NISPPAC, April 14, 2016

CIRA: -- the 53rd fall meeting of the NISPPAC. As you know, we tried to hold this meeting back in March but we had that unexpected cancellation of the Metro system so I don't think all of you are disappointed at the fact that we cancelled it that day because it would have been very difficult to pull it all off.

But anyway, I want to welcome all of you. I also want to welcome Ms. Beth Cobert from – Acting Director of OPM and Mr. Richard Hale from DoD. I'll be introducing them more later.

I'll introduce myself because I don't normally come to these meetings. But I am Bill Cira. I'm the Acting Director of the Information Security Oversight Office. So I'll be chairing the meeting today.

Some of you may know that back in January our previous director, John Fitzpatrick, moved on to a new job at the National Security Council. He's now the Director for Records, Access, and Information Security at National Security Council. And in that capacity he basically functions as our conduit into the National Security Council and the person that we go to at the NSC for policy matters

and other operational matters. So he's still very much involved in what we do here and our business here.

Our selection process for a new director is underway and we should be able to find out from the Archives who the new director is going to be in the not-too-distant future.

A couple of reminders for everybody. This is a public meeting and it's audio recorded. The microphones around the table can be repositioned in front of anyone who wants to speak. There's a floor microphone provided for any audience members to use. And anyone who's making a presentation but not sitting at the table can use the podium over on my left. Additionally, we have a teleconferencing capability set up for anyone who wants to call in and did not travel here today.

So we'll start off with the round of introductions. I've already introduced myself. I'm Bill Cira. And we'll take it this way, going to my left.

TORRES: I'm Greg Torres, back in as Director of Security at DoD. Started about two months ago. Really glad to be back.

PIECHOWSKI: Carl Piechowski for the Department of Energy.

BRADY: Denis Brady with the Nuclear Regulatory Commission.

DODSON: Jeffrey Dodson, NISPPAC Industry representative and also representative for United Coal Industry Association.

ACKISS: Scott Ackiss with Department of Homeland Security.

KEITH: Dennis Keith, NISPPAC Industry.

DESMOND: Lisa Desmond, Army.

BEAROR: Jeff Bearor, Director of Security, Department of the Navy.

LANZ: Steve Lanz, Air Force [APCO?].

WILKES: Quinton Wilkes, NISPPAC Industry.

HARRISON: Anna Harrison, Department of Justice.

MCLEOD: Donna McLeod, OPM, Department of Investigative Services.

VISCUSO: Pat Viscuso, one of the associate directors of ISOO for [CY?] program.

TRUE: Robert [True?] (inaudible) ISOO.

BRANCH: And Kathy Branch?, ISOO.

BAUGHER: Kim Baugher, State Department.

HANRATTY: Dennis Hanratty, National Security Agency.

SUTPHIN: Michelle Sutphin, Industry.

LADNER: George Ladner, CIA.

ROBINSON: Phil Robinson, Industry.

GORTLER: Fred Gortler, Defense Security Service.

MORRISON: Dave Morrison, DNI.

PANNONI: Greg Pannoni, ISOO, and the designated federal official for the meeting.

INGENITO: Tony Ingenito, Industry.

CIRA: And starting over there and going around the wall.

BERWICK: [Dan Berwick?], (inaudible).

MATCHETT: Noel Matchett, Information Security Industry.

BROWN: Shirley Brown, National Security Agency.

GREEN: Heather Green, Defense Security Service.

WALSH: Justin Walsh, DSS.

PULZONE: Doug Pulzone, Defense Security Service.

KUNKEL: Nissa Kunkel, Industry.

JARVIE: Vince Jarvie, Industry.

LAWRENCE: Mitch Lawrence, (inaudible) and Industry.

GORDON: [David Gordon?] representing (inaudible) International.

KIPP: Steve Kipp, Industry.

PAULSON: [Kirk Paulson?], Industry.

MIKE: [Keith Mike?], Defense Security Service.

HARBOR: Justin [Harbor?], DSS.

M: (inaudible) DoD.

LEWIS: Steve Lewis, (inaudible) government solutions.

HALE: Richard Hale, DoD.

COBERT: Beth Cobert, OPM.

BROWN: Tracy Brown, Defense Security Service.

ONUSKO: Jim Onusko, [MBIB?] Transition Team.

WILDER: Christy Wilder, [MBIB?] Transition Team.

MOSS: Leonard Moss, Industry.

SMITH: Anthony Smith, DHS.

CIRA: All right, and over there?

OHLEMACHER: Rick Ohlemacher, Industry.

NOVOTNY: Gary Novotny, ODNI.

EDINGTON: Mary Edington, Industry, and the NISPPAC (inaudible) working group (inaudible).

WENNERGREN: Dave Wennergren, Professional Services Council.

SOWELL: Charles Sowell, Industry.

M: (inaudible).

BRUCE: Eric (inaudible) Bruce, Industry.

BODIN: Mike Bodin, National Nuclear Security Administration.

BRAXTON: Kisha Braxton, Department of Commerce.

CIRA: OK. Well, thank you everybody. Definitely have a nice full house here today. At this point I'm going to turn to –

M: (inaudible) on the phone? I don't know, is there anyone on the phone?

CIRA: Oh, is there anyone on the phone?

RUSH: [Mark Rush?], Industry.

M: (inaudible) for NISPPAC.

CIRA: OK. Sounds like we got a couple –

SHIMER: [Michael Shimer?], Industry.

RUSH: [Mark Rush?], Industry.

ARIAGA: [Dennis Ariaga?], Industry, and MOU [NCMS?] rep.

CIRA: All right, thank you. So at this point I'm going to turn to Greg Pannoni. As he said, he's the designated federal official for the NISPPAC. He's also an associate director of ISOO and he's going to cover some administrative items before we get started.

PANNONI: Thank you, Mr. Chair. So good morning, everyone. I would like to recognize and welcome Kathy Branch. She's new to ISOO and the senior program analyst, having the NISPPAC and NISP as her primary responsibilities. So you'll be hearing and seeing her. Many of you already know Kathy. So welcome, Kathy.

No administrative items from the last meeting. The minutes, though, are in your packages on the left-hand side from the last meeting, as well as all the handouts for today's session. Back to you, Mr. Chair.

CIRA: Thank you. So as a lot of you know, at the November meeting we were discussing the breach of the OPM systems and the impact on us and industrial security. A lot has gone on since then in terms of security, suitability, and credentialing reform. And so then at this point I would like to turn it over to Ms. Cobert and Mr. Hale and they're going to give us an update on what's been going on in those areas. So... Did you want to use the podium?

COBERT: Sure.

CIRA: OK.

COBERT: That mic? Good morning. Thanks everybody for having us here today. Sorry about what happened with Metro. That was, as I recall, a very busy afternoon at OPM, as we were trying to figure out how to deal with that. So we appreciate everybody's understanding and patience. We are hoping that snow season is over at OPM. An interesting part of my job. Three in the morning is a really good time for a conference call.

But thanks, Bill. Thank you for everybody here for having us together here today and for giving us the opportunity to update you on the government-wide effort that we are working on to improve the background investigation process for the federal government. The input of the people in this room who we've worked with and who we will continue to have a dialogue with will be very important as we continue to shape our work. I wanted to provide a little bit of context just to level set about where we've been and where we're going. There will be time for questions but I thought it would be important just to set the context, sort of create a level playing field for folks here. So some background.

Following the increasing cyber security threats and the breaches of last year, and following and building on

the recommendation of the 120 review that we all completed the Navy Yard, the PAC began a comprehensive review of the background investigation process. Our aim was twofold. Was to think about the best ways to secure the sensitive data collected as part of the background investigation processes and to seek ways to modernize this critical government function so that its governance, workforce, and business processes meet the ever higher performance standards that it requires by the environment we're operating under.

Now, as all of you know, OPM's federal investigative services conducts investigations for more than a hundred federal agencies, about 95% of the total investigations government-wide. And in January the administration announced a framework for strategic and structural changes to modernize and fundamentally strengthen how the federal government performs background investigations. As part of this effort OPM will stand up a new government-wide service provider for background investigations, the National Background Investigation Bureau, NBIB, and that will be housed within OPM. Also as part of this framework the Department of Defense, with its unique national security perspective and capabilities, will design, build, secure and operate the NBIB's investigative IT systems, in

coordination with the NBIB. And Richard's going to talk about that in just a moment. This is a true partnership. They will be both our core supplier on IT, as well as our largest customer in terms of the outputs of the background investigation process. We think that creates a really productive helpful relationship and gives us a lot to build on.

