DEPARTMENT OF HOMELAND SECURITY

DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE

FULL COMMITTEE MEETING

WEDNESDAY, MARCH 12, 2008

Wyndham El Paso Airport
Sandalwood/Satinwood
2027 Airway Boulevard
El Paso, Texas 79925

MORNING SESSION

MR. HUNT: Good morning, my name is Ken Hunt, and I am the designated federal officer for the Data Privacy and Integrity Advisory Committee, which operates under the Federal Advisory Committee Act. Under the statute, the designated federal officer is required to be present for all meetings and so I have met that requirement.

I would like to say before I turn it over to Howard Beales, the Chairman, a few things today. First, I want to thank all the committee members and panelists and members of the public for coming to El Paso, Texas for our meeting. I know that was a long haul for a lot of us, and I appreciate that very much.

A word about the schedule. Due to a family emergency, the Texas State Homeland Security Director, Mr. McCraw, will be unable to join us this morning. As a result we're going to shift, not the order of things, but the time of things a little bit. I'm sorry for any inconvenience that causes anyone.

Just this morning we received written testimony from CDT, and I will be printing out copies of those and having them distributed to the committee as soon as we're able to get a sufficient number of copies of that.

I want to say a word about the field visits yesterday. I think the committee was very pleased with the exposure we all got to ICE and CDP operations at the border. I want to thank particularly Sandra Hawkins in our office who really made a long hard pull to arrange those things.

And I think they were due in great part to her very hard work over the last couple weeks. She did have help from Tamara Baker and Rachel Drucker so I'll mention them as well, but Sandra gets a special place for making that happen. Finally, I've been asked by the audio/visual staff to make sure that members speak close to the microphone so everything will be caught for the record. And with that I will turn it to Howard Beales to get the meeting started.

MR. BEALES: Thank you, Ken, and welcome to everybody to our public meeting today. If I could ask that everybody please make sure cell phones are turned off. If I could ask that everybody please make sure that cell phones are turned off, and -- that would be much appreciated.

And if there are any members of the public who are interested in signing up for public comments, please see Rachel Drucker in the back of the room, and we would love to hear from you at the end of the day.

First item on our agenda today is the Privacy Office Update. Hugo Teufel testified in front of a house committee yesterday so he was unable to be here, and so we will hear instead from John Kropf who is the Deputy Chief Privacy Officer and Senior Advisor for International Privacy Policy.

John became the deputy in July of 2007, and he advises on issues related to clients with privacy laws, DHS policies and programs, and agreements that adhere to Fair Information practices. And he's the Chief Operation Officer and Policy Strategist for the Privacy Office.

He also oversees the Office's international privacy work and has represented the Department on U.S. government delegations to OACD and APEC. He's served as advisor on various international negotiations. Before joining DHS John worked ten years as an international lawyer with the U.S. Department of State and the Offices of Legal Advisors.

He earned his law degree and his Master's of Public and International Affairs from the University of Pittsburg. He's a member of the bars of Pennsylvania and the District of Columbia, and he's published numerous articles on privacy issues.

John, welcome, and we look forward to hearing what's new in the Privacy Office.

MR. KROPF: Good morning, and thank you very much for that very kind introduction, Mr. Chairman, and good morning to the rest of the committee. I only wish that my mother was here to hear that introduction because it was probably a lot better than perhaps I deserve or it certainly sounded quite good.

I would also like to echo the thanks from our executive director, as well to the committee, for coming out here to El Paso and meeting here. In talking to committee members last night and this morning, just informally, that the feedback that I have been hearing is that yesterday's site visits were extremely fruitful and extremely useful.

So that's very positive to hear that the utility of the site visits to the board and/or EPIC were informative for the committee. Again, I would also like to mention that the Chief Privacy Officer Mr. Teufel sends his regards, regretfully could not be here today, but I will attempt to serve as his able understudy.

I would like to open the formal part of the meeting again with an update of what the Privacy Office has been doing since we last met in September. I think I would just open with a summary to say that I believe that the DHS Privacy Office continued to be a leader in the federal government on privacy.

We've been active in a wide swath of various privacy policy, privacy compliance, technology, international work, and we're also building the office to meet our new statutory responsibilities. Just to begin with, some of the more significant policy developments that have happened since we last met -- I'll only briefly touch on them.

REAL ID -- Privacy Office has issued a Best Practices Guide for states regarding the protection of privacy and the security of personal identifiable information. And it's posted on our DHS privacy website, as well as the REAL ID page.

Second, we've had a very successful CCTV workshop that was back in December that was led by our senior advisor on policy, Toby Levin. We had close to 100 attendees to that workshop, and the workshop itself provided a real cross-section of both privacy practitioners and law enforcement to talk about their best practices and how they use CCTV, and how it is -- how they work with it to make it privacy sensitive.

And what we hope to come out of that is, I believe, we have a transcript and a summary of that transcript. If it's not already complete and on our website, it will be shortly. We also hope to develop from that workshop a CCTV initiative for the department to really start setting down some guidelines and guidance on how CCTV would be privacy sensitive.

Also, at the last meetings I think I mentioned that Privacy Incident Handling Guide, but I only reiterate it here because at all of your places I think you'll have pigs with wings on them. And this is meant to stand for the Privacy Incident Handling Guide, the PIHG, so that is just a little reminder that we have issued this Privacy Incident Handling Guide.

And I will say we've also finally issued our annual report for 2007. You'll see that there are copies available out on the table out in front of the entrance to the conference room. This was -- as has been noted in the press, it was submitted later than we would have liked to have had it presented to Congress.

There were some process issues which have been discussed in the media, but what we believe here is the important thing is we have resolved those process issues so that hopefully going forward we will be able to submit future annual reports in a timely fashion.

In the compliance realm, compliance is very much a numbers game so I'll throw a few numbers at you here. Since we last met in September, we have issued 29 Privacy Impact Assessments, 3 Systems of Records Notices, and some of the more notable areas I would like to mention.

We have done a PIA and a SORN on the identification system, which is the IT system that helps support the E-Verify Program. We have done a PIA, SORN and a Notice of Proposed Rule Making on the ICE Pattern Analysis and Information Collection System, which is a law enforcement system.

Another significant compliance area was a PIA for RFID technology for border crossings, which is part of the Western Hemisphere Travel Initiative, WHTI as it's sometimes referred to, and we have also done a PIA for REAL ID File Rule.

Also, just to step back and talk about compliance overall, our Director of Compliance has come up with a very good plan for reducing what's been called the privacy backlog, which is those SORNs -- when DHS, we stood up, we had well over 200 SORNs to bring into compliance, and our plan is really to reduce that backlog and have it down by the end of the calendar year to zero.

That's the plan, and many of these SORNs are redundant in some cases, and we hope to, with a lot of diligent effort with our new hires and the privacy compliance area, to be able to bring those SORNs down to a state of full compliance.

Let me turn now to -- just to mention FISMA reporting. We have also been -- since September we have also submitted an additional FISMA report, which tracks a slightly different set of information. It does cover PIAs and SORNs under a slightly different definition, but what I would like to mention with our latest FISMA report is that our PIA and our SORN percentage points have improved. Our compliance rates are up on both PIAs and SORNs.

Also, I want to mention now, moving from compliance into the testimony area, as the Chairman mentioned, the CPO yesterday afternoon testified on the use of commercial data brokers and associated privacy issues before the House Subcommittee on

Information Policy Census and National Archives. It's a subcommittee of the Oversight Government Reform Committee.

I want to pause here just for a moment and say that this is an area where the committee's past work has really proved quite valuable to the Department. Much -- many of your recommendations that you did do in the area of use of commercial data and data brokers were extremely useful in preparing for this testimony. So it's really worth pausing here for a moment and just saying that this work that you have been doing with the Department has proved its worth, proved its value.

I would like to move over to talk a minute about the -- some of the new compliance responsibilities that we have with -- under the 9/11 Act. Essentially, those can be broken down into two general areas.

We've had additional responsibilities to do training in both -- with the fusion centers and, in fact, I believe we're attending -- there's a fusion center conference next week in San Francisco, and we'll be doing other training throughout the Department. In fact, the office is working to staff up to increase its capacity to do privacy training throughout the Department.

We've also been tasked with doing additional reporting under the 9/11 Recommendations Act. We have filed our first quarterly report that -- the Act requires us to file quarterly reports on privacy inquiries and complaints. And we refer to it shorthand as an 803 report. That first report has been filed successfully. We also were asked -- required to file a data mining report, which we have also done so we are on track for meeting our 9/11 Recommendation Act requirements.

In the technology area, there's -- this is one of the most demanding areas that we have in the office, and I won't go through a whole lot of detail other than to mention a couple of the more significant areas that we're working in.

We're doing a lot of work with U.S. CERT to update their current PIA. It's sometimes called the Einstein program. It will be Einstein 2.0. And this new PIA will be published on the DHS website shortly, just as soon as that PIA is completed, which we believe is in the near future.

We are also going to be observing -- the cyber area is a very big area. I see that as a very big growth area for the office. We're also going to be observing Cyber Storm 2. Several senior members of our office will be observing that this week. It's an exercise that's scheduled all this week. It's a simulated cyber attack exercise.

One other significant item under the technology area is the Identity Management Task Force, which is an area that Privacy is serving, participating in this task force for the Department and identity management, and also possibly identity theft will be big areas, big challenges for the Department to work in.

Moving off of technology and on to the international front, I'll mention just briefly that the international team has been working to serve as advisors on international data sharing agreements that the department negotiates that involve sharing of personal identifiable information.

Just this morning it was reported that DHS and the Department of Justice have concluded an agreement with Germany on sharing information for law enforcement and counter-terrorism purposes. Our international team has been able to sit in on the negotiations and advise on privacy matters and come up with sharing PII.

We have also been participating in the OECD working party. I was there last week in Paris to be part of the U.S. delegation that was looking at specific issues like cross border cooperation on privacy issues, and the OECD is possibly interested in opening what they call a global privacy dialogue, which would potentially entail reopening the 1980 OECD cross border privacy principles.

We've also been official observers to the international working group on data protection and telecommunications. We had a member of our team go to Rome, Italy, last week as well. There one of the significant issues that they are looking at is identification management, ID management.

And I'll also close by mentioning on the international front that the international team continues to be very much involved in a high level contact group, as it's been called. It's a group of experts that is made up of the Department of Homeland Security, Justice and State Department negotiating with the Europeans to try to come up with a common framework for information sharing in the law enforcement and counter-terrorism area.

Moving toward the health of the office, the office itself is in very good health. We are growing to try to meet many of the new demands. I think I mentioned we're going to be hiring three new positions.

We were advertising for an associate director for privacy policy education. That will be coming out very soon. We also hope to bring on an associate director for technology that will have a -- specialize in intelligence areas, which is one of the demands that we have on the office. A director, third a director for privacy incidents and inquiries. And finally we have funding -- we are funding two attorney positions that will be -- they will physically sit in the Office of General Counsel. However, they will be dedicated to us to provide both legal guidance on both of the FOIA disclosure side of the House and to the privacy side of the House.

I would also like to mention that our budget -- we've got good news on our budget, which has just received a -- we have -- moving forward with a 1.3 million dollar increase for FY '09, which is good news. Most of this new money will be devoted to bringing on additional personnel, the folks that I mentioned.

And last, in terms of the office, I would just like to say that we've had some very nice welcome recognition to some members of the office. I would like to mention that our Director of Compliance, Rebecca Richards, was recently named to the Fed 100, which is for top executives from government, industry and academia who have had the greatest impact on information systems in 2007.

And this is quite a significant recognition of Rebecca's work, and it's really something that we're all quite thrilled about in the office. We feel like it's a recognition of a whole lot of hard work that her team and Becky have done. She's going to be part of an awards ceremony at the Ritz Carlton at the end of the month at Tysons Corner, Virginia.

And if that were not enough, Toby Levin, our senior advisor was recognized by Secretary Chertoff during December. They had a department wide awards ceremony, and she received the Secretary Silver Medal, which is the second highest award granted by the Secretary for exceptional leadership and diligence. This work, I think, was particularly on her tireless efforts on REAL ID.

And then, finally, a member of our international team received -- was part of a team award for DHS excellence recognizing of the entire negotiating team for the passenger name records negotiation, which concluded last summer. So the office has gotten some very positive recognition.

I think, just looking at the future, again, I'll emphasize some practical areas, and then some substantive areas where I see a lot of demand for the office. We'll be doing a lot of growth in the training area, a lot of growth in the incidents and inquiries area. Substance -- we're going to be taking on a lot of work in cyber security, identification management, ID theft and also, finally, really trying to close out the -- get ourselves into the full compliance with the SORNs and, of course, the PIAs.

So with that I'm also going to take the opportunity to put in a personal thank you to Ken Hunt, Sandy Hawkins, Tamara Baker and Rachel Drucker for arranging the meeting here today in El Paso. It's a lot of work to pull together all the logistics from afar to do this meeting.

And then finally a note of thanks related to the committee for your hard work and you’re sticking with this. Your work is certainly very much appreciated by the Department, and we continue to look forward to working with you. So with that I think I've run out my half hour and would be happy to take any questions that you have.

MR. BEALES: Thank you, John. You have my congratulations, and I'm sure the Committee's to Becky and to Toby for their awards. That is wonderful news. And I would just note in the -- if this global privacy dialogue is going forward, that perhaps the Committee's framework document would be a useful background piece for that. If you are going to revisit the principles, that seems like a wonderful place to start is with that framework.

John Sabo.

MR. SABO: Thanks for your comments, flattery about the work of our committee. Two areas you talked about, the Einstein 2.0 PIA, but more particularly you talked about the cyber area being an area of future emphasis. Can you -- and some of us had in our subcommittee yesterday -- had some dialogue about the possible role of the advisory committee in aiding some of the cyber work.

Cyber initiatives to protect the government and private sector's cyber infrastructure means a huge amount of data collection, information sharing. The attacks can be based on content, as well as technical attacks such as denial of service. So there's a whole range of implications for data privacy.

And I'm wondering if you could expand a little bit on the areas that you see the department and the Privacy Office, in particular, playing in that space and, B, whether you see a role for the advisory committee to assist you in any way?

MR. KROPF: At this point on the cyber, the cyber area, our Director of Science and Technology has been Pete Sand who has been very much close to this project, and he's been brought in from the beginning so he's kind of -- I would describe him as sort of our scout who is way down the road getting involved in looking at how they are planning to design some of these systems.

And because he's down the road a ways, he's able to scout out an issue spot for the folks that are designing the cyber security systems. And his work with the Einstein, if you will, 1.0, is already up there and on our website. And shortly we expect to have the 2.0 out on the website.

I want to look over my shoulder here for a minute to see if Pete is in the audience. And, also, just a little bit constrained in terms of how much detail I can go into because much of the cyber work is fairly sensitive, but what I might encourage is an offline conversation with Pete and yourself to talk about -- I do think that there would be room for the committee to make some contribution here, and if I can leave it at that –

MR. BEALES: Ana.

MS. ANTON: I would like to thank you, Mr. Kropf, for your update and am happy to see so many wonderful developments and great work, and I can certainly congratulate Becky and Toby for their work as well. You mentioned that you had received data privacy complaints, and I was wondering what type of complaints you've received or types of complaints you received and how the office is addressing those.

MR. KROPF: We have just filed our first 803 report, and I'm going to pause for a moment and look over my shoulder to the people that really know the numbers. I think -- if you wouldn't mind, if I can bring Becky up to the microphone since she actually prepared the numbers.

MS. RICHARDS: So our very first report is actually a narrative report, and that will be going up on our website in the next week or so. It just is in the midst of being transmitted to Congress so we don't put anything up. On there we describe the complaints as basically three types so there's no numbers at this point.

