kept in a Privacy Act system of records.

So it adds protection in the sense of due diligence where the Privacy Act leaves off. I don't want to suggest that PIAs are not required for information maintained in a Privacy Act system of records. You will have PIAs for both. But the criterion is really identifiable information and not whether or not the information is kept in a Privacy Act system of records.

The statute doesn't require that PIAs be conducted for employee data. That is, it doesn't require that PIAs be conducted on information technology systems that house or administer information about employees. However, OMB encourages that agencies take the conservative approach and protect information across the board, regardless of whose information it is.

Like the Privacy Act, the purpose of a - - like the system of records notice, the purpose of a PIA in part is transparency to the public. Usually a PIA is conducted on a specific information technology system, as Bob distinguished from a Privacy Act system of records. That is, it's conducted on a system of hardware and chips and wires, usually at the system level, but sometimes in some cases at the program level. An example that comes to mind is U.S. VISIT, which is a complex system, a complex body of interlocking information technology systems, used to accomplish a single business process that affects the public.

PIAs must accompany budget requests for the information technology systems that they relate to in appropriate cases. That is, new or substantially altered systems that administer information in identifiable form. This is part of OMB's evaluation of the budget request. That is, to the extent that an information technology system requires a PIA, the PIA must be submitted with the system and OMB notes whether or not a PIA is submitted with applicable systems.

The part of the -- and PIAs conducted outside of the budget process, that is later in the year if there's a substantial alteration to the system, those PIAs do not need to be submitted to OMB, but they do equally need to be made available to the public upon request.

The part of the PIA that's often missing is the assessment part, and that's the wrap-up analysis of what risks were encountered in developing the system, what choices were made in mitigating the risks that were identified, what risks remain, if any, and how the agency plans to mitigate these or live with them or the extent to which they really compromise the data or individuals or systems.

The analysis part, the assessment part, is really a narrative of what choices the agency made and why in developing the information technology system. This is really important. Otherwise the PIA looks -- is a static document like a system of records notice, and that's really not the purpose. The PIA, as Barbra said, is a dialogue about how the system was developed, all things considered.

So OMB sees system of records notices and PIAs as essential analytic tools and as well as vehicles for notice. It has added privacy to the E-Government management agenda so that the agencies' quarterly E-Government scorecard reflects whether they have achieved the milestones set for conduct and publication of PIAs and system of records notices for applicable systems. And as well, it's added privacy to the FISMA reporting requirement. This is section D of the FISMA template. It's moved the reporting of privacy from the E-Government report and put it in the FISMA report, basically to streamline reporting for the agencies and allow them to do all their reporting in one place.

It's also revived agency analysis of Privacy Act activities, including publication of the SORNs that previously had been separately reported. So all reporting is done by the agencies in this one FISMA vehicle.

On the Exhibit 300's that will be coming in the fall or at the end of August, these have been greatly simplified. We attempted to eliminate ambiguity in the questions and thereby enabling OMB to obtain better information. We attempted to eliminate ambiguity by providing the universe of possible answers in the questions.

In the privacy section, for instance, we asked whether the agency conducted and-or published PIAs and SORNs under particular circumstances, and it really leads the agency through the analysis and helps them identify

exactly what they need to do or should have done or did do. Again, this year's PIAs are to be submitted with the budget request.

Regarding certifications and accreditation, I am no expert here, but it is akin to the privacy assessment insofar as the agency is analyzing actual security capability and performance against the theoretical security vision. I'm talking about technical security controls that support privacy, not the privacy controls.

As I understand it, what you've got is a hopefully robust system security plan that's built around the documented system security requirements. Then you examine the extent to which the security controls operate as intended, based on the security requirements. You evaluate the delta between the ideal and the actual and analyze what actions should be taken to correct deficiencies or reduce identified vulnerabilities. Then, depending on the remaining risks to agency operations or agency assets or individuals, the decision is made to accredit the security system or not -- to accredit the system security or not.

What's important here from my perspective is that OMB does not accept an interim authorization to operate the system under specific terms and conditions. As far as OMB is concerned, the accreditation must be unconditional.

Then finally, you've mentioned Fed Circ and the reporting of incidents. The final point I'd like to make is that since the unhappy occurrences of the last several weeks OMB is working with agency representatives to develop notice policies for when data is compromised and also working with the agencies to help them close the loop between IT security incident reports to Fed Circ and DHS, have the agencies close the loop with their privacy people so that it can be determined whether or not identifiable information's been compromised and then the agency can take the appropriate steps to mitigate the harm by notice to individuals.

So those are my remarks based on what's gone before and I think we're ready to take comments.

MR. TEUFEL: Thank you very much.

Wow, there are a lot of questions up here. Unfortunately, we don't have enough time to answer all of them in detail. So yes, no, no, yes, it happened once but it was fixed.

I've got a couple quick ones here that I can answer for you and then we'll ask one question of the panel, and if we have enough time we may hit another one, but we probably don't.

Should PIAs be conducted for components- directorates primarily dealing with businesses and contracts? And the answer is: If the system contains personally identifiable information, yes.

Next: Although PIAs are not required for databases that house employee information -- and I wonder why -- what about systems that maintain information for former employees? The law doesn't require it, but as a matter of policy we do.

Then -- and thank you very much for those cards and letters.

Then for at least the one question that we've got time for for the panel, I will read that now: Does the PIA requirement apply to systems developed prior to November of 2002? When changes are made to these systems, should agencies conduct a full PIA or just with respect to the change?

MS. KLEEDERMAN: Systems in existence before 2002 are not subject to the PIA requirement until such time as there is a substantial change made to the system. Our guidance 03-22 identifies what substantial changes are. At that point I believe a full-blown PIA would be in order, because discussing just the change doesn't illuminate a whole lot.

Agree?

MS. SYMONDS: Yes, absolutely agree. In fact, I think I put the nine triggers of the OMB memo of a major change determination for your references. But the only thing that I would say, what we've done is we've actually gone backward and caught up the legacy systems so that we have a baseline

understanding. Part of that is interpretation of section D in the FISMA report of how do we get to green for our quarterly report if we say our total inventory is X but we're only 40 percent PIAs?

So we've actually gone through a tremendous exercise of making sure that all of our FISMA-reported inventory of systems do have a PIA. So I think it's a matter of good practice and good business that you should understand at least from a baseline standpoint. Sometimes the legacy systems are hard to catch up and mitigate and correct, but knowing what they are when you're ready to do an upgrade or system change, you'll already have that baseline understanding of what you need to correct.

MR. WEST: If I could add just sort of a DHS perspective, and this is I'm speaking jointly for my office and for the Privacy Office. In our C and A process, it really is a process and we are -- in this last year, this year, we're taking all the legacy systems and remediating them. We have required privacy be addressed as part of the remediation project.

But in any case, as systems come up either for major changes, when there are major changes or at least every three years, you have to go back and re-accredit the system anyway. When that happens, regardless of any prior rules, when that happens the privacy will be addressed appropriately on that system.

MR. TEUFEL: Thank you all very much, and thank you all for attending. As I understand, we're breaking for lunch. I'm not sure what that means, but probably some of you will be eating. Thank you all very much.

(Applause.)

MS. KAVANAUGH: If I can ask you to be back in the room at 12:30, we'll resume our afternoon session. We're going to have a lot to cover, so 12:30 back in this room.