NBIB is going to be focused on its mission to produce effective, efficient, and secure background investigations for the federal government. This process will represent significant change on a number of dimensions that I just wanted to highlight briefly here. One, the head of the NBIB will be a presidential appointee and a full member of the PAC. A full member of the PAC. So that will help us align the operational and policy components of the background investigation work together and bring all those forces, people, together. Second, the NBIB will be provided with its needed operational flexibility and dedicated support structures for the specialized skills while still utilizing some of the more general administrative support that OPM's organization structure provides. But it will have that dedicated support. And finally, as I mentioned earlier, NBIB will operate and

leverage DoD's considerable IT, national security, and cybersecurity expertise.

So we are starting down the implementation efforts to stand up the NBIB. We've established a transition team, and you'll hear from two of its leadership in a few minutes. It's comprised of experts with expertise in background investigations, and suitability and security policy, as well as those with significant organizational and change management experience. We've explicitly set out and have succeeded in getting a true interagency group. We wanted to have those different perspectives as we bring this work together to think about how we can maintain momentum where we have it and accelerate improvements where we need them. Their work's going to focus on business process analysis and reengineering, resource management, IT, and cybersecurity, and the transition to DoD, how we structure appropriate mission support services for NBIB, and overall the change management process involved in standing up NBIB. They have been and will continue to work closely with the existing [FIS?] leadership and with other folks involved in the security and background investigation process across the government so that we can make these changes while minimizing disruption to the ongoing

operations. And you'll hear more from them in just a minute.

I wanted to just pause for a minute. Richard's going to talk about where we're going around our IT systems with DoD but I wanted to just reiterate to folks here that there has been and continues to be an ongoing effort at OPM to strengthen our systems in a very focused, in a multilayered way. We have made significant improvements over the past year in building our defenses and responsiveness. To cite a couple of examples – and I could go on and on, by the way. We've implemented enforcement of [PIV?] cards for two-factor authentication for network access. We've increased the number of stands that we do on a regular basis to review the network for signs of compromise. We've worked with our interagency partners. And I need -- so there's representatives from those agencies in the room who have all been incredible partners to us. This was a true intergovernment effort with support from DoD, DHS, NSA, the FBI, OMB. WE would take -- we took all the help that was offered and we really put it to work. So a big thanks there. We've tightened our policies and practices for privileged users. We have an ongoing review process for our high value assets. We have a new acting chief information security officer. Four new SES leaders in the

IT organization, four new senior program managers. We've brought in into my office a senior advisor on cybersecurity and information technology from the private sector, deep experience in running large IT organizations, a former West Point grad, former Army, as well, on security issues. And we have at the moment the privilege of having Lisa Schlosser, who was the deputy federal CIO, has come over to OPM as our acting chief information officer and a senior advisor to me. So we have brought in a great deal of expertise as we continue to do the work to strengthen our systems, even as they operate today, and to work closely with our colleagues from DoD in this transition process.

One more comment since I think a few of you might have questions about this, just to talk about where we are also in our ongoing work and reducing the backlog of investigations. We know we need to address this and are taking steps to move forward. There are a number of efforts we're putting in place to try and think about how can we run the process more efficiently and do that in coordination with our stakeholders. We have increased our hiring capacity for federal staff to be field investigations. We have a target of getting to 400 this year. We are well on our path to do that. We actually just graduated another class of folks last week who are now

out in the field doing work. We're also working with our existing contractors to help them onboard and increase their own capacity.

So those are all the pieces that we have under way. I wanted to just provide that context. I also want to say that this whole effort in terms of decision-making to get us to the NBIB and the work that's going on to stand it up has been a great example of interagency collaboration. Our colleagues from the DNI, from DoD, from OBM, the rest of the PAC membership, we meet together on a frequent basis. We have very frank and open conversations and what makes it effective is that we are all focused on a shared goal about doing this process well, making sure it is effective, making sure it is of high quality, making sure it is responsive to the needs of our stakeholders. We have a lot of work to do but I am very confident in the team and the way we are coming at this from a whole government perspective. So I look forward to taking your questions. But first I'm going to turn it over to Richard.

HALE: Thank you, Beth. So I'm Richard Hale. I'm the cybersecurity lead for DoD but I'm also the lead for putting a new investigation system on the ground. So what's going on in DoD is that we've put a team together and it's a handpicked, first-rate set of folks working

closely with the NBIB, in particular in the business process reengineering effort, so that whatever we put in place as a new system for this is sensitive to the way the whole process is going to change as we move from mostly episodic investigative driven data about people to more continuous big data kind of approach. So the requirements gathering is going on. There's been a great deal of work that's been done before DoD, who owned this job of building a new system, and so we're taking that as the primary input right now. We are going to do a model-based requirements process, an iterative sort of build and try process that is primarily focused on better defining requirements. So we're trying to make pieces that are going to be visible to customers, available early so we can sort out what really -- what problems we really need to solve as opposed to the ones that we think we need to solve. And some of that capability may turn into pieces of the operational system depending on how this end-to-end business process (inaudible) works out and how our end-to-end architectural look works out. The one thing I'd say we've concluded already is that we have a lot of pieces to this, right. There are a bunch of pieces around. Deciding to look into someone's trustworthiness, right, so this idea that you need to initiate something, to look into Richard Hale and

what we know about him. And then there's the part about learning about Richard Hale and then there's some part about making a decision about Richard Hale and publishing that decision so the right people can get to that decision and use it for something. And DoD is working in the middle piece of that end-to-end process but the cybersecurity, the performance, the dependability all have to be worked end-to-end. So we're going to want to work with everybody as we puzzle out interfaces and puzzle out boundaries because, again, they are not clear necessarily going forward as the business process changes. And we're going to want to make sure, again, the customers who are initiating (inaudible) are customers who need data, are customers who are involved in doing this process, of learning about Richard Hale, are getting the inputs that they need or the outputs that they need, and that we again come up with a completely new security approach to this data model. Because, again, as we move to a more continuous evaluation model we are going to have a lot of data about a lot of people, far more than we've ever had before. So, again, the structure of this thing is going to have to be end-to-end. So we'll have some challenges around what legacy stuff is allowed to connect to whatever new things we build, and that's legacy stuff either on the deciding to investigate Richard Hale or

making a decision about Richard Hale, adjudication systems, systems that hold the results of the adjudication, that kind of stuff. And we'll put processes in place. And, again, we'll be as transparent as possible about how those are going to work. And we will start to set standards for some of the inputs and outputs.

So just for one second to talk about the current system. So we're going to continue to use the existing investigative infrastructure at OPM for a while. So DoD money starts in fiscal '17 for this effort. But, again, we are allowed to do pre-acquisition activities and then OPM is funding some of this early architecture work and business process engineering work. The current system, though, is going to be operational for probably some years as we transition incrementally off of it and onto the new system. And so DoD is already committing to putting more DoD people on the ground at OPM right this second to help with better securing and operating the existing system and then help to manage this transition. So we really are joined at the hip on both the current system and on whatever the new system is going to look like. Again, I think the message I'd leave is it's going to be challenging because, again, there are serious security, privacy, civil liberties issues in the design of this new thing that's

going to know a lot of data about a lot of people and we're going to need help from everybody to come up with the best way ahead, whatever best means. So thanks.

COBERT: Let me -- do you want to introduce yourselves? Is that OK? And then we'll do questions?

ONUSKO: Sure, yeah.

COBERT: Is that OK? SO let me just get Jim Onusko, who's going -- who's leading the NBIB transition. I thought -- I know it's slightly different on the agenda but maybe if they introduce themselves and what they're doing, you sort of have the whole picture, and then we're happy to take questions if that's OK. (inaudible).

ONUSKO: Thank you. I'm Jim Onusko, the NBIB Transition Leader and nice to be with you today. I know many of you so... If I don't know many of you after this, I'd certainly like to meet you. Christy Wilder.

WILDER: Hi. Yes. Christy Wilder and I know many of you guys, as well, in my prior role with ODNI, in which I was a member here in brief for about three and a half years, metrics, and the oversight capacity of that. So happy to be back. And were you going to say a few words about the team? OK.

ONUSKO: Yes. So we are very fortunate to have a very talented team on the NBIB transition team. They bring a wealth of

knowledge and experience with both change management and the personnel security expertise. So to start with, we'll have five work streams, the first of which is change management. So change management will actually change the culture that we need to transform all aspects of the new organization come 1 October into the future state that's required. Secondly, a business reengineering process work stream. So as has been mentioned, there's already been a business process reengineering study kicked off. For those in industry you'll be glad to know that DSS is firmly embedded within that study group. It includes representatives throughout the federal community. So we're really looking for an integrated sort of analysis of what needs to change and certainly then working very closely to build out those requirements to achieve those ends. We have a resource management work stream. That's from Laura Duke. She comes over from OMB and brings a wealth of knowledge and experience. Our IT work stream, led by [Curtis Mayor?], and Curtis would work very closely with DoD and DISA in building out our requirements both for security and then for a new innovative IT system end-to-end that can actually perform the mission in the desired state that is at issue here. And then mission support will be led by [Jamal Hardy?] --

WILDER: [Harley?].