We're in the midst of doing our second quarter one, and so probably in the next two weeks those numbers will come out, but we basically, in our first iteration of this, have three categories of complaints.

One has to do with sort of notice and transparency so complaints about that, things that would be incorporated in there would be if there were comments on a particular rulemaking, on a particular system of records where people are saying that we are violating their privacy, you know.

As an example, the automated targeting system received a number of comments that claimed that we were violating their privacy. Those would be counted in that group.

The second group has to do with redress. So redress are -- you know, I am on the watch list. I shouldn't be on the watch list or, for example, TSA has a number of programs where they are going through and credentialing people. Something comes up in their background that says you have a disqualifying crime. They go back to TSA.

TSA does further review and either makes an adjudication that says, no. You do have a disqualifying crime. Thank you. You can't have the credential or oh, no, we have now corrected that information. Here's the credentials.

The third are the general ones, and I think as we gain experience and knowledge, we will further flush those out, but these are just sort of the general -- I'm trying to think of one of the examples that we gave.

They were just sort of vaguely -- they said it was a privacy problem. They didn't like something. Most of the complaints we get actually get referred back to someone else so referred -- so actually an example would be we've been getting quite a few complaints regarding CVP's search authority or searches at the border, and we refer those to CVP for them to handle.

Secondly, we will get complaints that are saying you are wiretapping us, and the PATRIOT Act is horrible. I get the PATRIOT Act is not the -- the Department of Justice, and we refer those. The resolution, as it will be reported, will say it's resolved, pending, referred or not resolved, unable to assist.

Unable to assist is the best example we have. You had a disqualifying, you know, crime under a TSA credentialing program. You do, in fact, have that. You don't meet the standard for it. We can't really help you. So those are how the complaints in this first go-round will go.

We have quite a bit of -- I think it will take some time to get some additional reporting as we go through, but those were sort of the first, and that was similar to an interagency group that separately had met and come up with some of the categories.

MS. ANTON: Thank you.

MR. BEALES: Any other questions?

MR. PURCELL: I have a short question on the PIHGs, the Privacy Incident Handling Guide. Can you explain to the committee the distribution and deployment and training on that incident guide inside the department so we better understand not only that there's documentation about what to do, but that there are people who are familiar with the documentation and ready to take the needed actions?

MR. KROPF: I'll start and then, of course, Becky will correct the mistakes. It had been put out department wide and, I believe, distributed to all the PPOs, the privacy points of contact within all the components. We have also -- we're bringing on line additional training that will be more than just privacy 101.

There will be specialized training that will be targeted to meet -- depending on the manager's level of access and encounters with personal information, the privacy training will be sort of tailored to meet their levels of expertise. And so we're trying to build training modules that will help reinforce the PIHG, the PIHG material. With that, I'm going to give this to Becky.

MS. RICHARDS: So the PIHG is -- Toby Levin and Cathy Lockwood have been really pushing this forward, and they have trained every -- Cathy has gone in and trained every single one of the Privacy Points of Contact.

She works tirelessly with the Security Operations Center, and we have worked extensively with the Information Systems Security Board and the Information Systems Security managers so we are just latching on to an existing process whereby security incidents are already made -- already go through and are reported.

We then have trained the Privacy Points of Contact on how to do that, and then any privacy incident that comes through is reviewed by our office and closed as being handled appropriately. So there's been quite a bit of extensive and ongoing training.

We meet on a monthly basis with the Privacy Points of Contact, and the training and discussions of particular incidents are otherwise brought up during that time as appropriate to provide further training to those groups of people.

We can always do more and better training on anything related to privacy, but Toby and Cathy have done an amazing job of really getting this up and off the ground and incorporating into existing processes so it's not something that's just sort of strange that's specific to privacy.

MR. BEALES: Thank you very much, John. We appreciate your report.

This morning we have two panels on E-Verify. We will start with a panel on the federal perspective and follow that up with a panel addressing broader public perspectives. Our first speaker today will be Ms. Sonja Barnes who is the Chief of -- the Acting Chief of the Customer Relationship and Learning Management Branch in the Verification Division of the U.S. Citizenship and Immigration Service.

She is responsible for all external facing components of the Verification Division, which includes a support section, a training and staff development section and an outreach section. Prior to joining the Verification Division in 2007, Ms. Barnes worked for the USCIS Information and Customer Service Division on quality assurance, call monitoring, training and performance objectives for the National Customer Service Center.

I think what I'll do is to introduce you in turn and let you speak in turn. And then if you could confine your remarks to 10 or 15 minutes, we can come back at the end with questions for all three of you. So, Ms. Barnes.

MS. BARNES: Sure. It's great to be here. Thank you for inviting the Verification Division to your meeting today. The Verification Division -- I'm not going to add any more to my bio. That's it in a nutshell. The Verification Division not only manages the E-Verify program, but also the SAVE program as well, which is the segment of the verification process in which government agencies use to verify those who are applying for benefits.

E-Verify was once known as the basic pilot program, which was mandated by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996. It is a partnership between the Social Security Administration and the Department of Homeland Security, and it does provide for employers a means of -- to verify the employment eligibility of their newly-hired employees.

Just to make it a little simpler, I did bring a PowerPoint so you can follow along with me. We have several program goals. That is to support the need to reduce unauthorized employment in the United States. We want to minimize verification related discrimination, and to -- you know, with the understanding that when the law was enacted -- IRCA was enacted, that employers were then placed in a position of feeling as if they had to become document experts, so E-Verify, in terms, helps the employer out in that respect.

We want this to be quick and non burdensome to employers, and we're also interested in protecting civil liberties and employee privacy, which you'll hear later we have a privacy branch that is included in our program to meet those needs. The privacy branch -- and I do have with me today -- we have a couple of individuals who are members of the -- staff members of the privacy branch.

Their job is to protect the E-Verify records in the manner consistent with all applicable privacy laws and regulations, to secure and mark personal information as confidential and to ensure that the information is restricted, and that only those who have a need to know receive this, the private information. And to assure that we are doing what we should be doing in terms of safeguarding the data that's used.

I'm just going to take a few moments to go through how the E-Verify process works and what the responsibilities are of employers and employees. We start with the I-9. This system, this process does not negate the I-9 process. That is still very real and it is still the expectation that employers will use the I-9 process. However, the information that's acquired from the I-9 form is what we use to verify with E-Verify.

The system queries the Social Security Administration databases and that of the Department of Homeland Security. Within a matter of seconds, the employer -- once the information is provided in the E-Verify system, they will receive one of three different responses that is of employment authorized or SSA tentative nonconfirmation or the employer may receive a response that says DHS verification in process.

And what happens, at that point, is that the information is transmitted to a team of immigration status verifiers that are in Los Angeles, and those verifiers will then check in additional systems to see if there's an issue that they can resolve. And a response will be returned to the employer within that 24-hour period.

If the employer receives a message that the employment is authorized, the employer then records the information on the I-9 form or they may print out a copy of that page and attach it to the I-9 form. If there is a tentative nonconfirmation, the employee then has the right to contest, and this is very important. The employer would then make a -- print out the notice from the E-Verify system.

And depending upon whether or not it's an issue with the Social Security Administration database or a discrepancy with the DHS database, the TNC notice will then explain to the employee what is taking place. And it is a manual process, and the employee and the employer would then sign that form. If the employee chooses not to contest, then the employer has the right to terminate employment with that individual.

And this simply reiterates what I've just stated, that the employee has the right to contest. It is a manual process to print and review the TNC with the employee. It is expected that there is a conversation between the employee and the employer. The employee is then referred, if they choose to contest, to the appropriate agency that is of SSA or of DHS.

And there is -- by the way, there's an 800 number that is provided for those who receive a TNC based on a discrepancy in the DHS database. The employee has eight federal government workdays in order to contact one of those two agencies in relation to the TNC. And, for your review, this is simply a snapshot of the tentative nonconfirmation form that is provided to the employee.

This information, at this time, is available in English and in Spanish. However, plans are being made to make it available in other languages as well. Once the TNC is -- the employee decides that they want to contest, then there is a referral notice that is provided to the employee that provides instructions on how to either contact the Social Security Administration, if it's related to Social Security or to contact DHS, instructions on how to -- the telephone number to call.

What's also emphasized over and over again in the MOU and in the education that we provide to employers is that the employee continues working throughout the TNC process. Once the employee resolves a discrepancy in the records, then they should inform the employer. However, with both the SSA, TNC and the DHS TNC, the response is automatically sent to the employer so the employer will simply go back into the system, and they will receive a response. And that response will either be of an employment authorized, final nonconfirmation or review and update of the employee data, and then resubmit, and then the employer would, then, resolve the case in E-Verify.

The employer has certainly responsibilities. This is indicated in the Memorandum of Understanding that the employer signs, and also in all of the education that's provided to the employer. E-Verify can only be used to verify new hires, and it must be initiated after the employee accepts the position and within three days of the employee's actual start date and just to add to that this is a process that takes place after the I-9 form is completed.

E-Verify procedures must be applied to all new hires regardless of their citizenship status. The employer responsibilities also include the posting of a notice in an area that's visible for prospective participants so that they are well aware that the employer is an E-Verify participant, and there is also a notice that's posted, the antidiscrimination notice from the Office of Special Counsel for Immigration Related Unfair Employment Practices in an area also visible to the perspective employee.

And, again, this just gives you a visual of the posters that the employee will find at the employer's site. I want to emphasize the employee rights. The employee has the right to contest or not contest. Every employee has that right. And the employee, if they believe they are or have been discriminated against, they are provided a telephone number. That telephone number is on the TNC notice and also on the referral notice.

If they feel that they are being discriminated against by the employee -- excuse me, the employer, then they may contact the Office of Special Counsel for Immigration Related Unfair Employment Practices. The registration process for employers -- they are responsible for reading and understanding the Memorandum of Understanding between DHS and SSA.

Once they have signed the Memorandum of Understanding, they are then provided a name, the password and the E-Verify website, that they would then use to verify new hires on. However, prior to gaining access to the system, they are responsible for downloading and reading the user manual and also completing an online tutorial. An online tutorial requires the employer to go through each page of the tutorial of the manual, and also to take a mastery test at the end of completing that tutorial.

The employer is then responsible for downloading the E-Verify participation poster and the Office of Special Counsel on discrimination poster.

What has been done rather recently, September of last year, is that the E-Verify now has pictures of those who -- if someone has a green card or an alien registration card, and the -- or the employment authorization card, that information -- those pictures are now available in the E-Verify system. These pictures were included in the database in order to assist with the concerns with the employee being -- you know, our need to detect against the instance of document fraud.

Here are just a few statistics. We are now over 56,000 employers participating or using E-Verify. Over 3.2 million queries were run in 2007 and so far this year we are at 2.7 this year. 92 percent of the verification queries are instantly verified, and what you see here are some of the top industries that are currently signed up to use the E-Verify system.

E-Verify improvements -- we want to reduce the incident of mismatches. We recognize there is a segment of the population that are affected more heavily than others in terms of the need for -- the TNC's coming up there are persons who are newly naturalized who these -- the Social Security databases may not have this information available if they were naturalized the day before they applied for a new job. It would be affected.

We also are developing a marketing plan to recruit employers. We began the testing in the environment of the marketing and the media in Arizona. There were billboards. There were online ads. There were print ads in the Arizona area to educate employers as well as employees, about E-Verify. And we want to do that on a more national scale in the future.

We are also developing monitoring compliance functions. And the monitoring and compliance group that we have, what they are doing is looking at the information in the E-Verify database and looking at the employer behaviors. Our goal is to be sure that employers are compliant and that they are using the E-Verify system in the manner in which it is -- they have agreed to.

And here is just a snapshot of some -- the state legislation. And this happens to change almost daily. However, we have a team, a strategy team who are looking very closely at what is happening in various states. Arizona is the most -- has the most far-reaching law at this time, which requires that all employers in the state of Arizona utilize the E-Verify system in order to verify new hires.

There is also a general information line available for those who have questions about E-Verify and what is also planned is an employer hotline, as well as an outbound call system, in which -- again, we're using education more and more to ensure that employers and employees are aware of what the E-Verify system is all about, what the impacts are and what the -- they can be sure to use the system the way it's meant to be and employees are aware of what their rights are. That's all I have this morning. I can answer any questions that the panel may have.

MR. BEALES: I see that there are a great many questions, but I think we will come back to that at the end of the panel, and we thank you very much for being with us this morning. This is very interesting.

MS. BARNES: Thank you.

MR. BEALES: Our next speaker will be Jon Cantor who is the Executive Director of the Office of Public Disclosure at the Social Security Administration. Jonathan started his legal career in 1996 as a summer legal intern with the Office of Corporation Counsel in DC. He graduated from law school at George Washington University National Law Center in '98 and joined the Social Security Administration Office of the General Counsel where he focused on FOIA and Privacy Act and Computer Matching and Privacy Protection Act issues.

In October of 2003, he became the deputy executive director of the Office of Public Disclosure, also serving as FOIA and privacy officer. And in 2005, he became the executive director for Public Disclosure. He received his AB degree cum laude from Duke University in 1994.

Jonathan, welcome. We look forward very much to hearing from you.

MR. CANTOR: Thank you very much, and I'm glad to be here in El Paso. And the first thing I want to do is thank all of you for being here. I also want to thank Ken and Sandra and everybody in the DHS Privacy Office staff for putting this together.

What I've decided to do a little bit is talk a lot about -- explain a little bit about the Social Security Administration, privacy at Social Security, and how Social Security is involved in the process that's now known as E-Verify.

As my bio pointed out, I am the Executive Director of the Office of Public Disclosure. In tremendous federal government speak, that's sort of Social Security's chief privacy officer position. In Social Security, the way that we're organized, I report directly to the General Counsel who reports directly to the Commissioner of Social Security. The commissioner of Social Security is the Social Security Administration version of a secretary.

So just a brief primer on Social Security. I assume that most of you have probably heard of us. We are an agency. We date back to the 1930s. And to understand how we're involved in E-Verify, you really have to understand our program in context.

The Social Security Administration was created during the height of the Great Depression and during the days that were leading up to World War II. At that time, the Social Security Board, as it was then known, began to implement a popular program that would help people maintain a certain level of financial security during retirement.

The program, which is basically the same program that is still in place today, is an insurance program where all employees, nationwide, contribute a certain payment via tax on earnings, and employers also contribute a share. Self-employed individuals are lucky to contribute both shares.

Upon reaching retirement age, the employee becomes eligible for benefits based on his or her earnings and insured status. The program also allows widows or widowers to collect on a deceased spouse's earnings, and for dependents, auxiliaries and others, they can also collect as well.

The program also includes a disability insurance program, which provides similar coverage to an employee should he or she become fully disabled and unable to work. And that disability program also covers family members, depending on the circumstances So that Social Security tax that both employees and employers pay funds both of these programs. So there's tremendous nexus between the Social Security core programs and employment.

And so, of course that's where Social Security began collecting the type of information that Sonja was just talking about that they are interested in reviewing. Many years later Congress established the supplemental security income program, which is similar to the disability program in that it provides a cash payment to certain disabled individuals. Unlike the disability program, however, SSI does not require a person to obtain any insured status to qualify. Instead it's an income-based program.

So how do we do this? These programs are huge and they cover nearly every person in the country and many workers overseas. Going back to the 1930s, Social Security required some sort of easy efficient manner to work with employers to collect earnings information on all those individuals across the country and keep it filed on employees.

Given what was going on in Europe at the time -- remember this is the point I pointed out about World War II .there was a strong sentiment about avoiding anything like a national ID card. And so the solution was a Social Security number, which was a nine digit number, and back then the purpose was strictly for reporting to Social Security. It had no other value. It was not used in the private sector. It was not used in education. It was not used for other purposes.

And as the program rolled out, people applied for numbers. And so our system in use today is still the one that we developed in the 1930s. The first three numbers are called the area number. The second two are called the group number, and final four are called the serial number. The area numbers are assigned geographically. The lowest numbers are in New England and the higher numbers are toward the west.

The group numbers are assigned in sort of a strange even/odd sequencing, mainly for processing purposes, and the serial numbers are assigned within each group number until they run out of numbers. We've recently sort of started to find in certain areas of the country that we're running out so we're going to shift that plan around, but that's very, very recent.

The numbers are never reassigned. When a number assigned to a person who has passed away or that we reassign for some other purpose will never be reused. Obviously, we will eventually run out of these. We still have around 500 million left to use but, you know, we will eventually run out.

There's a lot of information that the public has asked for and we have shared over the years about how the process works. That is widely available in our Freedom of Information Act website. Privacy was an early consideration of Social Security, and the first regulation issued by the Social Security Board dealt with personal privacy.

So in 1937 Social Security issues a regulation on personal privacy. The members of the board recognized immediately that collecting earnings information and other personal information created a need to protect that information from widely sharing it with others, other agencies, other individuals.

It was in the current version, still is widely called within the agency Regulation 1. At the time there was no Open Records statute like the Freedom of Information Act or the Government Sunshine Act, but the regulation did provide a right of access to individuals.

There were restrictions placed on disclosure to third parties. Again, that was for the years before the Federal Privacy Act came into being. The regulation recognized that so much of the information was being provided to Social Security under a mandate of federal law, and so people had little choice in participation, and thus the regulation was really focused on making sure that the information was used properly within Social Security or as otherwise mandated by law.

Employees were trained in what the regulation meant, and that training is still a part of new employee training at Social Security today. It's been updated a little bit, but it's still the same kind of core training. Over the years as notions of privacy have evolved and changed so has the regulation.

Eventually, Congress added a provision to the Social Security Act, which dealt expressly with the Privacy Act, which gave the additional authority and statutory underpinnings to our regulations. The regulation now encompasses Privacy Act protections and leverages those Social Security Act provisions. Social Security has used our regulations to narrow the discretionary provision related to disclosure without consent from the Privacy Act.

For example, we place conditions on law enforcement disclosures, disclosures pursuant to court orders, and on the definition of compatibility as that term is used in the Privacy Act. Again, that underlying principle, again, is that participation in Social Security programs is not optional and so limits need to be placed on the disclosure of personal information.

In fact, we recently amended our regulations to include the Privacy Impact Assessment and to clarify confusion over obtaining access to medical records. So some of these things were to incorporate the changes that came in from the Act of 2002. Social Security has always had a tremendous role in helping the federal sector administer similar types of benefit programs, as well as assisting the states and local entities in doing the same.

So Social Security programs are closely related to other government insurance programs, thus retirement eligibility and Medicare Health Insurance work hand in hand, and SSI and the Medicaid program also have a close nexus. Many states also have a supplementation benefit on the SSI payment.

And so we work closely with the states, the Department of Health and Human Services to help administer the Medicaid and Medicare programs, and the SSI supplementation. We work closely with the Veterans Administration, the Department of Defense, the Office of Personnel Management on their pension, retirement and disability programs, and we work with them to assist each other.

We all work together to assist each other in the administration of each others' programs. There are offsets that are very complicated. We work with nearly every state on similar health and income maintenance programs, such as low income heating and energy assistance, state welfare programs, medical programs that often supplement the Medicaid program, and certain other similar programs.

In many of these our cooperation is also statutory and mandatory. We also cooperate in activities in which we are required by law to participate. Some of those include our cooperation with the Office of Child Support Enforcement, Internal Revenue Service, Department of Homeland Security, Department of Education. So E-Verify is one of these programs.

And as I talked about earlier, Social Security's connection to employment goes all the way back to the beginning. We collect a tax that helps administer our programs. Employees are required to present that Social Security number to their employers so the employer knows which number to tell Social Security and the IRS that they are working for us. That helps us track the earnings.

There are now provisions in the Social Security Act and the Internal Revenue Code requiring Social Security and the IRS to cooperate in a unified tax processing system. Both agencies are required to collect information from employers on earnings. Social Security is the first point of contact to process all that information, and then pass it along to the IRS.

As Social Security is the agency that issues the numbers, we're the only one who can absolutely verify that a name and number are in line. We carry out that work with employers on a daily basis and always have. Showing proper wage reports allows those employees who become eligible for our program to obtain a proper benefit. If a report cannot be associated with an employee, it goes into suspense until we are able to associate it.

Many of these wage items are collected when somebody files for retirement disability and we are able to work with them to figure out from their records and our records, okay, this is where that suspense item is, and then associate it, but Social Security does not, however, have a role in determining work authorization.

That role used to be handled by the old Immigration and Naturalization Service, which is now part of the Department of Homeland Security. So E-Verify, as somebody pointed out, came along in 1996 when Congress enacted the Illegal Immigration Reform and Immigrant Responsibility Act, and that required the testing of three alternative methods of providing effective, nondiscriminatory employment in eligibility processing.

And the basic pilot, as it was then known, and is often still called in Social Security to many of us, was one of those three pilots, which was initially available in just seven states, which were those with the highest estimated populations of aliens unlawfully present in the United States.

The pilot was deployed and evaluated over four years and slowly expanded by Congress two additional times to now include all states, DC, Guam, Puerto Rico and the United States Virgin Islands.

(Continues less than 5 minutes off the record due to equipment malfunction.)

MR. CANTOR: The DHS -- the DHS system, and in my mind, I like to break it out. Because of privacy, I like to talk about where the systems, in fact, interface with each other so how it moves to help me keep my hands in the technical guide when it moves from A to B.

And so the DHS system helps collect information directly from the employer reading information provided by the employee from the I-9 form and that system, the DHS system, transmits that information from DHS to Social Security.

Social Security verifies whether the name, Social Security number and date of birth match using our information system. The DHS and that system cannot query the system directly. The system passes the query to SSA's architecture. If an individual employee alleges that he or she is a citizen, we will attempt to match that information with any information in our system.

If he or she is a citizen, he or she is work eligible, and in many cases that's simply what it is. We're able to determine very quickly that the person was naturally born here and was given a number at birth and fly right through.

If he or she is a non-citizen but the person has a valid name SSA/date of birth combination. Social Security will refer the employee back through the system to DHS and then DHS, as Sonja points out, will make a decision on work out authorization status.

And as she pointed out, employers have a very high success rate using the system. She said the latest statistic was over 92 percent of employees are verified as work authorized within seconds. If Social Security is unable to match the information or we are unable to determine United States citizenship status, we reply to DHS and the employer through the system that there is a tentative nonconfirmation.

And when that happens, employers are required to tell the employee so that the employee has time to contest the information. Employers provide the employee with that referral letter. And if contested the employee can then visit the Social Security office to correct the information.

In many, many cases, probably in the vast majority of cases, it may simply be an error in data entry. There's a lot of times where there's data entry and it takes place in that process. The person puts their information on a form. Somebody types that information on a form into a system and sends that.

So, for example, the employer may miskey a name. They may flip around digits in a Social Security number and similar types of problems. Those will trigger a mismatch and that will trigger a tentative nonconfirmation.

Employees may have also failed to update Social Security on their status in life. When a person changes a name after marriage, for example, he or she may fail to tell Social Security, thus the name wouldn't match. This problem frequently occurs when a person applies for benefits with Social Security as well.

Frequently people naturalizing as citizens do not inform us of the change in status. It was not uncommon, over the years, for people to lie about their age when they were applying for Social Security. Some people did it for the vanity reasons because they didn't want people to know how old they were, and some people did it because they wanted to work earlier than the state law permitted.

State laws often have a minimum age; 15, 16. Some people would go apply for Social Security numbers when they were 14 because they were ready to work. And these problem -- people forget about it over the years or realize when they get that information in a different context that it may trigger a mismatch with us. So these problems come up when people apply for benefits as well, and with appropriate evidence we can resolve these errors.

For example, in those dates of birth problems, we work with the state bureaus of vital statistics or registrars to ensure accuracy to get certified copies of birth certificates. And we're able to update those records, and that information would feed back into the system, and the employer is able to follow up and verify to check the status of the tentative nonconfirmation.

Again, that system contains that information so even if the employee, after they visit Social Security, forgets to take that last step of telling the employer I visited Social Security and took care of everything, that system could -- now contains that information where the employer can log on to the system and check the status. So that's Social Security role in the system. Thank you.

MR. BEALES: Thank you very much, Jon.

Our final speaker on this panel is Neville Cramer who has spent 26 years as a law enforcement officer with the Immigration and Naturalization Service. At the time of his retirement in 2002, he was one of the most experienced INS special agents in the INS.

He began his career in 1976 as a border patrol agent, after four years as a police officer in Arizona and Florida. After his tour of duty on the Mexican border, Mr. Cramer served eight years as both a special agent and a supervisory special agent in Chicago and Washington, D.C. and the district offices.

He is the author of Fixing the Insanity, America's Immigration Crisis in 2003, and also Immigration Chaos, Solutions to an American Crisis that came out just last month.

Mr. Cramer, welcome, and we look forward to hearing from you.

MR. CRAMER: Thank you very much. It's certainly an honor to be here. This is quite a thing for me to be in front of this committee for several reasons. What was not mentioned, and I probably failed to submit it, was I was the original developer of the SAFE system at INS in 1984 before the Immigration Reform and Control Act.

So I have quite a history with verification and data integrity and so forth. In fact, historically, I can remember when Social Security wouldn't even sit at the table with INS so it's nice to see the two of you sitting over here to my right. And when I was -- sitting together.

And I can remember when I first began developing or we began developing the SAVE program, I was called over to Main Justice and asked about data integrity and privacy, and it was in some dark room over there in Main Justice so looking at the committee today, I think it's wonderful that we've come this far.

I was asked to come here today and represent the State of Arizona. I'm a resident there and have been quite involved with Representative Russell Pierce who is the head person who developed HB-2779, which is the Fair and Legal Employment Act in Arizona. I'm not sure if you are familiar with it, but very briefly this was the employer sanctions law which was passed in Arizona last year, signed by Governor Napolitano, and has been tested in the courts, which is very interesting.

The federal court, three times, took a look at this and has gone up to the Ninth Circuit, and the Ninth Circuit has recently decided not to issue an injunction against the implementation of this law so it looks as thought it is going forward. And as Sonja mentioned Arizona -- employers in Arizona are now required, as of January 1st of this year, to use E-Verify.

That is something which America has never seen before. I would simply like to now interject two pieces of history, which I think is critical to this entire conversation. First of all, back in 1988 after the beginning of the implementation of employer sanctions in the Immigration Reform and Control Act, the failures of the I-9 process became quite evident.

And I have here a GAO report, which is entitled Immigration Control, A New Role for the Social Security Card, and its date is March of 1988. I simply bring this to your attention to show you that there is a historical relationship between the verification of

Social Security numbers and immigration control in this country, and it goes back many, many years.

After, again, the realization that employer sanctions was not working, the Congress authorized the Immigration Commission or the Commission on Immigration Control headed by Barbara Jordan from Texas, the late Congressman Barbara Jordan. I would simply like to read to you one comment that came out of this commission.

It says a computer registry to verify that a Social Security number is valid and has been issued to someone authorized to work in the U.S. is the most promising option for eliminating fraud and reducing discrimination, while protecting individual privacy. The date on this report is September of 1994. That's 18 years ago.

Ladies and gentlemen, there is a significant relationship now between controlling illegal immigration and verification of Social Security numbers and immigration status. We have not had it mandated by Congress, but there is pending legislation right now in Congress. And as I mentioned, I'm here to represent the State of Arizona, which has legislation in place right now.

It is premature for me to start giving you anecdotes about people fleeing the State of Arizona because of this law or employers discriminating against people because of this law. It is absolutely premature because we have only had basically three months to implement this law.

We don't know of any instances where individuals have been denied. And, as I mentioned, anecdotes are not what I came here to tell you so I am simply going to ask you if you have any questions of me. I do have a couple of things I would like to bring to your attention before I end.

We have had great success, by the way, with the use of E-Verify. However, there are some questions that we have that have been raised about the State's usage of the information on the I-9, our access to the I-9 and our access to the data that comes from the E-Verification system for enforcement purposes.

Secondly, we are not certain how much cooperation we are going to get from CIS and from ICE regarding enforcement activities, but, again, we have had no enforcement activities so we don't know whether that's a problem or not.

And lastly, there is a paucity of handbooks that are currently available for employers to use if they don't go online regarding the use of this system, but I'm certain that CIS will be working on that and they have done a tremendous amount of advertisement on radio and billboards, as Sonja mentioned, so I am finished and look forward to your questions. Thank you.

MR. BEALES: Thank you very much. Our first question will be from Tom Boyd.

MR. BOYD: During my government service many years ago, I was intimately involved in the creation of the '86 Act and working with Al Nelson who was then a commissioner. The executive branch then and subsequently failed miserably with respect to enforcing employer sanctions, and as a consequence of that we are where we are.

Now, you mentioned in your remarks a moment ago that there is a pending piece of legislation at the federal level, I assume, which is preemptive, I assume, and would mandate the use of the E-Verification system; is that correct?

MR. CRAMER: Yes, Mr. Boyd. The legislation is termed the SAVE legislation. It is -- was put forward by Heath Schuler, a Democrat from North Carolina. It is supported also by many Republicans, one that was on the television last night talking it was Republican Bill Ray from California. And it is legislation that would mandate E-Verification throughout the United States.

And I won't go into the -- my feelings about it. I think it's a good piece of legislation, but I am one who thinks that we need to take a look at this thing as a lot bigger picture, but you are absolutely right.

And I can tell you historically that the executive branch was not only responsible for the failure of employer sanctions, but that there was a feeling within the INS that there was no way that we were going to allow verification to be part of that I-9 process. That was from the day that the legislation in 1986 came over to INS.

MR. BOYD: I remember.

But I have a question for Ms. Barnes with respect to that legislation. What kind of a priority is there at DHS to see that the preemptive legislation is enacted, since I gather the way it's proceeding now is a case-by-case, state-by-state basis, and each of the states is consistent with the other?

MS. BARNES: Well, I'm not sure I can answer your question in detail that you might be looking for. We are aware of the legislation. We were aware of legislation that was very close to being enacted, we felt, last summer. We're just pushing forward. We're ramping up.

If Congress decides that there will be mandatory legislation or legislation in place that would require all 50 states to use E-Verify then we simply want to be ready to meet that need.

MR. BOYD: I gather from that -- sorry to interrupt you, but I gather from that it is not a priority of the department. You are saying you are aware of the legislation so it is –

MS. BARNES: It has mandated its way into being a priority that's driving any of the work that we are doing.

MR. BOYD: Is there any reason that the department has not supported, as part of its own legislative agenda a preemptive piece of legislation.

MS. BARNES: No. I would not be able to answer that for you.

MR. BEALES: Neville Pattinson.

MR. PATTINSON: Thank you, Mr. Chairman.

My questions, which are three short questions -- at least I'll try to make them short. First of all, you talk about the eight days required for somebody to lodge a challenge to the decision. Once they have done that, what is the time for resolution? There doesn't seem to be any kind of a response back to the individual that it will be resolved in 30 days, nine days or is open.

MS. BARNES: The vast majority are responded to and resolved by the tenth day.

MR. PATTINSON: Tenth day?

MS. BARNES: Right.