ONUSKO: -- [Harley?] and she comes to us from ODNI and some of you know her. She's a very talented lady who will bring the resource capabilities in both people and resources to provide the dedicated support and operational flexibility to make NBIB more successful. So given that... I failed to mention Victoria Gold from ATF will lead the change management work stream. And for the business process analysis and reengineering we have Mark Sherwin, who's the deputy associate director at FIS, who knows the operations of the current FIS process extremely well. So we feel we have a very robust team and collaboratively working with you all and others in a very aggressive outreach process to identify your requirements as stakeholders and reel all those in, working very closely with Richard and his team to bring it all together. Thank you.

COBERT: So we're happy to take questions. We can answer where we have answers and, if not, they'll be good questions for us to put on our list of things we need to get to if we haven't gotten to them yet. So happy to take questions from anyone. Go ahead.

M: Thank you for joining us today. I guess since we have you here –

COBERT: Sure.

M: -- what is -- what's the single thing that we in industry can do to help enable you moving forward?

COBERT: That's a very good question.

M: Right? I mean, you've got a captive audience in this forum and if you want to follow it up with Greg or whatever that's fine, too. But I think it's important that, you know, we can (inaudible).

COBERT: So let me just... I'll give you my answer and then Richard can weigh in. So, one, industry are our partners in this on many different dimensions. Right? You need individuals to be cleared. Industry also provides some of the data. I mean, there's a whole different way we interact. We are working to set up a structured way to get that input. We need and want your input and so that's the first thing I'd say, is we need your input. And what we'd like as you do that is to think about it from this end-to-end perspective. Right? You know what you need as stakeholders/customers. But as you think about that, you know, thinking through so we can leverage your experiences and creativity for how we can get some of these knotty problems solved. Because the one thing I've learned in my time working on this issue, as I've said in a couple of other forums -- the first thing I was tasked with when I was joined OMB as the deputy director for management was

actually as the PAC chair leading the Navy Yard review. That was literally the first thing I got on my second day of work. This is a very complicated and difficult process. Right? We're trying to sift through reams of information to make really tough judgments on things that have a really high stake to get right. So your input is what we need and we will come back with ways that we can do that. But thinking about that and thinking about that, saying, you know, how can we get that done in a way that will work for the full set of the enterprise? We would really like that input. The second thing I will ask you for is some patience. There are many changes we need to make. The shift to continuous evaluation, which we talked about following the Navy Yard, is a very important one. It involves some very, very fundamental changes. And we are going to be coming at this and the systems developed with sort of an agile mindset. We are going to try some things. We're going to do that in a way that is careful and thoughtful, manages our risk. But we will be doing some of this -- the way to do that well is to try and learn. So a little bit of patience while we go through that. But not so much patience, because we also all know that we need to be moving on this quickly. It is important work. It needs to be done. So ideas, a little bit of patience, a little

bit of pressure to keep us moving. That's what I'd say. I don't know if you want to add anything?

_: (inaudible).

M: Beth?

COBERT: Yeah?

INGENITO: Hi, Tony Ingenito. I think it's admirable that you guys have now gotten, you know, 400 new positions. But we know that that whole process and training and implementation... What is the timetable that you guys are looking at to try and get them all in place and trained, because we see -- in industry we see the continual growth of the backlog and we also see the potential with some of these new major contract awards on the government side, a drastic increase in cleared individuals to support some of those particular programs.

COBERT: So we are bringing folks onboard. We've actually... I think we finished one class, I think we've finished the second class. So we have actually pushed up the hiring of those folks. The commitment was to have 400 onboard by year-end and we are trying to do that and get them through training as rapidly as we practically can because we feel the same pressure you do and we know the operational and the challenges that having the backlog creates. We're continuing to work with our contractors to help them and

add capacity and to think about things we can do within the context of the current workflow that can make changes happen. So we're actually working through a number of those things. It is going to take some time but we've accelerated where we are. We've already got -- some of the new folks we've hired are now out in the field. They've finished training. And we're looking at other things we can do to build up capacity faster and making sure we -- though we're doing that in a way that ensures people actually have the training they need to do their jobs right. The longer-term solution to this comes with things like the recompete of the field investigation contract, right, which has just gone out to the market recently, to think about how we can also use those things to sort of create a more systemic solution for the long haul. But the FIS team will tell you we talk about this every -- so we're working and tracking those things.

TORRES: Hi, Beth, this is -- it's Greg Torres, and so I'll add to that. You may not know but as we speak, right this very moment, there is a team of folks from OPM, from ODNI, from DoD, and others, looking at what we can do to mitigate the requirements that we have right now. So there is -- there's always... You know, we have rules and policies on what we need to do, when we need to do it, and how we need

to do it. So this group is working right now in another meeting to understand where we might be able to make some changes that might have some significant impact to help us as a collective group buy down the challenges that we have going on right now. So that's something that's ongoing. So we're all working together on this and I will say certainly the challenges that are being felt by industry are being felt beyond industry, right, inside the Department of Defense, as well. And I just got a request for a meeting, to meet with the components, to talk about what are the impacts to hiring, what are the impacts to periodic reinvestigations, all those things. So we're working to do that. So I think that we will come up with some innovative solutions that will be added to the larger effort that will help this, as well, sooner rather than later.

M: Yes, this is for Mr. Hale. Can you speak a little bit more about the model based requirements process that you were talking about and whether or not that's addressing sort of the work processes in existence today or some yet to be articulated, to be state?

HALE: So we're looking at both. And the as yet to be articulated, to be state, is partially articulated. So we have the business process reengineering effort going on as

a government but, again, there was a tremendous amount of business process and reengineering work that was done before this. So we're taking that as a given, although it'll change. And so we have this idea that early on we want to prototype some of the things that we think are going to be stable in the requirement, in particular how people enter the system for the first time. So I fill out... You know, I just finished filling out my reinvestigation form for the millionth time, since I'm an old DoD guy. And so we're going to start with that. Below that we're going to do some prototyping of some data model things around the cybersecurity that won't be visible to customers but we're going to do the application part and then we're going to try prototyping some of the interface things to adjudication systems or to personnel systems. And then we're not sure where we're going to go from there. We have this iterative thing with architecture business process, architecture business process, and we'll have contracts in place that allow us to try a lot of different things. Again, those are a couple of the early ones. Sure.

POULSEN: Good morning. Kirk Poulsen. I'd first just say that Christy and James did a great job the other day. They briefed a number of industry representatives (inaudible).

But I wanted to ask you if you had a timeline for when you expect to be -- to reach your full operating capability.

COBERT: So we are -- we will have a timeline. It's not quite there yet in terms of what are the key milestones we need to reach. We've spoken about some of them, getting the initial standup of NBIB, you know, at the end of the fiscal -- this fiscal year. Partly because, as everybody here knows, sort of once you're into a fiscal year there's some other things that get hard to move. So we are working through that. That is actually the first task of the transition team and we are happy to come back and T some of that up as we go. So we... You know, more to come. But it is thinking about, again, how do we accelerate progress, move towards things, but also do that in a way that, again, keeps current operations running at the pace they need to be running, at the quality and security they need to be running. And so it's getting all those things balanced together. So the transition team will be working on that. And as we get that out we will be, you know, making that available because we need to hold ourselves accountable to meeting the deadlines that we all agree to. Sure.

M: Excuse me, Beth.

COBERT: Yeah.

M: This is more of an implementation comment, maybe not a question.

COBERT: That's O-- comments are OK.

M: I've been involved with this group for more than 11 years and they seem a little shy this morning. But, nonetheless, one of the things -- one of the themes that I've seen many times over is we have policies which are wonderful but in terms of implementation and consistency this is where oftentimes we hear from our industry colleagues in particular areas like reciprocity, how we do things. And it really transcends not just the clearance environment but the suitability environment, getting access to a base and different commander requirements or whomever's in charge of having (inaudible). So I think the idea of a champion for consistency and implementation is something that would be very helpful. And I'm not sure who that champion would be but... Just... That's my comment.

COBERT: Yeah. It's a very helpful comment. In my role at OPM and in my prior role at OMB both of those organizations have responsibilities that my definition cut across the federal government. Right? That's what they do. They are not sort of down through a line. It's much more across, which is a hard thing to do. And one of the themes that I've stressed with my teams in a number of different areas,

not just this one, is once we have the policy how do we get clarity about implementation? How do we get consistency in implementation? And that we need to spend as much, if not more time, thinking about how we communicate, make things clear, make things happen in all the disparate places, frankly, in this part of the world, right, around the globe where it has to happen. And so I think it's a really important issue. That's one of the reasons, as we were pulling together the transition team, we wanted to have broad interagency representation on it. Is because it'll bring us experiences of how things happen differently in different places. What did it take to get something to work at the VA versus the State Department versus here and then how -- and through the multiple parts of DoD, right. So we've got folks that bring different perspectives as we're thinking about policy, thinking about how we're going to implement it. Is critically important. So I would agree with your comment and please keep raising that issue to us. It'll be an important one. Ideas on that as much as policy and model design would actually be really welcome in terms of what makes the network work well.