MR. PATTINSON: Do you keep records of the employers' queries to the E-Verify system.

MS. BARNES: Yes. There is -- the information pertaining to the record is held, yes.

MR. PATTINSON: How long is that held for?

MS. BARNES: That's held for -- and the folks in the back can help me out -- I do believe for a ten year time frame.

MR. PATTINSON: And the last question that I have is when you look at the employment verification to reverify, obviously it's linked to citizenship status or immigration status. The immigration document, in the case of an immigrant, may have a particular expiring date, such as a green card or so. Do you indicate to the employer, yes, they are valid for employment but it's for the next, you know, duration left on the immigration document?

MS. BARNES: The use of E-Verify does not negate the I-9 requirements as supported by IRCA. There is a reverification process associated with the I-9, and that is what the employer would, then, refer back to. E-Verify is not used for reverification.

MR. PATTINSON: Thank you.

MR. BEALES: If I could just interject my own question here, there was a recent enforcement action against an employer who had been participating in E-Verify. And the number of people who had been verified were determined to be illegals and not eligible for employment.

Can you tell me something about how that happens and where it is in the system that those kinds of false positives are coming from? Are they coming from the immigration side? Are they coming from the Social Security side? I mean, how does this happen?

MS. BARNES: It could happen because those persons were hired prior to that employer signing up to use E-Verify.

MR. BEALES: No. These were people that had been verified. The employer was not prosecuted because they had used E-Verify. It was just the illegal aliens who were deported.

MS. BARNES: Well, it could also have happened that the system, again, cannot detect whether or not someone has a false document, a fraudulent document in front of them. So the information that was input into E-Verify, the card that was used, the number, everything associated with someone who had valid employment authorization.

MR. BEALES: Do we know anything about the rate of those kind of false positives? I mean how often does this happen.

MS. BARNES: Well, I'm not sure if I have this information for you now. I may be able to provide that information at some time, but it's a very small percentage of persons who would be categorized as false positive in the E-Verify system. I just don't have the actual numbers. It's something like less than one percent.

MR. BEALES: And you don't know anything in these cases about what it was -- I mean what it was specifically in this set of cases that did result in enforcement actions, that was the source of the problem?

MS. BARNES: No. That was ICE that made the decision to go in and to raid that particular company.

MR. CRAMER: One of the things that obviously is going to be created with this verification system are packets of data that relate to an individual. Go south of the border right now and they will sell you a Social Security number, a green card with a photo that you have put on there.

So these packets of information will be coming across and be sold to the aliens that are coming in here to work. We know that that's coming. Not we, but ICE knows that's coming. One of the things that will come out of the use of E-Verify will be this Social Security number, this name and this alien registration number are going to show up in 50 or 60 different places at the same time, within a very short period of time for verification.

That indicates you have a problem. You have an identity which is being abused. That is something that will be transmitted back to the ICE and to the enforcement people, hopefully. I'm not part of it, but I know this is being discussed.

But to answer your question, I don't think anybody knows how many of those false positives there are out there, but once the verification begins to go en mass, it will be difficult to get through the system.

MR. BEALES: Because you are going to pick up the multiple entries.

MR. CRAMER: Absolutely.

MR. BEALES: And people have different identities in order to do this fraudulently. You need a lot of fraudulent identities, not a few.

MR. CRAMER: There's no way that anybody maintains this is going to stop anything. What it's going to do is curtail it. It's going to curtail illegal immigration. It's not going to stop it.

MR. BEALES: And who is it? At what level are we watching for these multiple queries against a single identity within a short period of time?

MS. BARNES: That would be the monitoring compliance group that we have in-house who are looking at those types of issues in the E-Verify system. We have been able to identify the circumstances where folks have used Social Security numbers more than -- and then a few times in the system thus far so that would be the job of that section.

MR. CANTOR: Just to touch on that point, you were just saying more than a few times. It's one of the interesting questions that we've worked on together between the agencies. One of the presumptions, almost immediately, when we are working with ICE is if it's more than once, it's going to be a problem and, at the same point in time, it's not at all unusual for an employee to have multiple jobs and may live in a multi-jurisdictional city, for example, Washington, D.C., which is three to five states.

Depending on which part of the area you live in, you could have a job that's in Baltimore, Maryland; Charlottesville, Virginia; York, Pennsylvania, and Dover, Delaware, and it's all doable in a couple days. And so you literally do have multiple people showing up in multiple jurisdictions with multiple jobs during the same calendar year, even short periods of time.

So you do have to monitor that. While you are looking for fraudulent activity, you also have to be careful that there are legitimate reasons that an employee would use his or her Social Security number to apply for a job in multiple circumstances because you can easily have more than one or two jobs at the same time depending on the circumstances

MR. BEALES: John Sabo.

MR. SABO: A quick question for Sonja, I guess, maybe Jonathan. Actually, Mr. Crammer's comments about sitting down with INS. I worked for a long time with the

Social Security Administration. I remember the old days that the culture of us to say -- to talk about the privacy advisory committee.

The culture was we do not share unless we must share, and even times when we must share, we fight it out. And I was very proud of that history at SSA, being very good stewards of data privacy. I think to some degree the Privacy Act itself has eroded that, generally because of routine use and other considerations, but I think that had always been a strong hallmark of SSA, and obviously the practice continues. And that's something to be proud of.

When you move a program, and the front end of a program to an agency, DHS, that has a really strong Privacy Office and does not have that tradition of protection, now the front end query is managed, as I understand it, by DHS so you are in a new ballgame with new privacy rules and privacy offices and so on.

So my question gets to the employer vetting piece of it. I know when SSA, some years ago, did an employer verification program, it was a hugely elaborate employer vetting process because a disclosure of yes or no on a match was considered a Privacy Act disclosure by the agency. It wasn't just a minor thing. It was a disclosure.

You could use it to test the system. You could use it to validate the combination of name, date of birth, number to determine, ah, this is something I could use for other purposes.

So the question would be what, you know, what steps are in place, given your slide presentation to validate that the employers who are applying for rights to access to get their e-mail and so on are really valid employers, and whether you have an audit process in place to ensure that these are valid employers?

It looks to me on the slide presentation like the online registration was completely electronic. And then I think you said they have an electronically signed MOU. I presume that means they hit an accept button or something. So could you just elaborate a little bit on, A, the process for an employer and, B, your process for auditing employer use of the system to ensure that it's not misused, for example, browsing or using it to match a set of numbers.

MS. BARNES: Well, the program has been around for some time. However, the resources haven't been. And prior to the last year, there really had not been a lot of attention placed on finding out whether or not employers are actually -- have companies and/or employees. I'm going to refer back to the monitoring and compliance group, and also the E-Verify programs who are working together.

We are currently taking a look at the list, at the employer list, and at the information that's provided by the employers, but going forward there would be a much more intense look at validating the information that's in the system.

However, it's not something that I can tell you that has been in place in the past, but it is something that's being done now, now that we have resources and the additional staffing in order to get the work done. At the rate of 1,000 employers signing up per week, you can just imagine that it does take an enormous amount of resources.

And we're currently staffing up, and there are other offices that are being opened in other areas so that we can stay on top of the employer list.

MR. SABO: Just a quick follow-up. So what you seem to be saying is there is no independent verification that an application as an employer is actually an employer as of this time, and, B, you also seem to be saying there is no audit process against the employers. In other words, Mr. Cramer's point about this will generate good information related to multiple accesses across the country.

Particularly, I'm focusing more on the users of it. You have brokers who give you packets of information. One could conceive of brokers who take a combination of name, SSN, DOB, and create an employer account and begin using it for test purposes.

So basically you are saying that, as of this time, you don't have those processes in place. Is that a correct statement?

MS. BARNES: More or less, that is correct. Not to say there isn't work being done in terms of looking at the list, but there would be more emphasis or more resources on that in the next -- as we move forward with the program as we grow with the program.

MR. BEALES: Could you at least verify against Social Security records that is an employer with an EIN who is actually paying payroll taxes?

MR. CANTOR: The information we have on EINs directly from the Internal Revenue Service so it's tax return information and we're not permitted to use it for a non-tax reporting purpose.

MR. BEALES: Okay. But you could look at whether this -- or could you. Is there a system where you could look at whether this employer was actually posting wages to this Social that they were inquiring about.

MR. CANTOR: Well, if they are new hires, we wouldn't know.

MR. BEALES: That wouldn't be -- okay.

MR. CANTOR: E-Verify is, by definition, a new hire system. It would be at least a year before we would have any data in there that they were working there.

MR. BEALES: Okay. So there really is a problem. Okay.

Dan Caprio.

MR. CAPRIO: Just a quick question for Ms. Barnes. You mentioned, I think, in response to Mr. Pattinson's question about the resolution and the mismatch, usually within ten days or so, but my question is sort of two questions.

What, if any, is the responsibility of the employer during that period of resolution? And then the second question is who ultimately has responsibility for correcting the information in a mismatch environment.

MS. BARNES: The employer's responsibility, of course, is to notify the employee that there is a discrepancy. The employer is also expected not to do anything in a person's employment that is adverse to that person's employment, such as if there were training scheduled, that individual is still expected to go to training. Nothing in their job experience should change.

The employee, however, is responsible for contacting either SSA or DHS to initiate the resolution of the discrepancy. That is the employee's responsibility. An employer, then, would only have to go back to the E-Verify system to find out whether or not the discrepancy has been resolved.

MR. CAPRIO: And the 8 percent or so of cases where you found the mismatch that were resolved within the ten days, who has the ultimate responsibility to correct the record.

MS. BARNES: The agency would then correct the record and transmit that information in E-Verify, after the employee has contacted SSA or DHS.

MR. CAPRIO: Does SSA correct the record or does DHS.

MS. BARNES: I'm sorry. It depends on the nature of the discrepancy. If it is a Social Security Administration-related discrepancy, then, it would then be the Social Security office's responsibility to correct the discrepancy. If it's something associated with DHS, then, of course, DHS would then make sure it's resolved.

MR. CAPRIO: Thank you.

MR. BEALES: On a related question, there was a rulemaking proposed on safe harbors for employers who were using the program. Can you tell me what the status is of that rulemaking?

MS. BARNES: I don't have that information. I'm not able to answer that at this time.

MR. BEALES: Okay. Thanks.

MR. CRAMER: I would like you to know, though, that safe harbor is given to any employer in the State of Arizona when he uses E-Verify. Under new Arizona law, safe harbor is given. If E-Verify is used, we obviously don't have the same process as the federal government, but in Arizona if you use E-Verify and show it to the enforcement individuals, there's safe harbor.

MR. BEALES: That was my understanding of the federal program, too, is it's a safe harbor if you use it. But if you get the tentative non-match, there was a rulemaking that was a set of obligations that an employer would have to take in order to take advantage of that safe harbor.

And if the employer didn't qualify for that safe harbor for pursuing the non-matches, then they would potentially be subject to enforcement action even though they participated in the program.

MR. CRAMER: Well, you are right. But in some of the enforcement action that you mentioned earlier -- I know this from talking to the ICE people involved -- that when individuals who are arrested who had passed through the E-Verification system, yet the operation was raided, when it came to those individuals who had beat the system with their own documents and had nothing to do with the company, then there was safe harbor.

They were not -- those individuals were not considered in the fining process. However, what ICE usually goes after is when there is complicity on the part of the employers in creating the documents to get through the system, where they have a good employee, okay. That's when ICE does not give safe harbor, when they have a wiretap and they find out that there's complicity on the part of the employer.

MR. BEALES: Jim Harper.

MR. HARPER: I think my question is a follow up to Caprio's, and it's addressed to you, Ms. Barnes. Anyone can answer, of course. Things won't always go just exactly as they are supposed to so let me pose a hypothetical about this nonconfirmation process and learn some more about it.

A tentative nonconfirmation comes to someone, comes to the HR, comes to a busy HR office late in the day. The person prints it out and leaves it on the printer. Someone else prints something else out and picks it up to carry it to their office. In the morning, the person who had received the tentative nonconfirmation just doesn't remember that it came in so the employer never contacts the new hire and the new hire starts work.

And two weeks later a final nonconfirmation comes through, and they are supposed to be let go, but both the citizen employee and the employer want the work relationship to continue. What happens next?

MS. BARNES: What would probably happen is that we would get a phone call from the employer, if it's valid in your scenario that the employer has just forgotten or got lost in the process or a call from the employee. And what we've done in those cases is that we would then go back into the system just to find out -- you know, to work with that employer or work with that employee to resolve the case

MR. HARPER: So is there a process for opening a final nonconfirmation.

MS. BARNES: There is a process that's being developed now. It would be sort of a reconsideration process to allow for issues like that, yes.

MR. BEALES: You could also just start over, couldn't you, hire them again?

MR. HARPER: I would imagine the system would pick up and say this employer is defrauding us by running the same employee through again. I assume that would be –

MS. BARNES: That would require a termination of the employer -- I mean employee, I'm sorry.

MR. CRAMER: Take a look at the attestations on the I-9. I think that might answer your question.

MR. HARPER: My question about?

MR. CRAMER: About the employer just rehiring the person over and over again. The attestation says that knowingly -- that you've looked at the documents and the documents appear to be correct and that you are not knowingly doing anything that's illegal.

MR. HARPER: But as a systematic matter, E-Verify would then cause the employer trouble. Much later you might be able to address the form I-9, but if an employer were to repeatedly submit the same employee, I suspect the system would say there's something going on here.

MR. BEALES: Sure. But I guess the way I was understanding your hypothetical is that somehow after this final nonconfirmation comes in, there is a problem that can be fixed as opposed to this is going to be an ineligible employee. And once you fix the problem, presumably you could start over.

MR. HARPER: I suppose so.

MR. BEALES: And you are not violating of the attestations on the I-9.

MR. HARPER: From what I understand of the program, though, is when a final nonconfirmation come through, the employer is supposed to terminate the employee.

So then to terminate and rehire -- I just assume because of the way you've launched the use of the system, it's suspicious for the system, and so then you are talking about a harassive issue. When a poorly-organized HR department does this enough times, they look like they are breaking the law or they are just stupid.

MR. CANTOR: I would like to add one comment on what you were just talking about, Jim, and that's just in the context of day-to-day, certainly in Social Security, and I assume to a certain degree in CIS as well, that a day in the life involves phone calls and contacts from hundreds, if not thousands of -- whether they are individuals or employers trying to resolve issues about either -- I'm sure in the CIS world it's employment status, and at SSA it's a problem with name, SSN, date of birth combinations to get these things squared away so in both agencies, certainly Social Security fends inquiries in multiple situations for -- I certainly speak on behalf of Social Security.

I can say if a person comes into a Social Security office, comes to talk to a field office employee, has the evidence on hand, we'll update the record regardless of why they are asking. That is a policy. We do have that procedure. And they have been on the books and codified for many years.

So those types of procedures are day-to-day operations for a lot of us that. You know, facts change. You need to update your current records all the time but I think, you know, that specific issue I would have to defer to Sonja, but the general problem is that most of us work with people every day, whether it's in this context or out of this context to help update their records and create that.

MR. BEALES: Joanne McNabb.

MS. MCNABB: I have a couple of questions for Sonja Barnes. When DHS is doing the check in the verification process, what databases are you checking against, just to determine legal presence or are you checking against terrorist watch lists or –

MS. BARNES: There are a number of the DHS databases that are used. We have the Central Index System. We have our naturalization systems that are used. Databases that are used for non-immigrants, that has non-immigrant information. There's -- I don't have the complete list, but there are quite a few databases that are queried. Watch lists, no, are not one of those databases.

MS. MCNABB: And I have a couple questions about Social Security. And my office, in the California office, we hear pretty often from people who have learned one way or the other that their Social Security number is being used by somebody else to work.