M: Thank you.

M: Continuing on that point. From -- within our companies and industry, one of the directions that we're trying to go is

to... When we put out policy at the top we try and minimize it to where each entity below that needs to put out their own policy to support that policy. And we know that there's been a lot of concerns over the years about the timeliness to put out policy from the government to the entities that then need to develop their own implementation of that policy all the way down. And we're going years with inconsistent guidance and so forth. It'd be nice to see an approach, you know, especially, you know, from a government standpoint, when we try and design something at the top, try and put it out so that not a lot of changes can or should be made just to personalize it for each particular agency and branch.

HALE: So I'll make a comment about that. I think a lot of us here agree with that wholeheartedly. I think the challenge is finding the balance. And so when you take an organization, just DoD, for example, and it applies to lots of organizations, when we're writing policy it's generally easy to write a piece of policy that is so generic that nobody can object to it. Right. But then you have inconsistency. And then when you try to become very specific you get a lot of objection. You know, it's trying to get... When you get that specific, get everybody to be satisfied that it meets all of their needs. So I think

that our experience has been that you're exactly right and that is the challenge is trying to find that sweet spot where you have enough specificity that everybody's not doing it differently but enough leeway that you're not trying to solve every individual organization's challenges. So we agree with you. We need to find that balance.

M: OK, I'll ask one more. So I'm really sort of fascinated with the change management and cultural work stream. So what's the biggest challenge in that?

COBERT: So there's a whole set of issues as we think about this that cut across multiple dimensions, right. So there is the question of how do we, within NBIB, sort of continue some of the transformation that was started with some of the, frankly, strategy and policy recommendations out of the 120-day review. Moving from just a mental model of sort of the periodic, call it more paper-based, person-based investigatory model, to a continuous evaluation model that is much more driven by data analytics, right? That was a clear recommendation coming out of the Navy Yard review. That is a very different mindset for an individual, for someone working in that space. And you've got to make sure you're doing that. So that's one example. You know, there's a set of culture and change management issues as we create the operational flexibility and

dedicated resources within NBIB. There's a set of implications for the rest of OPM and our -- the other parts of our mission, which are ensuring we have a terrific workforce inside the federal government. Background investigations is an important component of that but it is not the only thing we do. So as we make those changes to have NBIB operate the way we all intend it to act, it's got a bunch of implications for the rest of OPM. We are building a tighter working relationship with DoD around the IT side. Right. That is different than how we've operated before and there's a lot of things to work through there. The good news, particularly for that one, is we have worked together on so many different things over time and in particular, frankly, following the breach this year, on a whole range of very operational things, whether it was standing up and executing the contract for identity theft protection. We worked with [NAPC?] as our contract support. We worked with DLA and [DFAS?] to get the letters out. It was, you know, a whole new set of things that we didn't do. Richard and I talked every single morning at 8:30 about how we were doing on those things. So we've got real opportunities to sort of build on some successes, to sort of have the mindset of we are creating something that serves us all and not just DoD and OPM but the entire

federal government and our industry partners. And so I think it's bringing all of that mindset, working those things through against this goal of modernizing the systems, doing them the best way we can, improving the processes and ensuring things are secure. And so I think that's -- keeping those things -- when we focus on what the goals are you actually can work through a lot of the other pieces. But it will require changes in people's jobs and how they do their work every day and you have to think about how you do that in advance. That's really what we're focused on. Right.

F: How do you foresee utilizing social media in future investigations?

COBERT: You know, we are continuing to work through a social media policy. Right. We are doing a bit of a pilot now at OPM. DoD's done some work with that, with their pilot. So there's both a policy perspective on how we do that in a way that is appropriate, respects people's privacy, but leverages the valuable information that's there. We've got to do that right. So we are continuing to work that through and working through the final stages of the policy around that. But I do think the approach of doing some pilots... Right? This is new. It's a new type of information. We have to make sure it's relevant. We have

to think about how we do that. So DoD's been running some pilots. We're actually going to start a pilot at OPM. There's other places. We're going to have to actually do some learning as we go because it is valuable information. But we've got to make sure we treat it appropriately for what it is and what it isn't and all the, you know, appropriate privacy protections that go with it. (inaudible). So let me just say thank you again for the comments here today. Please, we really do want your input. The forum we held yesterday was one of a series of things we're going to be doing. So we would love to continue to gather feedback from our industry partners, our government partners. This is a task that actually falls to all of us. We all play a role in making it happen. We all play a role in the consequences of when it goes well and if it doesn't. So we look forward to continuing the dialogue with you, finding ways to get that input, getting your ideas, and working with us as we continue to make improvements on this really important topic. Thanks so much for the time today.

CIRA: Thank you again, Ms. Cobert and Mr. Hale, for coming out here and speaking with us directly on what's been going on and answering our questions. Also thank Mr. Onusko and Ms. Wilder for their presentation and comments. I'd like to turn now to the reports and updates section of our

meeting. And for that we'll start off with Patrick Viscuso, who's an Associate Director of ISOO and our director for the CUI program, and he will give us an update on the controlled unclassified information program. Patrick?

VISCUSO: OK. Good morning, everyone. Can everyone hear me all right?

M: Yeah.

VISCUSO: Great. All right. So if we look at the CUI program there are three main elements to it. It was established by an executive order in 2010 and these are the three elements that are contained in that executive order. The first one is that there is a scope and that scope is all information that a law, a regulation, federal regulation, or a government-wide policy requires to be protected outside of classified information. So this is unclassified information that a law, a regulation, a government-wide policy require to be protected. And NARA is the executive agent of this program and we were required to establish that scope within a year of that executive order, and we did. And we have added to what is that scope, which is contained in a CUI registry which is online right now. Twenty-three categories and 83 subcategories of unclassified information that requires protection

throughout the entire executive branch and each one of these categories contains links to the exact authority, the law, the regulation, the government-wide policy that requires that protection.

A second element of the program which is rooted in the executive order is guidance. And the executive order speaks of consistency of government practice in four main areas, which are safeguarding the dissemination of the information, the marking of the information, and also it's (inaudible) control. And for that purpose the order directed that the CUI executive agent issue directives and the appropriate vehicle for such a directive would be actually a federal regulation. The 32 CRF 2004, which we have been developing for five years now. We developed it informally with a CUI Advisory Council. The executive order said consult with affected agencies. So the affected agencies that are in that CUI Advisory Council are actually based on the membership of the CFO Council, the Chief Financial Officers Council, and control most of the federal budget. So there are 28 agencies represented there, with the addition of CIA and FBI. And with them we developed informally a federal regulation and then embarked for the past two years on the formal OMB managed public rule making process, numerous interagency comment periods and a public

comment period, resulting now in the final stages of the finalization of this federal rule. We are expecting an issuance in May with an effective date 60 days afterwards, most likely in July. And so its status is in its final stages.

There is a third part to the program and it is also contained in the executive order and it speaks to the implementation of the program, which is phased implementation. We have established milestones, phases, deadlines. That's what the executive order told us to do. We have established them with the affected agencies. And we have coordinated with OMB. It is captured in a national implementation issuance that will accompany the federal rule. What does it call for? Well, here are some of the milestones. Within 180 days we expect parent agencies to develop policies that implement the federal regulation within 180 days from their finalization of their agency, the parent agency policy. We expect them to then do the same with their components. From the date -- 180 days of the finalization of the agency policy we expect the development of training to take place and 180 days from that point, the training of the federal workforce. We expect within the first year to be a transition assessment and development of transition plans for the IT systems.

There are IT requirements in the federal regulation. It centers on a requirement consistent with OMB policies and NISP guidelines and standards, which is to be at moderate confidentiality for the protection of the information. There will be the development of a self-inspection program by the agencies, which will be related to the obligation established by the executive order for the CUI executive agent to do an annual report to the president on the status of the program and its implementation.

I think this group would be most concerned in how this will affect industry. We intend from the finalization, from the issuance of the federal regulation, to embark on the process of developing a universal FAR clause that will be used to bring about consistency in the implementation of the requirements of the program for industry. And it will make reference to a document that we developed in partnership with the National Institute of Standards and Technology, which is the NISP special publication 800 171, which addresses how moderate confidentiality should be implemented within the non-federal environment. What guided this document was the idea that you would not be concerned with things that would be particular federal requirements, such as COOP plans. You would not want to require COOP plans for the non-federal environment. A good

thing but obviously a federal requirement. You would not be concerned if you were focusing on -- if you were focusing on confidentiality you would not want to be involved -- the government would not have an interest in the availability of a contractor's internal system, receiving federal information incidental to the provision of a service or product to the US government.