And currently it is, generally, almost impossible to get that straightened out, either by contacting SSA, by contacting the employer of the other person or anyplace else. Do you -- do you have currently any systems in place that are monitoring earnings reports to flag this person's working in California and Texas at the same time or something where it's not in the D.C. area, for example.

MR. CANTOR: Well, I mean, for example, our Inspector General regularly, I think at least annually, sometimes more often than that does look at our records and does talk to the agency and conducts internal reviews with us. JEO has also done that, and in many of those cases talks about California and Texas we will find an independent contractor during the course of one year doing work in two states, even though they could be very far apart.

As a general matter, you know, we do monitor our records for irregularities and look into them. One of the difficult things we find in some of our reviews as an agency is the reasons for suspense records. And I talked about them a little bit in my initial thing, and they could happen for so many reasons.

Those flip-flop numbers can cause suspense; name errors. There are just literally hundreds of reasons, including fraud or someone else using someone else's number to obtain legal work. One of the benefits of verification is right now not every employer is required. Right now, for example, Social Security has multiple verification programs available for employers to help them get ready to do a wage report. All of those are optional.

Wage reporting itself is not optional because that's part of the tax filing system so we get all of those, but those verification programs which we do to assist us and to assist them is much easier for communication back and forth. All of those are still voluntary programs, as is E-Verify right now.

MS. MCNABB: You mentioned something about SSA verifying with state vital records offices. Does that something you routinely do to verify birth dates or –

MR. CANTOR: What happens is if somebody comes to us -- and remember I was talking about somebody who -- a vanity date of birth. They came to us and sort of said they were born much later than they actually were. And that would impact, of course, for us when you file for retirement. We will, then, actually go back and, to the extent possible under state law -- and that does vary with states, work with the state's vital records office to get a certified copy of a birth certificate.

MS. MCNABB: That's only when an individual has come to you.

MR. CANTOR: Right. Well, because, in some cases, we need the individual to go get it. And in some cases, depending on the state's open records law, we can contact the state office directly. It just depends. 50 different states, 50 different sets of rules.

Some states are much more -- have much more privacy around those offices. But either way we need the individual to get that report for us because that's the only record that we can update the date of birth with.

MS. MCNABB: And you can tell -- somebody in the field office looks at the paper documents and says that looks like a good one to me.

MR. CANTOR: It has to be certified.

MS. MCNABB: Might it not be fraudulent.

MR. CANTOR: It could be.

MS. MCNABB: Because it seems like it's an electronic system built on a bunch of paper documents that may or may not be good.

MR. CANTOR: Again, we do the best we can to work with the records that are available, what the state documents -- unfortunately, the birth certificates -- and remember some of the people at Social Security work with varying age and go back much further.

MS. MCNABB: On their birth certificates?

MR. CANTOR: Right. Their birth certificate is a very old document so a certified copy might actually come now from a microfilm printout. So it is very difficult. So we do the best we can. So one of the things we try to do is when we see one, if there are any questions, we try to contact that registrant's office and work with them to the extent that they are allowed to work with us, if we have a document. So if it's from Arkansas and you are from California, that field office may try to contact that office, but Arkansas is a very restrictive law. They are not allowed to talk with you. There is a decision that has to be made there.

MS. MCNABB: And it's made by the person in the field office at the time following some guidelines?

MR. CANTOR: Yes. We had policies. Often, at that point in time, the manager is brought in as a consultation. We have regional privacy coordinators in each one of our ten regional offices, and that's state based. And then, of course those ten privacy coordinators are given special training by my office. We have monthly calls by conference with -- where we focus special training on policies around privacy, correction, amendments and things like that directly to them.

MS. MCNABB: Are those guidelines available?

MR. CANTOR: Yeah. They are publicly available on our website.

MS. MCNABB: Will you show me where to find them?

MR. CANTOR: Absolutely. How about we talk off line and I'll give you the link.

MS. MCNABB: So imagine somebody who has gotten this tentative nonconfirmation, whatever it was called, because there's a mismatch at Social Security.

So that person has to go into an office and take something. Are they told the mismatch is the date of birth is wrong or just told there's a mismatch?

MS. BARNES: Yes. The notice that's provided to the employee will indicate the nature of the discrepancy.

MS. MCNABB: And does it say go get a birth certificate if it was the date of birth that was wrong or they would go into the office and then they find out what they need.

MS. BARNES: Well, there is a 800 number provided to the employee should they have questions of Social Security to prepare for their visit.

MS. MCNABB: That would be a thing to do first, call and say what do I need to bring.

MS. BARNES: Yes.

MS. MCNABB: So if it's a name mismatch and I didn't just get married, you know, what would I be likely to bring? How would I -- what might that result from and how could I establish it?

MR. CANTOR: For example, one of the causes of name mismatches is nicknames. So a lot of times people –

MS. MCNABB: Jack and not John?

MR. CANTOR: Yeah, Jack and not John. Chip and not Christopher, things like that where there's enough of a difference so it's usually not -- it's usually where there's a significant spelling change as opposed to letters being changed around. So Dan as opposed to Daniel probably wouldn't, but Chip as opposed to James would.

MS. MCNABB: What if it's somebody else's name entirely because somebody else is using my social?

MR. CANTOR: That would trigger a mismatch.

MS. MCNABB: So what do I bring in to show that I'm innocent?

MR. CANTOR: You are the one who -- somebody is using Joanne McNabb.

MS. MCNABB: I say that's really my social.

MR. CANTOR: You would bring in your Social Security card, other documents that are attached to you because that way we can associate -- we look at passports, driver license, other identity documents that -- you know, we look at all of those to figure out that you are you, but plus we would have your information.

MS. MCNABB: You are going to be busy at your field offices.

MR. CANTOR: Right. We are busy already.

MS. MCNABB: Step up. I'll be sending you customers.

MR. BEALES: Can I jump in for just a second here? I'm concerned with how this fits with the lack of employer verification because -- are you telling the employer to relay to the employee here is where this record does not match? This sounds like a system custom made for fishing.

MS. BARNES: The information that is provided to the employee and the employer, of course, has -- is seeing the same document. It does indicate and it's in very general terms, the reason for the mismatch. A copy of it is in the slides.

MR. PURCELL: How do you communicate with the employee? What methodology do you use? The employee doesn't have access to the E-Verify. They have no log on. Right?

MS. BARNES: Right.

MR. PURCELL: So how do you -- and the I-9 form captures postal or street address. Is that the way you communicate is by sending a letter?

MS. BARNES: No. This is all done between the employer and the employees.

MR. PURCELL: So it's the employer.

MS. BARNES: The employer sits with the employee. And this is -- the whole scenario takes place. The employer would sit with the employee, say, hey, you know, we have received a TNC. E-Verify had -- the response was a tentative nonconfirmation. What do we contest or not contest?

This is a manual process, which means the employer would print the notice. And the notice can be printed in either Spanish or English at this time, and go through the letter with -- the system-generated letter with the employee, give them the opportunity to decide whether or not they choose to contest or not contest. And if the employee decides that they want to contest, then another system-generated letter is provided to the employee.

MR. PURCELL: And that is good in a perfect world, but if the employer is not verified, then your scenario falls apart because the employer is receiving information from you when there may not be an employee. They may not be an employer.

They may be an organized ring that uses your system in order to fish for information and get back verification that says, oh, yeah, that Social Security number is just fine. Great. Now I've stolen a Social Security number and you've told me it's good to go. I don't even have to suffer the slings and arrows of getting it rejected.

You guys will tell me that. You'll verify that for me. Or to use name conventions or, I mean, it just sounds like there are -- and I think this is the point we want to make here. There are ways that because the EIN is not collected or a Social Security Number isn't verified from the employer that you are opening up a gap that allows people with malicious intent to come right in and use your system in order to aid their actions. That's a concern.

MS. BARNES: Understood.

MR. CRAMER: Can I make one comment about that very quickly? I'm a user of E-Verify. I'm a designated agent, which means that I can represent employers and do E-Verification for employers. That is a weakness.

However, when you do the MOU, and you sign up for the system, you tell the U.S. Government, as you do with a lot of things, that under criminal penalty you will not misuse the system. So I mean there's a lot of things you do out there that you swear you are going to do, but -- and you tell the government that, and that's the basis behind this thing. But I suppose anybody could try to verify the information and do it using E-Verify.

MR. PURCELL: And hope not to get caught.

MR. BEALES: Thank you.

MR. FRANCOIS: I had two questions about the E-Verify system and they are not related, I don't think. First is, had there been any consideration or discussions about working with the IRS to allow for some sort of method to query an EIN, whether it's valid or not so they are at least -- you know, an employer presents an EIN to you in the process of verifying a Social Security number of a new hire and/or a potential new hire.

And then you take that EIN and at least query against the -- what the IRS has and the information that you get back is, essentially, yes, this is a valid tax-paying employer? Was there any sort of discussion -- maybe will there be any sort of discussion in light of this conversation about something of that nature?

MS. BARNES: I hope I haven't misrepresented things. We are -- we recognize or know that this is an issue, that this is a gap that's apparent in the process, and that there's a need for more robust monitoring to ensure that the employees -- excuse me, the employers who are utilizing the system are utilizing -- are valid and should be using the E-Verify system.

So I just want to say that, that although I cannot sit here now and say to you, yes, this is the process by which we're going through to verify that the status of the employers who sign up and EIN numbers, this is a priority for us at this time.

MR. FRANCOIS: And the second question I wanted to ask you was mostly a clarification for myself. I noticed in a response to a question you had said that, while if an employee gets a temporary nonconfirmation back, then he is expected -- he or she is expected to continue with whatever training the employee is scheduled to do.

And my question is where does that obligation arise out of? Why can't an employer who is looking to replace someone or employ someone very quickly, if they get a temporary nonconfirmation that looks like it might be more complicated and take a little longer to resolve -- what is the obligation that I, as an employer, have to keep this person employed or hire this employee?

MS. BARNES: That's what the -- first of all, the employer has agreed to that in the Memorandum of understanding.

MR. FRANCOIS: Okay.

MR. BEALES: Last question.

MR. CANTOR: I just actually have one quick comment. It came from the front end authentication discussion. I would just like to point out that Social Security has, within the confines of the law, encouraged, as the process has moved from what was a voluntary participatory pilot in a few states to being a voluntary national program to beef up the -- we've been working with DHS, as best as we are able to do so.

This is one of the gaps that we identified early on from our perspective that needed to be -- I would just like to add that our participation in this is not a voluntary program. Social Security's participation is mandatory so as DHS evolves the system, we have to go along with it. So we've made comments similar to some of what you've made.

MR. BEALES: All right. Last question, John Sabo.

MR. SABO: Really quick question. Mr. Cramer triggered this. If you were a registered user of E-Verify as an agent for employers, presumably that's authorized under the federal law; is that correct, or is that under the Arizona law.

MR. CRAMER: That's part of the E-Verification system of DHS. You can be a designated agent, which means you do verification for other employers.

MR. SABO: So it's a whole other category in terms of identity and authentication?

MS. BARNES: Right. There are three access methods in the E-Verify system. One is that of an employer. The other is that of a designated agent, and third would be a corporate administrator that is a person who is not actually performing verification queries; however, they may be in the parent company or in the corporate office, and they simply want to ensure that their divisions are utilizing E-Verify.

MR. SABO: So the second quick question is are individuals -- individual household employers employing domestic workers, et cetera -- are they required or are they eligible to use E-Verify -- required and/or eligible to use it as household employers of domestic services.

MR. CRAMER: In the State of Arizona, under 2779, if they are going to file, what is it, a 1099 where you employ someone and you file a 1099, yes, you would be required to do an I-9.

MR. SABO: In some cases, an EIN is an SSN.

MR. CRAMER: I'm sorry, what.

MR. SABO: In some cases an EIN is an SSN because it's a person like me who may employ domestic services, and many small businesses. So from a federal perspective, are those people required to use E-Verify.

MR. CRAMER: Well, you are an employer, correct?

MR. SABO: Yeah.

MR. CRAMER: You've got this individual in your employ that used a Social Security number. You are filing FICA taxes for them.

MR. SABO: Yeah.

MR. CRAMER: Then whether you are a small business or a household owner or whatever, if you are going through that process, you are required, yes.

MR. BEALES: So all that employer verification amounts to is verifying that I really am a person.

MR. CRAMER: No, verifying that you have the right to work in the United States.

MR. BEALES: No, no, verifying the employer on the front end, not the employee because under the Arizona system anybody who is an individual may hire a person in their household who may not currently hire somebody has to be eligible to participate in the system because otherwise they can't use E-Verify.

That means anybody can sign up. There isn't a front end verification that will screen those people out because I am a person. I don't have to be employing anybody.

MR. CRAMER: Well, if you are an employer -- all that I'm saying is if you are an employer, you are going to be required to use the system. And as far as an employer is concerned in getting E-Verified, I believe they can, yes.

MR. BEALES: Okay.

MR. PURCELL: You are going to need a big help desk.

MR. CRAMER: No. Actually I would like to make one final comment, again, from a street level point of view. Most, if not most, all the people that we have encountered that have had a problem with either their Social Security number or their immigration status knew before they ever walked in the door they had the problem.

So the idea that you are going to have tens of thousands of people going to Social Security or to immigration to get their status straightened out or -- is not a fact. Most people know when they have a problem with their data that it's there. Now, that's something that we've come across on a consistent basis so the fear that we're going to have these hordes of people going to get their records fixed is not right.

MR. PURCELL: I get that. I take your point. I think that over time with -- how many businesses in the United States, 55 million businesses and the potential for 100 million private employers that the shift, the thinking may have to shift from support of the employee to support of the employer using this system, verification of their identity, the use of their system, access to it.

I cannot imagine the Hmong family in the local grocery store trying to figure out how to use E-Verify if they are required to; language barriers, access through computers that they don't have and have to use in some other facility. I can just see all kinds of help desk kinds of challenges arising.

MS. BARNES: Absolutely. Education is going to be key to ensure that employers know what their responsibilities are and, as well, employees are aware of what their rights are associated with the usage of the system. And so, yes, there's quite a bit of emphasis placed on educating employers, making information accessible to employers.

And, also, we are instituting an outbound call services so that new employees who -- excuse me, employers who sign up for the system -- that we do a little more hand holding and actually reach out that to them, those employers. And to -- in order to educate them to the point where they are more knowledgeable and we have more reliability in their usage of the E-Verify system.

MR. CRAMER: Pending legislation has a five year implementation period, whether it passes or not, but I just thought you would like to know that.

MR. BEALES: Well, I want to thank all three of us. It's been a most interesting if somewhat frightening panel, and I want to thank you for taking the time to meet with us today.

MR. CRAMER: Thank you for the invitation.

MR. CANTOR: Thank you.

MS. BARNES: Thank you.

MR. BEALES: Our next panel will address the E-Verify issues from a public perspective the program note says. And our first speaker will be Tim Sparapani who is the senior legislative counsel for the American Civil Liberties Union. Prior to joining the ACLU he was an associate of the law firm of Dickstein, Shapiro, Moore and Oshinsky.

He served as a legal intern for the Senate Judiciary Constitution Subcommittee, where he assisted Senator Russ Feingold. Before attending law school he was a legislative assistant at American International Group. He is a graduate of the University of Michigan Law School and Georgetown University.

Tim, welcome, and we look forward to hearing from you.

MR. SPARAPANI: It seems as if a number of people had to step out. Would you like me to wait or should we go ahead and just get started.

MR. BEALES: Yeah. Let's wait five minutes. (A recess was taken.)

MR. BEALES: We're only missing one. Tom is in the back of the room. So let's just go ahead and start. I don't want people to miss you, and I don't want to cut you guys short.