So these were some of the factors that guided us in the development of the NISP document. And we anticipate developing this FAR clause using the usual processes of the FAR Council and its public rulemaking process, which would involve considerable comment from industry. We have an interest in hearing industry on these points and we have met with industry associations to hear their concerns and their needs. We will continue to do that. We want to be informed. We also are very concerned about the university and the academic community and we have had very good discussions with associations that are involved with those communities and have focused our discussions with them on the whole idea of fundamental research and the need to protect fundamental research in order to maintain the technological edge of our country.

That, in short, is a brief high level overview of the status of the program. And I do -- do we have any time for questions, Bill or Greg? Can I take a question or two?

CIRA: Sure, go ahead.

VISCUSO: Yeah.

CIRA: Go ahead. If anyone has any questions, go ahead. There's one back there.

VISCUSO: Yeah.

F: (inaudible) expected timeline for the FAR clause for industry?

VISCUSO: Yeah. So we... We project about a year for the development. We sort of flowcharted the process of how a FAR clause is developed. It's a very involved process, as you might imagine. It does involve public comment. The development of the NISP document involved several rounds of worldwide public comment. I don't think it extends that far. But nevertheless, I think all of the industry members in this audience would have an opportunity to comment on that FAR. And, as I said, we're very open to speaking in front of industry associations. We have done so. We will continue to do so and we would like to hear any concerns or needs that you might express. Obviously it extends beyond the group that is represented here, that handles classified information. Estimates are that this FAR clause would

affect 300,000 contractors to the executive branch. So that necessitates a different sort of approach. Self-certification, the use of SAM. Different ideas than would be used for classified information. OK. Well, if there's nobody else... Feel free to contact me directly. As all of you know, ISOO's contact information for all of the staff is posted online. Our email addresses and telephone numbers are quite open, so feel free to do a Google search on me with ISOO and you'll be able to get my contact information. Thank you.

CIRA: Thank you, Pat. At this point I'd like to turn the floor back over to Greg Pannoni, who is going to give us an overview of the revisions to the NISP Implementing Directive.

PANNONI: Thank you, Bill. Before I start I'd just like to take a moment to publicly acknowledge my colleague Pat Viscuso and his team. This has really been a challenging thing, as you might imagine, trying to stand up a new program. And they've worked really hard with the -- in our agency to get where they are today. And so thanks, Pat.

The NISP Implementing Directive, we're already far along so we don't have the same challenges. We already have a code of federal regulation 32 CFR for the NISP program. So we're in the process of updating it, as I

briefed at our last meeting. We've been meeting with the cognizant security agencies, plus DSS and the CIA since they are the primary implementers of the program for the government. We're close to having a working draft. This revision began, as I mentioned before at a previous meeting, because of the changes with the insider threat program coming onboard. We had to add some requirements for the government to implement those requirements vis-à-vis industry. But as we started to dive into the directive we saw that since we hadn't updated it in about nine years there were some gaps. There were areas where essentially we were relying on the NISPOM, which as you know is an operating manual for industry and not necessarily the document that the government is supposed to take its cue from. But in reality that's what's happened with things such as the facility security clearance process, foreign ownership control and influence, FOCI standards, national interest determination standards and a few others. So if anything we needed to get those documented into the federal regulation. And not just to have them there but the idea of a single integrated cohesive program which is just we saw the NISP is in its executive order. This will help drive it. So, for example, facility security clearance is actually a term that not every CSA utilizes. We have one

CSA that uses open, open cases, whereas DoD and others use facility security clearances. The nomenclature isn't necessarily important. What we're driving at is that the eligibility determination factors for -- whether we call it a facility security clearance or an eligibility determination for an entity, that we're all operating from the same baseline. If some want to exceed, OK, because of SCI and higher levels of sensitive information. But we all -- we need to be establishing a baseline that we're all operating on. So that's kind of what was uncovered as we've gone down this path of looking at the directive. We're well on our way. We're meeting again this afternoon. The CSAs and DSS, CIA. Hopefully in a couple of more meetings -- I know last time I said early in 2016. Perhaps it's not early anymore. But we intend to then provide the document to all the NISP government agencies that are impacted, to consult as we're expected to do by way of the order, executive order, and then from there on to the National Security Council for the approval. And then, two, we have to put this into federal register for a public comment period of probably 60 days. So that's kind of a brief summary of where we are with the implementing directive. Are there any questions? Yes?

SUTPHIN: Greg, is there any anticipation that any of this will impact the NISPPAC charter or bylaws?

PANNONI: I don't think there is, Michelle. And I'll add to that. Also, we don't think there will be any impact to the NISPOM itself because we're trying to be very careful not to break any of the requirements that are already there. So no, I would say not.

SUTPHIN: OK.

PANNONI: Anyone else? OK. Thank you. Back to you, Mr. Chair.

CIRA: All right, Greg, thanks. The Department of Defense has also experienced some leadership since our last meeting in November. Greg Torres is now the director of security in the Office of the Undersecretary of Defense for Intelligence and Greg is here to give us an update from the Department of Defense. Thank you, Greg.

TORRES: Great, thanks. And so I think it's been about, oh, I want to say seven years since I've been in this room, so I'm happy to be back seeing a lot of familiar folks that are still, I would say, fighting the good fight. And so good news. I think some people have already heard. So there are just a couple, three things I wanted to cover.

First is NISPOM change two and it has a clear legal sufficiency review. And so what that means for us is that we're just putting the final touches. And when I say we

I'm talking about Valerie Hale. So putting the finishing touches on that and hopefully that will be published here very soon. And when I say very soon, we're talking weeks, not many months. So if I had to guess I would say next month, if I had to guess when that will actually be published. So I think that that's really a very good new story for us.

Now, connected to that, the other thing I wanted to mention is the ISL, specifically for insider threat. We are well aware that from an industry perspective that is going to be critical to get the ISL done. The ISL, as you know, is -- you may not know -- is written. It is already in legal sufficiency review. And we know that that needs to come very quickly on the heels of change two. And we're expecting that's going to happen. We have meetings on a regular basis to try to help prioritize the things that go on inside the department to move these things along. So, again, I'm sort of newly back again, just getting into all of this about two months ago, and so this will certainly have a lot of my focus and I think we're now going to be in better shape with these two particular items. So I wanted to mention just one other topic from an update perspective. But before I do that does anybody have any questions about that timeline or anything regarding that?

OK. So just as an announcement, Ben Richardson -- where are you, Ben? -- back here has just been selected as the deputy director of security. So he's now my new deputy. Comes to us from inside the Department, ATL, acquisition and technology logistics. Has a history and wealth of knowledge in everything from CFIUS and also previously working at DSS. So we're glad to have him onboard. And he is really sinking into a lot of this stuff to help me with this, as well. So just wanted to welcome Ben onboard. I'm sure you will all get to know him.

And the last thing I wanted to mention is that one of the things that has recently come to my attention is that there are some, I would say, other government agencies that, for different particular reasons, would like to have access, direct access to JPAS. And I'm not really clear on the whys about that and what we might be able to do to help on that. But I think it deserves some dialogue and some conversation, so I wanted to let... If there's anybody here who is seeking that from another government agency, directly following this meeting I plan to stay around. So come and approach me and we can have a conversation about that. But that's really important updates that are going on within DoD, the change two and the industrial security

letter and we're really happy about that. I think that's all I have for right now. Yeah.

F: To that end, the JPAS access, I've actually written up something to say during the end of this meeting with regard to that, historically and our concerns. So that's really good to know that it's on your plate.

TORRES: It is. And like I said, right after this, if you want to have a dialogue, Ben and I will be staying behind to have that, anybody who wants to talk about that. So thank you.

F: And I'm going to say it to everybody.

TORRES: OK.

F: Because I think there's other agencies that have some concerns, as well. So great. Hmm?

F: (inaudible) talking about this for a couple of years.

F: About 10.

TORRES: Great.

CIRA: All right. All right. Thank you, Greg. I'm sure most of you have heard that Defense Security Service has also had a leadership change since our last meeting. Their director, Stan Sims, retired at the end of the year and Mr. Dan Payne, who came from the National Counterintelligence and Security Center, is now the director of DSS. And we look forward to working with him. But here today on behalf

of DSS is Fred Gortler, the Director of Industrial Policy and Programs, and he will be giving us a DSS update.