MR. SPARAPANI: Thank you. First of all, my name is Tim Sparapani, and I want to thank you the DPIAC for the invitation to come and speak. It's an issue I care about a great deal and I'll explain that a little bit in a minute.

A briefly introduction about the ACLU for those of you who don't know who we are. We are America's oldest and largest civil liberties organization. We count over 600,000 active members. We have a affiliates -- 54 affiliates in various jurisdictions around the county. We think we represent views of about 25 million Americans right now, and that's a conservative estimate from a liberal organization, but thank you again for the invitation.

I speak here in my private capacity, although I do represent the ACLU. This is an issue that's greatly concerned me for a number of years, and I've been actively involved in helping Senate and House staff try to create the ideal employment verification system in legislative language, in part to fend off what I see coming, which is the slow, mandated growth of the current system, which I think is fraught with enormous problems, and problems which the DPIAC probably is uniquely situated to speak upon.

So in the beginning let me preface my charge to you at the end, which is that you should get involved. You should write about this and you should sound the alarm over some issues that haven't been addressed.

One of the gentlemen on the previous panel mentioned there's a long history with this program. And that's an understatement. And that their program has enormous -- statements back in 1984, '86 -- actually we have 1978 where people were talking about how this program had enormous potential to resolve illegal immigration questions.

And the word potential is an interesting one because here we are some 30 years after the first statements that I can find back in 1978 where we -- it really is still about potential, and there are still problems that have not been ironed out. And it is the reason this remains a potential solution instead of a solution because some of the endemic problems have never been resolved, and I'm not quite sure we'll ever be able to resolve them.

Let me say again when working with Senate and House staff I was not endorsing this concept. In fact, I'm quite opposed to this idea because of the collateral damage we'll likely see from implementation of a nationwide mandated employment verification system. Philosophically it cuts against most of our American capitalistic society to imagine a system, which I believe will wrongly deny work eligible people the right to work in this country.

You go back to Jean-Jacques Rousseau, the beginning of enlightenment central to our philosophy that people should have the right to work and the right to make -- take from the common wheel and add to their own growth, and yet we were about to institute a program, if this is mandated nationwide, which I believe would prevent people from working in this country because of the intractable data problems I'll speak about in a minute.

And why do I say that? I say that because I have had close negotiations with the Department of Homeland Security about the legislation over the last several years. And DHS in its current incarnation has taken, to me, what is the absolutely untenable position that they are allowed to deny people the right to work who are work eligible, people who are born in this country, who are naturalized citizens, visa holders, et cetera, without giving actual redress to people who are wrongly denied the right to work. Yes. You heard me correctly. DHS takes the position that there should be no form of redress for people who are wrongly denied work through the application of E-Verify, no administrative process, no judicial process, no accountability on behalf of the government for making whole the individual who has lost wages, and that's a really serious problem.

I'll talk about it again a little bit later. I imagine what we are headed towards is the creation of what I deem a no-work list, which is far more damaging than the no-fly list, which you are all deeply familiar with. So, again, let me talk about the DPIAC and what your role is.

Let's talk about your name. You have the Data Privacy and Integrity Advisory Commission. Let me talk to you about data integrity because I think that's where the problem really lies with this system. It's less of a privacy problem, although they are important questions, but it's really about integrity.

You are all, I know, familiar with the Fair Information Practices, and the incarnation of E-Verify, as it currently stands, I think, violates the four key Fair Information principles. One, there is no true right of review for an employee or would-be employee to find the information and collect it about them and review it in the government's hands.

Two, there is no true right to challenge the accuracy of that information. I can't simply -- if I am a wronged employee, I can't simply insist that you give me accurate information or that you correct the information. Three, again, there's no right to correct the information. I can't force you, as an individual, you being SSA, you being DHS, to change the data that you have about me, even when it's absolutely wrong.

And four, as I mentioned before, there's no right of redress. You can't go through an administrative process. You can't go through a judicial process. After the tentative nonconfirmation process has been undertaken, after information has been submitted through secondary verification.

What DHS has instead insisted is that you sue under what is known as the Federal Tort Claims Act. Now, why won't this work? That's usually the method that individuals take when they have to sue the federal government for tortuous injuries.

The Federal Tort Claims Act requires a six month waiting period. You have to file a claim. You have to exhaust whatever administrative process there is. You have to have six months of time go by. You have to wait for the agency to respond, and only then, when that process breaks down, are you allowed to sue the federal government.

You have to sue in a specialized court in Washington. There is already a 30,000 case backlog for other types of suits against the government that have been deemed meritorious and so they are going forward.

The typical Federal Tort Claims Act suit takes two and a half years from its inception to its end to be completed. So we are hearing from the Department of Homeland Security that where there are individuals who are actually eligible to work that the government expects that individual, even if they are making, say, minimum wage, to retain an attorney for upwards of three years of time, to sue the government, to successfully sue, and only then would there be some potential redress.

That is the idea that DHS has put forward to resolve what we all know is coming, which is the intractable data questions where DHS or SSA has got wrong information about you or your friends or where they merged two files or there's been multiple people working under your name and your numbers.

So let's talk a little bit more. What do we mean when we say that there is no right to redress? I think what we are talking about is that we are going to again be creating a class of people in this country who will go through a series of tentative nonconfirmation submissions of information, who will then be presumptively unemployable in the United States. It's a totally new concept in our body politic.

We talked about Jean-Jacques Rousseau. We are talking about the government saying that people cannot earn a living if we mandate this. I don't think that's any kind of reach to say that because the only option that a person would have when this nightmare scenario unfolds, and unfold it will, is to work illegally, to earn cash wages, to not pay taxes on those wages, and then to literally be a scofflaw.

So my first request to all of you is to insist that as the department goes forward with trying to make E-Verify a nationwide mandatory program, that we try to avoid this. I really think this is an essential part of your mission.

We talked about -- I just talked about problems with the integrity. Now, why do we have a data integrity problem? It's really because we're still dealing with lots of inaccurate data, and you've heard some of the information from the prior panel.

And because we've had a 30-year history of this program, I think we can speak frankly that the data inaccuracies continue to exist. And they are actually, I think in some ways, getting worse, despite the good work of the Department of Homeland Security Act, because they are seriously addressing the inaccuracy problem.

But I think when we talk about taking a program, which has had only a few thousand employers, until the last year, and now it's about 50,000, and we talk about magnifying it so that all the nations 5.4 or 7.2 million -- depending how you count -- employers would have to participate, we're talking about an enormous problem.

So even if DHS is working diligently right now to resolve data inaccuracy, when you make a program nationwide, when you involve the nation's 160 million person workforce, and when you involve the current 55 million people per year -- I'm sorry, the current number of about 55 million checks per year, which the system would have to undertake, you are talking about problems where even if they are small data inaccuracies by percentage, magnified to the entire population of employers and employees, we are talking about really enormous problems.

The Gold Standards Report, which has not been mentioned this morning, was by Westat or Temple University. This was a report that was commissioned by the Department of Homeland Security. There's actually going to be a second report now, finalized in the fall.

That report said that studying the last three years of the E-Verify system that there were approximately only one/tenth of one percent of all the checks, which were inaccurate. These are erroneous tentative nonconfirmations.

We're talking about people who are actually eligible to work who the system -- all the verifications, reverifications, the manual verifications, still ended up showing that they were wrong -- that they weren't eligible to work when, in fact, they were eligible to work. We should celebrate that. It's only one/tenth of one percent.

It seems like a very tiny number. If you look at the study itself and you get deeper into it, it extrapolates. You can actually look at the numbers, and say if you were to expand it nationwide and mandate it, the number is more like .81 percent or closer to one percent.

Let's use one percent just as an example. If we are talking about mandating EEVS nationwide, and for the 160 million people in the workforce, and we only have that .81 percent erroneous nonconfirmation rate, we are talking about putting 1.34 million people into some sort of jeopardy.

Now, you know the no fly list is big. Imagine having 1.34 million people who might not be able to work who would either be delayed or denied the right to work.

Similarly, if we're talking about only checking new hires for a year or the number of times that a person in America seeks a new job, which is about 55 million times, we are only talking about -- and only talking about here 494,000 times per year will this problem arise.

Either way we are talking about an enormous change in the relationship between the government and the individuals and their right to work and we're talking about a small percentage of data inaccuracy causing truly enormous headaches.

Now, where do some of the data inaccuracies come from? I won't go into all the details because I know Sonja Barnes mentioned some of the problems, but one of the major problems is bad legacy data. By that I mean we are talking about problems arising from the keeping of files, primarily by aliens, in paper form until 1996.

It was the case that the then INS believed it did not have the legal authority to keep electronic records about people who became lawfully present in the United States who were aliens.

So we're talking about paper forms, lots of them with many errors, many of them which are outdated, many of them have not yet been scanned or updated, even though DHS, I understand, is undertaking an attempt to scan a lot of those pieces of paper.

And so I think we're going to see, as this Westat report tells us, some problems for some specific types of individuals which will be different than the broad class of citizens.

One, we're going to see problems that are especially bad for non-citizen visa holders. These are, again, non-citizens who are eligible to work. They received a visa. Given the current system that's in place, E-Verify is erroneously, tentatively nonconfirming three percent of non-citizen visa holders.

Now, when we talk about foreign born but naturalized citizens, these are people who are citizens. They are just born abroad. They became naturalized. They are now citizens. E-Verify was returning a 9.8 percent error rate. That's a really substantial percentage. Almost ten percent of foreign born naturalized citizens are likely to find themselves having difficulty being quickly prescreened whenever they want to start a job.

I think we're going to end up with a likely discriminatory impact on certain minority classes in this country. I won't go into it now because I think its outside of the purview of this committee. I'll be happy to talk about it in the question and answer period.

The Westat report is pretty clear. We're going to see some trend lines that will suggest a discriminatory impact on certain classes of individuals. I want to respond real briefly to this question about numbers showing up multiple times per year. And by that I mean the Westat report looked specifically at those situations where a Social Security number was used six or more times in a single given year and put through the E-Verify system.

It also looked at the same question about whether an A file number, which is an alien registration number, their first document when they start down the path toward citizenship; when that A number was used six or more times per year.

The assumption in Washington amongst DHS folks, I think, and some Republicans on the Hill is those people -- everybody who is in that category -- all but one of those people with each A number with each Social Security number, is likely to be an illegal immigrant, and that's just is not borne out by the data.

In fact, when Westat looked at this report, when they did this data analysis and they found that only, in fact, six percent of the times that a Social Security number was used six or more times. So six percent of the times that a Social Security number was used six or more times in a year was there actually a case where there's a final nonconfirmation.

So we can assume that the other 94 percent of the time the Social Security number was used six or more times in a year -- we're talking about people who were getting multiple jobs in the same year, not illegal immigration; actually legally immigration with people getting multiple times of employment throughout the year.

Similarly, when we talk about A numbers being used six or more times in a year, only 3.3 percent of the times were there final nonconfirmations. So the other almost 97 percent of the time we're talking about people who are, again, lawfully eligible to work in the United States.

I think those are sort of the data integrity problems based on inaccuracy, and I think they are intractable. They have not been resolved. There has been no systematic review of the data.

I want to speak very briefly about privacy problems. We can talk more about it on the question and answer period, but I want to let my colleagues speak and I don't want to filibuster here.

Here is my supposition to you all that there are enormous privacy problems. We have somewhere between 12 and 20 million undocumented immigrants in the United States right now by the best estimates. Again, by the best estimates, we are likely to have seven million or more people who are undocumented who are part of the current workforce.

This is both, I think, black-market and legitimate employment. And my supposition is that even a mandated system is not going to cause seven million workers to get up and leave their jobs nor frankly would we want that from an economic perspective. The amount of damage done in the economy would be quite significant.

I believe that if mandated nationwide E-Verify will cause the seven million or more workers and other undocumented individuals who want to work who enter the country after them will -- this will drive a market in data -- data theft that we have never seen before.

And this is where the committee really has to play an important role. If we think our identity theft is bad now, imagine the situation when seven million people who are already working are desperately seeking to stay in the jobs they have got.

They will go out and they will buy information. They will buy documents so that they can continue to work in the United States, even illegally, but under assumed names under other people's information, under forged documents.

And this problem has not really seriously been addressed, so beware the consequences of mandating E-Verify nationwide. We are talking about an explosion in identity theft. We are talking about an explosion in counterfeit document production.

And I think, frankly, eventually we will see some insider fraud. Just as we have seen that DMVs around the country are one of the primary sources of fake driver's licenses, I think when we have seven million people or more who want to continue to work lawfully in this country, at least under the presumption of law or legality, we will see individuals at the Social Security Administration, at the Homeland Security Department, other individuals who have access to these systems selling individuals' information who are work authorized to people who are not work authorized.

So we will see insider fraud. And I don't see anything yet in the system, as designed, that will take care of this insider fraud problem. I think it's very likely to occur. I know I've spoken for a while here. Let me ask for some action from the DPIAC because I think you really do have a unique and important role to play.

I would really like to see you issue one of your very helpful reports disfavoring a mandated E-Verify System, until and unless these data integrity and privacy problems can be resolved. I would like to see DPIAC recommend to policymakers in Washington that they undertake a systematic review of current files to rule out data inaccuracy.

I really mean going through file by file through people's Social Security records, through the various immigration records. It's going to be expensive. It's going to be time-consuming, but if you really want to do E-Verify, if you really think that this is the solution to illegal immigration, I think it's the only way you can eventually resolve the problem.

Again, the gentleman talked about the potential of this proposal as a means of solving illegal immigration. I think the only way it even has a chance of curtailing illegal immigration is if we do that systematic review.

And then, finally, I really think this body should, in a report, demand that the Fair Information Practices be made part and parcel of any E-Verify System.

And by that I mean a true right to review government data for employees who are put through the system, a true right to challenge bad data held about them, the true right to correct that bad data, and finally a true right of redress, including a right to an administrative process and a judicial process, both of which are expedited and where the government is the guarantor of erroneous decisions, and by that I mean paying financial compensation for lost wages to individuals.

Without that we are talking about foisting off on individuals who are going to be misfortunate individuals who will be subjected to bad data and bad systems and bureaucracy, the idea that this system can resolve our immigration problems. Again, if the government wants it, I think the government has to pay for it. And I'll stop there.

Thank you.

MR. BEALES: Our next speaker is Dr. Eugene Spafford who is the Chair of the U.S. Public Policy Committee, the Association for Computing Machinery, and Professor of Computer Sciences at Purdue University. He's been on Purdue's faculty since 1987.

He is also a professor of philosophy, of communication, of electrical and computer engineering. He is the Executive Director of the Purdue University Center for Education and Research and Information.

He has an ongoing record of accomplishments as a senior advisor and consultant on issues of security, education, cyber crime and computing policy for a number of major companies, law enforcement organizations, academics, government agencies, with nearly three decades of experience as a researcher and an instructor.

Professor Spafford has worked in software engineering, reliable distributing and computing, host of network security, digital forensics, computing policy and computing curriculum design. He is responsible for a number of firsts in several of these areas, and welcome to your first and hopefully not last visit before our committee.

MR. SPAFFORD: Thank you. I'm very pleased to be here. I'm representing the U.S. Public Policy Committee of the ACM. And I realize some of you may not be familiar with the ACM. It is the first educational and scientific computing society. It was formed in 1947 by the inventors of the Maniac computer for purposes of international education and promotion of computing technology in the public interest.

We try to advance computing as both a science and a profession. We currently have 87,000 members worldwide. About two-thirds of those are in the United States. These include students, professionals, academic scientists, many people working in government. We publish 45 periodicals.

We have 35 special interest groups, over 450 checkers around the world, and it's primarily a volunteer driven organization. We're a non-profit, and our charter actually specifically prevents us from taking positions on legislation, for or against, because our position is really to look at the impact of the technology and some of the issues that are involved.

The basis for this invitation was that we have provided input several times on issues related to systems such as E-Verify. And one of our senior members, Dr. Peter Noyman provided testimony before a Congressional committee on June 7th of last summer.

And I'm going to go through and summarize some of the points of his testimony and there are other testimonies that we presented. Basically, to start off, as an organization we have no position on immigration at all. We're an international organization. We're looking at the technology.

Our expertise is in IT systems, databases, data integrity, privacy, those issues. We want to note that our experience has been that deploying technology as a means of solving a political problem almost never works, and that's what this is.

We have a political problem with concerns over immigration, border control, possibly some concern over certain minorities. I think it's interesting that, for instance, this meeting isn't being held in Bozeman, Montana near the Canadian border.

And as a result, we have this significant problem politically that is attempting to be solved with technology. We also want to point out that very often the people who evaluate this technology fail to present a truly accurate picture, and I think Tim gave some numbers there to help show that case.

First of all, when you evaluate a system you need to look at both false positive and false negative. That is not only those that are judged to be kicked out by the system incorrectly, but those that are accepted incorrectly by the system, and consider the cost benefit of both of those of costs.

It's also the case that if you listen to some of the things that have been said and previous witnesses said, for instance, that most all cases were handled within ten days. Well, I would push back on that and ask, well, how long is the longest case? What is the average length of time for those over ten days and what happens to those individuals?

The fact that any take longer than ten days is an indication of a problem. So in a general sense, those are the kinds of things that I want to raise. So let me raise some more specific concerns.

First of all, matching is not verification. The fact that you find somebody's Social Security number and name in the record does not indicate that the person presenting the credentials is associated with that Social Security number and name.

To support that you need to have something like REAL ID, which has its own set of problems. And so this is a lead-in to a national ID, and we are very concerned about that approach. As an organization, we've gone on record that no nation should have a nationally-mandated ID.

There have been historical problems with such things. Passports is a different issue, although -- and if you want, I can address that. I wasn't really prepared to go into that in depth here, but it's important that matching is not verification.

Second, Tim pointed out very well the data is dirty. It has been dirty as long as it's been in existence because of transcription errors, people's memory has problems. We have numbers that have been reused because some people didn't understand the necessity of getting separate numbers for members of the family and so on.

What happens when someone does get a denial? Well, the statement we heard is that the employers have to sign a Memorandum of Understanding that they won't terminate the employee's employment in that instance.

Well, if you've got an employer who happens to be a day laborer or farm worker or someone who is eligible to vote, may not be entirely literate, doesn't have resources and is fired, and the employer writes down it's because of poor performance, poor attitude, whatever else. How are they going to challenge that?

So people -- this is another issue of the kind of underclass that Tim was talking about, people being terminated by employers without adequate redress. That's a problem. Errors and failures in the systems -- what happens if there's some kind of computer outage for a length of time?

What kind of impact is that going to have if it comes up erroneously, if the software has flaws in it? So that the data that gets reported isn't actually the data that is in the system. Who is responsible? Because that's going to have to go out to all of these end employers nationwide.

What about widespread failure situations? When the next Katrina hits and we have tens of thousands of people who have gone elsewhere in the country, lost all of their personal documentation and seeking new employment so that they can sustain themselves?

How are we going to handle that with a 20-person help desk at IRS or DHS? Probably not. There are other issues involved there in such large scale problems. And there are others that we can certainly think of that follow along those lines having to do with, for instance, a Bay Area earthquake.

If that happens, we won't have the telecommunications and power necessary for most employers to even get access to the system. As Tim noted, wherever you tend to concentrate data it becomes a target. It becomes a target not only for faking ID information but for using it for other purposes.

And there are a whole list of those we could come up with. One in particular is fishing. When you have people in-house who have to use this system to verify household employees who are currently falling victim to scams purporting to be from their bank and Paypal and eBay, if they get something that looks like it's official from DHS saying you must fill out this form again or else you must be penalized by law, how many of them do you think are going to fill out that information?

That's a really significant concern. We have individuals who are criminal who are going to be seeking alternate identities. This is a good way to find starting information necessary for fake IDs, and those criminals can be any where from petty thieves, embezzlers, all the way up to agents of non-national organizations with more malicious intent.

We're concerned about Mission Creek. Whenever you have databases that are collected from different places, how long is it going to be before we start trying to find all deadbeat dads, taxpayers in arrears, people who are on the do-not-fly list and otherwise, by tracking the information that are in these lists.

There appears to be no legislative impediments. There is nothing in place that will keep that from happening. And dealing with erroneous data and with the problems of entering information in, we have a whole new series of problems that I'm sure you can begin to think about, but if you spend some time becomes a very large list.

We have a number of people who have false IDs. And I don't have enough information about how this is represented in the system, but these are legitimate false IDs.

These are people in the witness protection program. These are people that are working undercover with the DEA and other law enforcement agencies.

These are people that work for the intelligence agencies and working undercover. They have to be represented and be able to work. And they have to do so in a way that isn't going to arouse suspicion. You have a system like this that allows you to go in and verify and look up information and possibly trace to other databases.

It's going to become a target, not necessarily for identity theft, but for finding any kind of suspect identity. And it could very well result in deaths, particularly some of the organized narco groups. If they are even suspicious of someone as possibly having been compromised, they just kill them.

So imagine that one percent who come up wrong in the system who happen to run afoul. We're not talking just right to employment here. This could have deeper consequences.

Tim mentioned insider threat is huge. Insider threat not only from those who are menal who are seeking out information that they are going to sell, but individuals who may be malicious, who are looking up information on spouses who may be protected by court order, who may be looking up individuals to try to find out information on celebrities, maybe looking up information on others simply as a matter of curiosity or for people who they are stalking to go in, and if they are in a position of importance, change the information.

What better way to get even with someone than prevent them from being able to work and to continue to keep messing up their records. We have to worry about not only access to the live systems but backups, transmissions, copies.

Some of the incidents that occurred the last few years with the Veterans Administration, for example, and what we've seen in Great Britain were losses of CE copies of the database. So it's not simply a matter of on-line protection. We need to have an audit in place that is actually audited and enforced. And most federal agencies do a very poor job of this.

Following through on security, if you've been following any of the news about the federal initiatives, is because our systems have been penetrated multiple times by entities from foreign governments and criminals, and even our military agencies and DHS have been unable to keep them out.

DHS actually received a failing grade on the FISMA scores, I think, the last two years, and they are the ones that are going to be protecting this database.

We have to worry about the transmission of data as I mentioned, not simply the storage. We have to be concerned about the burden on end users. How are they going to access the system?

Are we going to require that every employer, including everybody in the home, have a reasonably high speed dial-up internet connection and a computer that is equipped with the latest security technology because otherwise they may cause some problems?

What kind of burden is that going to place on each of them? And they have to know how to use it. There's cost and security issues there. He pointed out the problem of multiple registrations, multiple venue jobs.

I know how that happens because I do consulting at various places, and I've had to go through the I-9 process multiple times for my government positions. So I would show up as one -- in some cases, of those multiple venue IDs. How are you going to actually deal with that?

If you identify that an ID is coming up multiple times, we are going to have some pushback to keep a record of where everybody has placed a request. We are going to know where everybody has filed a request for a job. We are going to have a database of all the places where people have applied or are employed.

That's Mission Creek. That's additional data that we have to worry about privacy issues and security issues. And again, once that data is kept, that's going to encourage our lawmakers and our rule makers to provide new uses for that data.

Scalability is an issue. It's talked about this pilot program has worked well and it only has a few percentage points of error. Now we're going to scale it up by a factor of perhaps 1,000 to a national state. Again, working in computing, all you have to do is look at the examples. Very few pilot programs have ever scaled up successfully and within budget.

You can look at the FBI case management system. Look at IRS or the Air Traffic Control Modernization Systems. One that was just recently reported in the paper was the Army Future Combat System. After an investment of $200 billion, the GAO has recommended that a plan B be developed because they simply can't make the computing work on the scale that the Army intended.

Now, the vendors will certainly tell you it can be done and for a price they will do it. But for those of us who work in the profession, we want to tell you caution. Look at past experience. That scalability is a problem.

And then, in closing, I would effectively tell you what Tim said about fair information practices. Our committee has developed an expanded set of these practices, and we can make them available. Actually two members of your committee are associated with the ACM, USACM and can make those available.

Generally, those are problems on minimization, collecting only the information for what's needed, store it only for as long as it's used, implement systematic mechanisms to evaluate repeatedly, on an ongoing basis, if we need to keep that information.

And consent, require individuals or allow individuals to be able to look at their information and correct it. Openness, be very clear about how the information is being used, have explicit privacy policies with contact information so that individuals know where to go.

They don't have to depend on the employer but they have other mechanisms. That's going to be very important because if a potential employer turns them down and chooses not to go through the explanatory process, in a language that they understand well, and that language could very well be English, but they may not have an education sufficient to understand the default letter or the information.

They need to have redress. They need to have mechanisms about how to go about fixing things. Accuracy, certainly I mentioned. Security is a problem. Security of all those end points, accountability for all the information used for every lookup should be audited.

And it should be a random sample that is checked to make sure that they are legitimate. We need to maintain providence. Where did the information come from? When did it get there and who authorized that it was in place so that we cut down on some of this inaccuracy that we are talking about.

And then, last of all, require that appropriate training and accountability be in place for those people who run the system. Too often we have these cases where systems are developed. There's a bureaucracy in place. It's expensive to put in the controls in the audit, and so those are sometimes done away with, but no one is held accountable.

There is no feedback into the process to make sure that individuals are personally liable for failing to follow through on the security and privacy of the data of our systems. And with that I'll conclude my comments.

I could go into depth on several of these things during the questions if you are interested. I thank you for inviting me today, and I certainly wish you well on this very complex area.

MR. BEALES: Thank you very much, Dr. Spafford.

Our final speaker on this panel will be John Garza who is the Manager of Workforce Services for the Arizona Public Service Company. Mr. Garza's responsible for the Corporate Human Resources and Shared Services Group where he is responsible for providing and ensuring compliance in the areas of Equal Employment Opportunity, affirmative action, I-9 Form and E-Verify programs.

As corporate administrator, he led and successfully implemented the E-Verify program throughout the Arizona Public Service and Pinnacle West Capital Corporation and its subsidiaries. He is president of the Affirmative Action Association and executive officer of the National Industry Liaison Group. He holds degrees in management.

Mr. Garza, we are pleased to have you with us today.

MR. GARZA: Thank you, Mr. Chairman, Members of the Committee. Good morning or good afternoon, whichever day it is here, since our time is different in Arizona. Greetings from Phoenix, Arizona where it's not yet 120, but it will be soon. And after hearing some of my colleagues here speak, maybe it will.

Again, my name is John Garza, and I'm the Work Services Manager for the company, and thank you for giving me an opportunity to speak to you about the implementation of the E-Verify program at our company.

We chose voluntarily to sign up and have implemented a program that has been very successful for us. So I speak only for Pinnacle West Capital Corporation. But before I move on to show you the example of how we got there, I would like to, if you would allow me, to talk a little bit about my company.

Pinnacle West Capital Corporation is really the parent company of Arizona Public Service or APS. For more than 120 years, Pinnacle West and their affiliates provided energy and energy-related products to people in businesses throughout Arizona. And Pinnacle West has consolidated assets of about $11 billion.

Our largest affiliate is APS or Arizona Public Service, and is the -- also the largest and longest-serving electric utility. It delivers electricity and energy-related products and services to more than one million customers in 11 of Arizona's 15 counties. APS is also the operator and co-owner of the Palo Verde Nuclear Generating Station, which is a primary source of electricity for the Southwest.

Now, let me walk you through at least our process that we used to volunteer for E-Verify, and hopefully generate some questions around how we got there. I provided to you a flow chart, and I also have it on the board back here, but very simply a lot has been covered today, and some of it may be duplicate, but I wanted to share with you how we got there.

Once we volunteered, we put together a process and went out and created an awareness to our individual users who were going to implement the program. Approximately, about 22 individuals were trained to do that. Myself, as the corporate administrator who has oversight for the program, and then we also have a program administrator who, in essence, is the individual who does continual training and trained the 22 plus users that we have.

The users are the ones who actually get to do all the work once a person gets hired so beginning with the general user or designee, they complete the I-9 Form within three working days. The general user then reviews the completed I-9, and keys noted documentation into the E-Verify.

Again, all done within three days. Is the employee confirmed and eligible to work? Yes. To your right there, if it's not end of process, we send the original completed I-9 Form to a gatekeeper who was an individual who has responsibility for reviewing that I-9 one more time to ensure that it is complete, that everything has been signed, that there are no blank spots on the I-9 Form, and then it gets scanned into one of our systems for storage.

If the general user -- if, in fact, the employee is not confirmed or is ineligible, then the general user, then, informs the employee of the nonconfirmation status and it goes to the left there. It's a no. Employee is terminated, and then it goes to the gatekeeper for processing.

If, in fact, the general user informs of nonconfirmation status, then the employee opts to contest, and the next process is that the general user gives the employee the tentative nonconfirmation letter, signed by either SSA or with DHS, and it's clarified within eight business days.

DHS is then notified and the employee signed a referral letter. SSA or DHS initiates the referral. We at no time let the individual general user have any dialogue or conversation with that individual to talk about why, other than they need to go to DHS or SSA to find out and to get it resolved.

The general user, then, provides original data to the employee and keeps a copy of the contest letter with the I-9 to follow up. The employee follows up within eight working days. The general user initiates the resubmittal. The form I-9 is confirmed. If it is not, the employee is terminated, and the case is resolved and closed. If it is, then it goes back to the end process where, again, we have the gatekeeper who then processes the I-9 document.

So far it's worked for us. I can only tell you that we've used it January and February. We've hired 35 new employees. We've not had any issues. That's not to say we won't have. All I'm telling you is within the last start time that we started, that's what we have. I don't have anything to present to you other than our process for initiating the program, implementing the program, and that's our end results. Thank you.

MR. BEALES: All right. Thank you very much for being with us today.

MR. GARZA: Thank you.

MR. BEALES: I think our first question is John Sabo, although you may have a leftover flag raised?

MR. SABO: No.

MR. BEALES: Okay. You have a question. Then you are our first question.

MR. SABO: I guess this is addressed to all of you. Initially, you know, you deal with an issue that's political and then you deal -- from that flows business decisions to a fixed political issue, and from that flows your process and technical implementation and all this stuff that goes with it.

With respect to this program, I guess I'm looking for -- and especially Dr. Spafford, a huge number of issues all of which are relevant, which would each probably take a whole set of hearings and discussions, but let met focus on one, and that's the data integrity issue.

Agencies like Social Security know that they have inaccurate data. And they actually have a lot of experience dealing with inaccurate data. They have studies. They actually use tolerances in their matching process.

When you do a match at these agencies, you don't do an exact match because they would have so many bad hits that it would basically make the program grind to a halt. So you have to have tolerances.

So my question is, on that particular issue of the inability of our systems that are being used for this process, all other issues aside, where we know we have bad data, and I'm talking about bad data at the agency level. I'm not talking about the input stuff. That's a whole other question.

What would your feelings be about a scoring system? In other words, instead of absolutes, you would get a conference report. Let's say that there's high or moderate or some scale of confidence that wouldn't necessarily -- that would allow an issue to be resolved, but actually it would not get in the business of putting workers or applicants for work into a bad list unless you have a really rigorous process to say these folks are not eligible to work and it's been established?