GORTLER: Thank you, Sir. Director Payne returned from TDY late last evening but we think we'll introduce him to this forum in Nashville and he's looking forward to it. Let me add to the chair that the director is looking at four specific areas right now and not unexpected. But improving integration of counterintelligence and security. Next, improving integration collaboration at the federal level. And I guess this goes to the presentation from OPM and the CIO. Third, building on the very solid foundation of partnership between government and industry. And then lastly, strengthening relationships with our foreign allies. I'd like to add another note to something Mr. Torres said and that's on the industrial security letter. Seems like a long time ago now but it was November/December when representatives from this room came and for the very first time helped us to develop that ISL. So we recognize how important it is in terms of implementing change two. And we appreciate attention by OSD and Mr. Torres on that. Lastly, I'm joined by about six or seven subject matter experts. We came primarily to address PSI for industry but we're prepared to discuss anything, any other topic you

might have. For right now let me turn it over to Keith Minard.

MINARD: Good afternoon. Keith Minard, Defense Security Service. We've got a couple of updates for you, referenced primarily PSI but we've also been asked about a snapshot on the annual security cost collection survey that DSS conducts. Up on the screen you'll find a slide. It kind of gives a snapshot of what DSS does annually to collect the costs associated with NISP security program management. Thirty-two CFR subpart F of 2001-61 requires the Secretary of Defense, acting as the executive agent, to conduct cost assessment surveys to consolidate the cost of the NISP. This year it was conducted in January and February. It was a sampling survey of about 1700 companies, which results in an analytical review to determine the total cost for DoD oversight to the 13,000 facilities for security costs. Those costs are located in the FY15 column, about $1.27 billion in total that (inaudible) security costs. And you can see that those costs have been pretty consistent since about 2009, as he's been moving along.

Next to that is -- I have a couple updates on personal security clearance. e-QIP submission update. We're still continuing to deal with funding constraints. DSS has had to limit the number of investigation requests submitted to

OPM to stay within our budget authority. This is based -- has resulted in a delay in processing some investigations but we're prioritizing key management personnel, initials, and periodic reviews. If you have any concerns or any critical needs you can contact personal security management office for industry. And talking about contacting DSS. In the last month defense security service has restructured its call center to the knowledge center. It's created a new (inaudible) environment. So when you call in -- the primary number hasn't changed. But when you call in it kind of gives you a wider capability to reach those parties you need to reach. It's kind of been decentralized. It allows to reach out for account lockouts, personal security clearance, contact with the PSMO office, facility clearance information, OBMS stuff. And then on two new added areas in the phone tree itself is contacting our international office and actually contacting my office referencing this policy. So we kind of expanded that capability to reach those elements within DSS you need to reach by a simple -- starting with a simple contact number. And if you go to the DSS website and search for knowledge center you can find that number.

The next thing is the... This has been brought up, the industry stakeholders. But the personal security

investigation update for the PSI survey. It started on March 14th and it was anticipated to actually complete today for the cost survey for personal security clearances for industry but it's been extended one week. Right now we're at about 85% collection. Last year we had a total of 89%. So we're hoping that we can exceed that 89% to get a better understanding, because facility participation -- it's critical to DoD to make sure that we can program and understand what those requirements are for upcoming years for personal security clearance budget management.

The last thing I actually have to offer is actually for DSS oversight and DoD agreements. Recently the United States Postal Service signed an agreement with DoD to provide industrial security services. So what that does is it brings -- the United States Postal Service is the 31st agency with agreements with DoD where we provide oversight of cleared contractor operations related to the NISP and so they're kind of growing the process. That's kind of -- we've seen a trend in the last probably two to three years where we've added about five or six different federal agencies to the program. So it is showing growth. It is showing need for oversight and for those industrial security services. That's all I have, unless you have any questions. Thank you.

M: I have a question. Are you guys going to communicate to industry while you're -- with the backlog of cases that you have pending at the [PSOI?] as far as your -- you said your own process (inaudible) and that kind of thing. Are you guys going to tell industry, going to put it on your website, let them know what's going on so that we understand why it's taking so long to get interims, that kind of stuff?

MINARD: Heather, you have a communication plan?

GREEN: Yes. Yes, we do. So (inaudible) strategies and we're (inaudible). But yeah. And we're processing them all. So it's not that we're not processing. (inaudible) just take a little bit longer based on our quarterly (inaudible) applications.

M: Right. And we're just concerned that because (inaudible) is taking longer for you guys to grant the interim (inaudible) to put people to work but there's no communication posted out on why. So we're just concerned on... You know, we look at the growing numbers and see that it's taking longer but you guys aren't telling us why it's taking longer.

GREEN: Right. Well, we're certainly (inaudible) out there. We do have a little bit of information out there on (inaudible) website but I'll make sure it's up to date.

M: Thanks.

F: So are you going to get more funding or is somebody... I mean, this is a funding issue, right, the delays? So is somebody looking to get you more money because you (inaudible)?

MINARD: Usually throughout the year those issues are addressed up through DoD, to manage the budget requirements. And as you know, that we have pauses and periods of processing clearances because of budget but then we have to work through to make sure that the availability of funds there. And then DSS reaches out through our financial (inaudible) office to actually look for increases and redeployment of budget resources to meet those requirements. It's not always a 100% at the end of the year. The challenge is, with industry, is -- though the PSI survey is really important so we can capture those costs. So if you haven't or you haven't partners that haven't submitted that, it's a baseline that allows us to at least have an idea, functionally through that survey, of what those costs are going to be. DSS, like many of the government agencies that we provide services for, aren't able to actually capture exactly how many classified contracts will happen during a year, how many cleared contracts will be required. But we have to work within that allowance with our budget.

But the survey's a very important part of how we manage those requirements. So there's like a relationship here to what we're doing with our budget constraints in the survey that's out there. So on an industry perspective, make sure that you're actually addressing that survey and providing input.

M: As you do that survey, does it take into consideration – so it's OK to forecast any (inaudible) I'm going to have for my future requirements but does it take into consideration the backlog? Because as of right now that backlog's growing and that's going to be carried forward. So is there some consideration to make sure that the budget addresses what's currently sitting in the queue?

MINARD: I'll let Preston Harper from our PSI management office actually...

HARPER: Any cases that are planning to be deferred would be captured in that year (inaudible).

M: (inaudible).

_: Could you speak up, please, so the rest of the room could hear that?

HARPER: Sure. Any cases that potentially will be deferred to out years are captured in our out year projection.

TORRES: This is Greg Torres. I'll also add to that. I think that another challenge is that quite often within the

department funding doesn't come all at once, right. You don't get all your money for the whole year all at once. And it comes in increments. And as it comes in increments that increment might be a straight line increment. But in any given month, coming in from internal to the department or even in industry, you may be... You're going to be below or above that particular line. And if you go over that line but you only got funding at the line, that creates a bit of a challenge. But as far as, I think, the underlying question about how do we do a better job at projecting requirements, that is something that we're going to look at. Also moving forward there's a study going on right now at PERSEREC to try to understand that, to get better estimates. But also I would suggest that this will be something that needs to be considered as we build out the new system from end-to-end so we can better capture requirements. Because I think that's something that has challenged us, I think, forever. But I'll certainly be interested in having more of a discussion internal to the department in where my office might be able to help from a funding perspective.

M: And speaking of requirements, one of the areas we have to focus on from a government industry perspective is... From a government perspective, please be aware that the

investigations that DSS processes are only for access to classified. So take care when you're doing your 254s or requiring contractors to submit investigations from a government perspective for base access, for IT level [1Os?]. Those are a government respon-- agency responsibility for funding and managing. On a contractor perspective, please contact us if you see any deviations in there that we may be able to assist with your government contract, your government customer. Because while they may seem small, those numbers do impact our ability and funding to actually process the investigations needed to support classified contract work.

M: (inaudible) one additional detail for the two questions. So, number one, we do indeed account for the backlog. To get to Mr. Torres' point, we are even spending faster to maximize the flow and we are working with higher headquarters to get additional funding for the next quarter. And we will look to make sure that we get a clear communications line out to industry on this.

M: I just have a question for Keith, then. I understand if you don't have it (inaudible). What was the participation rate this year out of 13,000 (inaudible)?

MINARD: For the PSI survey?

M: Yeah. For the cost -- no, for the cost collection.

MINARD: Well, it's a sampling. There were 1700 companies sampled for that, to create the cost.

M: OK. I'll follow-up offline with you on some of these.

M: Keith, I have a follow-up one. Just how is this data used?

MINARD: What?

M: How is this data used?

MINARD: The data for the PSI survey or for the cost collection?

M: The cost collection.

MINARD: Cost collection is actually included in the national report from ISOO to the president (inaudible).

M: We have a requirement to report to the president --

_: (inaudible).

M: -- the cost of implementing both the program on the federal side, the executive branch side, as well as for industry.

M: So other than reporting is it used to -- with any adjustments to policy approaches? I mean, you --

M: Not that I'm aware of.

M: No?