Is that methodology approach a viable one with respect to the E-Verify system?

MR. SPAFFORD: Those approaches have been used in several systems that I can think of and are helpful because they give you a prioritization of where to place resources to do follow-up investigation.

But what has to follow, then, is that you actually do have those resources and you do a lot of follow-up. I'm not sure if you had a scale of one to five what it would tell an employer, the difference between getting a two and a three?

You would have to build administrative controls around that to do the follow-up, but it might put you in a -- that's associated with the idea of data providence that I mentioned.

And what that might do is give you a situation where you can say that everybody that scores three and above is assumed to be okay until additional evidence shows up, and only in the cases of the score of the one, for instance, might we demand some immediate resolution. So that might help, but without a further study, I wouldn't be able to tell you.

MR. SPARAPANI: I'm actually sensitive to my colleague Mr. Garza and the employment community. I think if you are an employer you want to have an answer right away because you either want to be able to proceed with that individual, training them or you want to go to the next candidate and, you know, that's part of the -- the other question is that the employer, of course, wants a safe harbor. They want to show they have been in the compliance with the law, and they want to avoid any liability, which again I have sympathy for.

Where I think this breaks down is that I think that this whole approach is trying to do illegal immigration enforcement on the cheap, and I say that sort of tongue in cheek because as Mr. Spafford has suggested, we're talking about a multi-billion dollar solution at the bare minimum, probably tens of billions.

What I think DHS is not ready, willing and able to do is actually do follow up at that place of employment and actually verify with an individual, with the employer, whether the person who had that lower confidence level score, whether they are who they say they are and whether, in fact, they are eligible to work.

And I think that's an endemic problem that this won't resolve. It also leads me to another problem that I didn't address, and that's that there are all sorts of ways to game E-Verify.

If I'm an employer, I can either pay my entire workforce cash wages and not submit people through the system and hide much of the earnings potential. I can submit half of my workforce and not the other half, and I have high confidence that DHS is not ever really going to show up at my door and check.

So I think there are a lot of problems with an assessment based on the fact that there can't be, under the current vision that DHS has put forward of their enforcement regime, the likelihood that DHS is going to actually follow up.

MR. BEALES: Mr. Pattinson.

MR. PATTINSON: The first question is for Mr. Tim. The question is what are your recommendations about doing a full review of all the files in the Social Security system? It strikes me there is a great deal of those.

I'm not even sure how it will all go around doing a review of those files because you have to base them on something to compare them against. So I would have thought that the process that the E-Verify system is going along now.

It's just that it's really, in my view, the ownership is of the individual to prove that they are legitimately employable and that they are a citizen and so on, that that is the exception rather than the rule.

The rule for most people we're hearing about is they are going through just fine. So rather than going through the entire database reviewing everything, it would be more pragmatic to continue the way we are doing now, which is to flag the issue as it's occurring, and then have the individual himself, as we heard from various other testimony, that the individual is responsible for telling Social Security that they have been married and changed their citizenship status, and so it is in their interest to maintain how to do that.

So errors are going to be cleaned up piecemeal by piecemeal as people get flagged. And so I'm just uncertain how you would go around performing a complete file review of the database.

MR. SPARAPANI: I write on my recommendation because of that intransigence that I saw at the highest level of the Department of Homeland Security. And these questions were put to them. If the Department itself and Social Security, frankly, but mostly the Department of Homeland Security are not ready to guarantee the economic loss for those who are wrongly or erroneously tentatively nonconfirmed, then we have to find some other way of shifting the burden and shifting the time when the burden occurs.

My approach is that it would be advantageous to individuals, both from an employment standpoint and a retirement benefits standpoint, to go through this very expensive, very time-consuming process before there is an immediate economic need, which would occur at their time of employment when they are erroneously nonfirmed as ineligible to work.

I assume that most people showing up to start their first day of work have quit their previous job because that's how E-Verify is supposed to work. We're not talking about prescreening applicants.

We're talking about people who have actually been hired, who have probably quit their other job, are showing up on their first day of work and only then are they finding out there's a data error so there's a gap of employment, when they can work, between that day when they get that erroneous nonconfirmation, an average ten days, as Sonja Barnes has said, and for others, as Dr. Spafford suggested, a much longer period of time when they cannot earn any wages. Awful.

And so my approach -- and I recognize that it has enormous front end costs, is an attempt to, first of all, find a position for policymakers, two, get people to be serious about the problems of data inaccuracy and, three, to shift the moment when that individual employee burden occurs by trying to do a systematic review first.

MR. SPAFFORD: If I might -- and this is not a technology issue. This is just a personal observation from working in policy. As a country we don't generally believe that it's okay to punish some of the innocent because we're going to get all the guilty. And that's really underlying, I think, a number of our concerns here.

And that actually goes to many of the programs that DHS runs, that if there are errors in the data, the presumption is that that person is not eligible and in some way they are penalized. The penalty may be that it's going to force them to go through a lot of effort to clean up the records.

And they may not be individuals who have the resources, the literacy, the access to telephones or transportation and other kinds of things that are involved. And so I think that's really -- I think that's really where a lot of these comments come from is we know there are going to be errors, but the question is on whom does the burden and the penalty fall, if they are, in fact, citizens.

MR. PATTINSON: Interesting. So the follow-up question was to you, Dr. Spafford, about -- you made a comment in your introduction about the data is dirty in the Social Security database so it's a very generic comment.

I was wondering to what extent you felt it was dirty and how that could be stopped from becoming dirty, if that's the right expression? What are the processes needed to clean that up?

MR. SPAFFORD: Well, if you look at databases in general and all the various ways the data gets entered into those databases, and Social Security, yes, is one of the examples. Where do all the various applications for Social Security come in? How is that information verified?

You have people who may use initials on some forms that are filled out and never use them again. The names are different. I know that we have some of the data that's present having transposition of numbers.

There are numbers that were assigned under the old Federal Railway Retirement Act. I don't know how many of those are still active. Some numbers have been reused over time and how many of those are still active?

So those are what I meant by dirty. There's not a perfect match of name to number for every individual who is out there. And part of it is because some things haven't been reported. Part of it is because the data has been inaccurately transcribed, and part of it is on purpose. As I mentioned, federal witness protection is an example.

MR. BEALES: Do we know anything about the incidence of dirt?

MR. SPAFFORD: I don't have access to that data.

MR. SABO: I can tell you, having worked with them and watching how they monitor their programs, Social Security has a huge database, when you think about it. And dirt maybe is the wrong characterization.

People may have applied for a Social Security card in the 1940s and you went into an office. It was a paper-based process. They already have preprinted cards, and then an SS-5 form is filled out manually by the human being who wants to work and is shipped off to Baltimore. At a center, they transcribed it.

Years later it's transcribed into a system of records that's electronic. So people may have made a mistake. The document may have been ineligible.

I think it's less -- I think it's dirty in the generic sense, but I think it's more like when you dealing with a vast database of three or 400 million entries -- and some people were issued additional numbers or lost their number and they applied for a new one. Now this one human being has more than one card.

All these factors create this sense that -- and they will be able to tell you, for example, that their confidence -- let's say in the mother's maiden name, as a data field, they will be able to give you fairly good data on that.

They know how to deal with it, and I think IRS and other major agencies do as well. But the question is policymakers don't understand that there are tolerances. And then you use matches for identity verification, and they want everything in absolute terms, and it isn't that way all the time.

MR. BEALES: I would just note in response to Neville's question -- and you guys can answer. I mean we do have another major system in this country that's built on correcting errors as we find them and that's credit reporting. It works pretty well. It has errors. The data has dirt, but -- and it's a system with major consequences for individuals.

I mean, you can't have a perfect system and fixing errors as you go is certainly the way that works best in that system to try to keep the data as accurate as possible.

Richard Purcell.

MR. PURCELL: Brief comment just on that prior comment. Keep in mind, please, that the Social Security system is a system of accounts that are active accounts. It's not just a numbering system. We think of the Social Security number as being the key, but keep in mind that these are active accounts that are having deposits and withdrawals and closings and deaths.

And, I mean, part of the problem with that integrity is it's not just an assignment of an identity number and left at that. That would be one thing. But it is an active account management system with lots and lots and lots of transactions happening from huge numbers of sources, and also from people with exactly the same names.

My father's name is exactly the same as mine. We lived at the same address. He moved. I moved. Which account is which is not incredibly clear. End the breeding records are the only thing that can clarify that, and we all know that the breeding records are suspect in terms of how accurate or how easily counterfeited they can be. But I do have a question for Mr. Garza.

Mr. Garza, you said they have 35 successful hires under the E-Verify Act in the last the 90 days or less than that?

MR. GARZA: 60 days.

MR. PURCELL: Of those 35, did any encounter or did you run across any circumstances where you had a tentative nonconfirmation.

MR. GARZA: We did have one where we had to refer the person to DHS, and within a couple days it was resolved and that was it.

MR. PURCELL: And the individual was satisfied with that process?

MR. GARZA: Yes?

MR. PURCELL: And you were satisfied –

MR. GARZA: I was satisfied.

MR. HARPER: As far as that dirt question goes, I think there was a study by the Inspector General's Office that the finding is the Numadent database has a 4.1 percent error rate. That's from the 2006 study. But I believe that's the key database.

MR. BEALES: What's a Numadent?

MR. HARPER: That's a database they run it against. That would be roughly consistent with getting one in ten of nonconfirmation out of 35 because four percent would be one out of 25.

MR. BEALES: You say their error rate was four percent?

MR. HARPER: 4.1 percent. There was a stark difference in the question of appeal, final nonconfirmation goes down. I asked this question on the earlier panel. There's a stark difference between what they said on that panel is that folks would call in and we would figure it out, and Tim's verifying the reporting you gave us that the DHS has taken a position that legally they don't have to do anything.

I just wanted to sort of explore that a little more and maybe understand better. It's true that you had specific conversations about this, and they have said our legal position is we don't have any? And maybe for Eugene Spafford, as a practical matter, you talked about scalability.

If the policy is -- it's obviously unfair not to have the first panel folks come up and talk about it further, but is a policy of who will get it taken care of scalable? Expand, please, on that question.

MR. SPARAPANI: Sure. Thanks, Jim, for your question. I have indeed had multiple high-level conversations with individuals who have the responsibility at DHS for making legislative decisions about the future policy of the Department and their approach to certain pieces of pending legislation, and that is exactly the approach that they and members of other offices with legal responsibility -- that current programs at DHS have taken.

This is with all sorts of people in the room, almost to gasps, in terms of response and not just on one occasion but on many occasions. The position has hardened into something of an internal policy.

Now, they will say at the DHS, at the Department of Homeland Security, that this situation will be very rare, and I hope that that is true, and to which I have rebutted by saying, well, it's very rare, then why wouldn't you put together an immediate redress process where you can actually, quickly resolve this situation in the unfortunate circumstance, in the one in every one million, one in every ten million individuals to whom this may occur, if you believe this to be that rare.

And they don't have a response. Even when we're talking about individuals hypothetically who would have minimum wage-earning levels. I just -- it's unconscionable that the government would be putting people in a situation where they are denying people the right to work and then they are not the guarantor to make somebody financially whole for the government's mistakes or the inability of the government to sort out the rightfulness of somebody's work eligibility.

To me it just seems like a policy no-brainer that if you want this system so bad as a political tool and as an enforcement tool that you should take certain steps to ensure that, as they would like to think, very, very rare circumstances, you would have policies in place to resolve those favorably for those few individuals, but unfortunately that's the situation.

MR. SPAFFORD: So from an experiential point of view, looking at pilot systems, you get -- and their expansion, you have at least two effects, possibly three. The first is the experimental system effect. People are really interested in that. They want to see it succeed. So you have people who are troubleshooting.

You put extra help in place to resolve the problems, to analyze them, if nothing else, and to be able to claim success. When you expand the system, you no longer have the investment in making it work and therefore you no longer provide the resources to get the same level of attention to those failures that are involved.

The second problem with expanding systems is something known as an emergent system effect. You have problems that occur which were never anticipated at the scale at which you tested. So new things appear when you suddenly make something larger.

I think a very good example is what happened when we suddenly decided that everyone going to the Caribbean, Canada and Mexico needed a U.S. passport, and the meltdown that occurred at the State Department for issuing passports that is still not completely resolved is an example of such an emergent effect. It was not anticipated but could have been, at least in hindsight now that we look at the issues.

And the third thing that comes is if you have a system that's operational enough so that you have only a small number of cases which are the troublesome cases and the ones that Tim alludes to where someone goes through the initial appeals process. They call them. They talk to the help desk. They are still told they are still eligible. They have to show up in person with documentation, and they may live someplace and not have transportation.

There's going to be a very small number of those that are not going to be resolved satisfactorily, and because they are a small number, they won't be apparent to the legislators and to the appropriators.

So they are going to say the appeals process is working well enough. We can cut their budget. And so there's a concern there over time, the attrition of the program, that those people who are most in need are not going to have redress. And that's -- all three of those have occurred regularly with large-scale systems.

MR. BEALES: I guess I have one question for Mr. Sparapani. This report that you mentioned, the Gold Standards Report, the Westat report -- could you provide us with a precise citation to that?

MR. SPARAPANI: I would be happy to. I've actually got a hard copy. I'm sure that the folks from the government agencies have access to Westat and can share it. It's pubically available.

MR. BEALES: I just want to make sure that we know precisely what it is. I'm sure they can get it.

MS. BARNES: It is available on the E-Verify website as well.

MR. BEALES: On the E-Verify website. Okay. And I want to ask one specific question about it because you said that according to that report the error rate was a tenth of a percent of tentative nonconfirms, but that that would go to .8 percent if the system went national. What's the gap? What's the difference?

MR. SPARAPANI: Oh, boy, you know, the methodology is interesting, and I don't want to -- I don't know if I can truncate all of the study methodology for why they would extrapolate out to .81 percent, but some of the reasons were -- of course, they are looking at about three years of use of E-Verify, approximately three and a half million searches during that time period for participating employers, and that's where they got to that .1 percent.

Now, there is some reason with those participating employers -- our employers would be less likely to have problematical individuals who would be employees. For example, a number of the original companies participating in what was Basic Pilot, then becomes EEVA, now is E-Verify, got there because they ran afoul of INS and then DHS.

They were rated -- they were found to be actually employing undocumented immigrants. As part of their consent decree settlement with the Department of Justice, typically they were required to participate in E-Verify. So these were people who had already been found in violation of the law as employers.

So it's likely that they would have a workforce, going forward, you would think, logically, that would be more likely to toe the line and actually employ only work-eligible individuals.

I think that's sort of the first point. I think the second point is that the other employers perhaps, like Mr. Garza, and I can't speak for his corporation, are upstanding companies. They are companies that want to do the right thing and they want to have the safe harbor of knowing that they have gone through the process and they won't incur legal liability.

So you would think that those employers, logically, would take extra caution to ensure that their employee workforce -- the people they bring in the door -- are likely to be work eligible. I think that's less likely to be true extrapolated out to the general populace and to the nation's other 7.2, 7.4 million employers, if you include all the small mom and pop businesses.

MR. BEALES: Okay. Are there other questions? MR. SPARAPANI: I'm sorry. The report goes into great length about how it is they reach that methodology. I would just commend that to the committee.

MR. BEALES: I will look at it. Are there other questions? If not, we will adjourn for lunch.

Let me remind you that if you are interested in making a public comment, please sign up in the back of the room, if we have a public. And for the committee, our administrative luncheon session is next door in our old favorite, the Walnut Room. And we will start up again promptly at 1:30.

So thank you all for being here this morning, and we look forward to seeing you this afternoon.