CIRA: No, it's just -- the whole concept for this goes back to the late 1970s and it was determined that -- back then that ISOO should include in its report the levels of classification activity every year and the amount of money that's spent on the security of classified information,

really just as a way for the government to be accountable and open with the public is the main reason for it.

M: All right.

M: That's its purpose.

M: Yeah. I think, just on behalf of industry, as we move forward kind of in this next evolution, this becomes a real key element. And so I for one would be interested in seeing whether the current methodology that was established in 2008 really reflects where industry is and non-traditional industry partners and how their defense industrial base has essentially expanded in what were heretofore not traditional. And so I'll take that offline and we'll work with DSS as our conduit to that.

M: Sure.

M: But I like -- noted that. I think that we should, as an industry community, look at this and probably get some more detailed information from Keith on the study and then really determine, as representative industry, whether the methodology is still a reasonable approach and is meeting the intent for this forum and for ISOO.

CIRA: That's fine. Yeah.

MINARD: Any other questions? Thank you.

CIRA: All right. Well, thank you, Fred and Keith and the other people from DSS. So then at this point we'll have an

update on combined industry presentation from Mr. Tony Ingenito, who's the NISPPAC industry spokesperson. Tony? There you go.

INGENITO: Thank you, Mr. Chair. Next slide. Consistent membership. Next slide. Same with the MOUs. OK. Under the OPM data breach I think a number of the items that were in here that I was going to talk about we covered when Ms. Cobert and her staff was just up on stage. So we appreciate, you know, the input and the update and we look forward to your transition plan with timeframe and so forth. So we can't -- we're very anxious on that so we can't wait to see it. Next slide, please.

On the CUI, we -- again, most of the data up there, it's consistent. We received a status from Pat and so... The only thing I want to touch on is that we are continuing to start to see through contracts clauses, you know, of the NIST 800-171 publication from certain government agencies, even though we know that the CUI has not been promulgated completely out. So we continue to try and educate our contract people to look for that and to go back and challenge it back with those particular user agencies that are trying to implement it right now.

Next slide, please. Consistency. We got the updates here on where we are in conforming change two. Happy to

hear it finally came out of legal sufficiency review. Look forward to when it does actually hit the street and we start to implement. We're just a little concerned based on some of that. I know that we're looking, and industry has had some meetings with DSS, Fred, and, you know, with basically some of the NISPPAC MOU representatives. We believe it's probably a good idea to continue moving forward once this hits the street so that we can have an insider (inaudible) working group that meets on a regular basis. And --

M: If I may, we can take that up under the NISPPAC and create that sort of ad hoc working group. And I'll be glad to do that.

INGENITO: OK. That sounds good. Next slide, please. We're still, you know, waiting to see what DHS starts to develop in working their section addendum to the NISPOM for those non-NISP entities that are now going to be falling in there. It's just kind of interesting that... I just received an email from Valerie [Hyle?] just last night about some individuals that are non-NISP are reaching out and wondering how can they participate and provide input to some of this type of data. So we'll need to sit down and kind of talk a little bit about it here on the NISPPAC and Valerie when she gets back.

Next slide, please. Well, I think we've heard everything when it comes to the status. I know... I think the team that has been working the NISPOM rewrite, both industry and government, has been very, very good. I mean, we've had the buckets and we've gone through all the buckets. We've provided the input back to the CSAs and now we just await the final review of whatever -- the CSAs changes so that can flow back through with the group. And, again, I know that with OSD working with the individual government reps and then working with industry and government in the same room on some of these, really, really was a good one. When industry brought up a lot of our questions or concerns it really was beneficial to have those government individuals in the room to listen to us, to see what it was and why we're saying that this is going to be a challenge for industry. And it did go back and make some concessions to some of that. So I think it was a very good formula that we should continue looking at as we move forward with other particular policies.

And from the standpoint of the special access programs, we know that all of the SAP manuals have been published and we have received guidance from the Air Force SAPCO about resending the [JFANs?] and to be implementing them and we haven't seen any other official guidance down

through any of the other SAPCOs at this time but I'm sure they're currently in development. Next slide.

In the area of policy integration, we continue to track in excess of 80 different initiatives out there. We did have a quasi-working group meeting with Greg and a number of other industry representatives for the policy integration and we did discuss and look to try and establish a little bit of a procedure or policy, whatever. Not a policy but working guidance here to make sure that when we start looking at some of these things... I mean, industry, we were tracking close and over a hundred different initiatives, because the whole reason that this working group was established was the continual promulgation of policy and/or procedures, why they're waiting on policy from different user agencies. And so it came pretty large. But one of the things that we've decided that we need to do is when we get these things we need to have like an executive level committee of industry, look to vet and validate some of these through the MOUs and the NISPPACs and then work with some of our US government counterparts so this way we can truly identify the cost and the impact. So the next kind of stage when Greg and I were talking is that we need to truly identify those representatives from the different one of these user

agencies that we can truly have as that belly button that'll work with the NISPPAC, that when we start to get some of these things we can flow it to them for some input, you know, to say "Is this in fact what you guys are trying to do? Are you even aware that this entity underneath your agency is trying to do this?" And before we start trying to run down the path and really surface it to everybody. Because we need to first work it with a smaller group before it becomes the real issue. So that's the intent where we want to formulate that and start to move forward. So we'll be doing that in some future meetings and I guess Greg will eventually be reaching out to you guys for some identifications of representatives for your policy and so forth.

Next slide, please. You'll be getting, I guess, some out briefs here on some of the NISPPAC working groups, you know, the personal security. I think we've already talked about some of the issues here but I will just, you know, reemphasize that, you know, some of the impact that we're seeing with, you know, the T3 investigative for background checks and the subject interview, we continue to start to see that that is, again, slowing the process down. We just touched briefly about the backlog of what's processing through the PSMOI office because of the financial

challenges with some of the funding being reallocated toward the credit bureau cost and so forth, that were being monitored. So, again, we very much support and encourage industry to get the most accurate projections and to take into account their business so that if they're looking at a flat growth for 2016, and we know that in industry we're starting to project for growth in late 2017 and 2018 and significant growth for 2018 and 2019. And, again, when I say significant, you know, we're talking possibly a two to three percent growth, especially as we see, as I mentioned previously, some of these very large acquisitions that were just awarded and knowing where that's going to be going, which then creates that challenge. As we look at the clearance reductions, the low hanging fruit that the government has identified and reduced by that 15, 20%, I don't think that that's realistic to expect that in the future as we're going to start growing. We are going to see the number of clearances going up. So we'll just continue touching on that. And I'll let the PCO working group touch on some of the issues.

SOWELL: Tony, just to add one --

INGENITO: Yes, Charlie?

SOWELL: -- request for predominantly industry members, but USCI and for ESS to look at, is the defense agencies that

are considering moving to the (inaudible) polygraph and some of the challenges in polygrapher numbers within DoD, DHS, making a significant number of hires, et cetera. It's just another pressure that's going to affect industry in a large way in the coming years.

INGENITO: And to add on that, Charlie. Also, the additional -- in some of the IC community, with the poly going for the next level of that poly based on (inaudible), with what accesses and so forth, you know, we can see individuals possibly being disqualified from their current jobs as they continue to roll that down to the next level. So definitely some concerns with those challenges.

Still in the area of personal security. We know that... We spoke in the past at the stakeholder meeting about the FBI and their ability to conduct the checks for the interims and for the CAT Cards. We know it's not the fingerprints, as had been the problem in the past with the automation of the fingerprint process. But now it's the actual, you know, physical check of the records. So we are feeling that particular impact, you know, in industry, in the interims and the delays in the interim, as well as the issuance and trying to get CAT cards through.

As far as the next one, the CNA working group, we believe a lot of good things coming out. And I won't steal

from their thunder. You know, we worked as a team. We've been working this for the past year-and-a-half and I think that the industry's in a lot better position to roll it out, you know, at the NISPOM level. So I'll let them brief on that.

Next slide, please. SAP working group. We haven't had a meeting. You know, we continue to try and work through and implement the JSIG and the RMF, you know, with the different user agencies. We still continue to have the challenges and I think it's both for the government, as well as industry. We can't keep up with those, you know, those IS, information insurance type people, and the level that's needed with the CISSPs. Individuals are changing jobs, going for $20,000 or more to change and go down the street to another company. And we see that on the government side, losing some of the scholars that we have been working with, are also jumping and going to industry. So I continue to see that as being a challenge as we start -- as we continue to try and work together on the government and industry side to meet the JSIG RMF requirements on the systems.

In the area of -- you know, under ad hoc we know that... You know, we continue to kind of...

M: Tony, can I ask you a question (inaudible)? So are you getting... Is the inconsistent guidance on the JSIG RMF stuff improving?

INGENITO: Well, we're -- what we're doing is... You know, we see the guidance. We see the regs. But what happens now is the individuals then are trying to work it and work it with their counterpart at the government to go down that path. Because it's not as simple as here's the reg, let's put the procedures and everything together and submit it. Because we're finding that, you know, each particular IA representative for the different contracts or for the different debts or so forth, they each have their own different interpretation as to what it should be and so it's a lot of having to dialogue with the give and take but because there's so many industry representatives going to that same stuff we're not getting the good dialogue that needs to happen because everybody is inundating them with that particular... You know, trying to get their plans in place and so forth. And so -- and that, in addition to, again, the change and the losing both government and industry, those people working it, and then we get a new person coming in and have to start all over again. So...

M: OK.

INGENITO: OK?

M: Thank you.

INGENITO: OK. The 254 NCCCS. You know, we continue to have industry involved and I believe -- I guess there's a new momentum on the beta test happening in that area, which is a good thing. Again, we continue to have industry representation on the NISS system, just looking for the next meeting, as to when that'll happen. We know that in the potential JPAS replacement, the Joint Verification Systems, looks like they are trying to roll out for industry in November, which is a little kind of concerning. Especially in the past, having lived through what we had to do for the JPAS implementation and the needs for training and development of training, that's an area where, based on some last meetings, that we don't see a training plan in place from the government with industry on this. Years ago the philosophy was, "Industry, you guys are smart. You guys will figure it out." Well, that didn't quite work too well. Industry took it upon itself to develop its own training before the government was able to take some of that training and NCDS really then accelerated and got those training plans in place. But we are a little bit concerned about rolling this system out without a true training plan and a rollout for that training plan. And

that's everything that I have from an industry perspective. Any questions? Thank you, Mr. Chairman.

CIRA: Thank you, Tony. So we can now move into the working groups portion of our agenda. And to start that off we have Tracy Brown from DSS here to talk about the Certification and Accreditation Working Group. Tracy?

BROWN: OK. Good morning. I'll be providing the risk management framework update for Defense Security Service, who is the security -- the (inaudible) office for DoD. The working group will be working with the other CSAs to provide their implementation to RMF in the future. Next slide.

RMF is replacing the certification and accreditation process. RMS processes were established by the National Institute for Standards and Technology in partnership with DoD, the intel community, and the Committee on National Security Systems.

Next slide. It provides an effective and efficient approach to risk management and creates a common foundation for information systems security supporting reciprocity.

Next slide. Here you see our key reference documents. Go from the NISP to the CNSS guidance to the NISPOM change two. One key note for change two. It will point all the CSAs to develop a process manual.

Next slide. The risk management framework. Just want to do a quick recap of the six steps, the first being categorization, selection of security controls, implementing those controls, assessing those controls, authorizing the system, and then going through the continuance monitoring step for the life cycle of the system.

Next slide. DSS is scheduled to release our next assessment and authorization process manual in July 2016. We are having a phased approach to implementing the transition of the systems. Effective August 1st we will be having new standalone systems to follow through the RMF process. The LANS interconnected systems will not be required to transition until next year, March of 2017. What we're doing right now in preparation of the transition, we have started an RMF pilot with industry that's running from April the 1st through May 31st. The pilot is intended to help us early on to understand if we want to have any challenges with transitioning to RMF. We don't want to relive the issues that the intel community faced in their transition. So the pilot will be used for, one, for us to assess the time it's taking with categorization and selecting the controls throughout authorization of the system. During the pilot we already

have -- we're using the draft assessment and authorization manual and all the supporting artifacts. At the end of the pilot, if required, we will update any of the information that we have before the July release of the process manual.

Next slide. Next slide. Pretty much covered that. To prepare industry for the RMF with DSS our training academy already have eight classes that's online within our step environment. To supplement this training we will be having webinars with our implementation for assessing the controls. We have our first assessment control webinar tentatively scheduled with CDSC for June 15th. We'll also have others hosted by the ODAA staff succeeding in July.

Next slide. OK. We're not going to do the backup slide. As far as our current timelines, ODAA is still sending (inaudible) and processing -- authorizing systems to process within the 30 days. We do suspect those timelines to be adjusted with RMF. However, we are pressing to keep our authorization timelines as close to the 30 days as possible. The pilot will kind of shake that out. Our goal is to not exceed 60 days but we are pressing to stay as close to 30 days as reasonably possible.

Any questions?

M: Tracy, just to make sure I clarify. You had a slide on timelines and I believe it said 18 months, existing 18 of

those approval (inaudible) will then have to convert over to the risk management framework within 18 months of August 2016. So essentially February of 2018 is the date by which all systems will have to convert over to the RMF. Is that correct?

BROWN: OK. Let me go back, Sir. Thank you for that question.

M: Could you pop that slide up again, Robert?

BROWN: Any -- any authorization that is existing would continue through its lifecycle, if that clarifies. So if you were to receive an ATO today it will have a three-year authorization.

M: Three-year auth-- OK.

BROWN: If -- on August 1st, all accreditations issued will not exceed the 18 months.

M: OK.

BROWN: OK.

M: So beginning on August 1st --

BROWN: Beginning on August 1st --

M: -- they will not exceed 18 months.

BROWN: Right. And that's for --

M: Any new ATFs. OK.

BROWN: -- any new ATFS.

M: That helps. Thank you.

BROWN: And so the systems that are not standalone will follow their existing process until next year.

M: OK. Thank you.

BROWN: (inaudible). Thank you.

CIRA: Any other questions? All right. Thanks, Tracy. All right, we have one more working group report. This will be from the Personnel Security Clearance Working Group. Kathy Branch from ISOO is now chairing the working group and she will lead off, followed by Donna McLeod from OPM, Gary Novotny from ODNI and Dan Purtill from the DoDCAF.

BRANCH: And thank you. I'm glad to have the opportunity to now chair this working group and we're going to continue to look at the stats as we have been from OPM and all of the agencies who do background investigations and make adjudicative determinations. So that's not going to change. But we're going to be most interested in the reform efforts and the standup of the NBIB. So we've been most happy to have OPM with us all along. The PAC has agreed to become a member of our working group. So I wanted everybody to know that And we are also going to turn this group into an issues forum. We talked about setting up a separate group for issues but we decided this is the issues forum. Some of the issues that come up are, quite frankly, outside of the purview of the NISP but

that's OK because it's a place for everybody to bring their issues because all of these issues affect industry's ability to effectively perform on contracts. So we're looking for industry to bring those issues and we'll try to address them as best we can and at least the issues are laid on the table. So just wanted to lay that out before we moved on into the actual presentation. So with that, Donna, I think you're next.

MCLEOD: So my discussion today, what I want to do, is really talk about what OPM federal investigative services, what we're doing to address the backlog. Director Cobert did mention some of it during her briefing and some other people had mentioned some. But I just wanted to go into a little more detail of some things that FIS is specifically doing moving forward.

So we're looking at multiple ways to streamline and improve the process that we have in place now for background investigations. We have the numbers here. I believe the numbers have been reported previously from Lisa [Loss?] when she attended the meetings. And our timeliness numbers have continued to increase. But we wanted to see what can we do to help get the numbers down and decrease the backlog. So one thing that we did, we met with our customer agencies, and we had a brainstorming session where

we talked about the things that we're doing and taking all their suggestions as far as what we could do to change our processes. One thing that came up was our report writing style. Maybe we can streamline the reporting content so when our investigators are completing the report maybe it can save time on their end and for the adjudication and may possibly save time on the time it takes to review the report. So that's something we're looking into.

Director Cobert already talked about the ability or our goal to hire 400 additional investigators and we are on track to do that. But also wanted to mention that once those investigators are onboard it will take time to get them up to speed. They have a four-week training class that they have to go to, in-class training up in our Boyers office or Slippery Rock office up in Pennsylvania. But they also have some mentoring they have to do with the investigators once they finish the classroom training and they have a one-year probationary period for them while they're performing their job. So once we get the staff onboard it will take some time to get everyone up to speed where they're fully productive and they can be doing work on their own.

The other thing I wanted to mention, and Director Cobert already mentioned this, is our work to increase the

contractor workforce. Because if we increase capacity we will have more availability of resources to help address the backlog.

And the final thing I wanted to mention is that when you talk -- when we speak of the backlog that FIS is currently experiencing, that is not unique to FIS. That we've also talked to our delegate investigative agencies that are doing investigative work also and they are experiencing the same backlog issues that we have at FIS. Primarily, one thing that -- and I think this was raised earlier, the problem with FBI and getting the record information from FBI. Because of their lacking capacity also, they have delays in responding to our request, which means that our investigations are pending a little longer waiting for that check to come through. So I just want to make sure that everyone is aware that it's a very wide problem. Again, it's not unique to FIS and we will continue to work with our stakeholders, with industry, and identify any additional methods we can do to improve our processes. That's all I have. Any questions?

F: Yes, I have a question. What specifically is FBI doing to address the problem? I understand that OPM is hiring more investigators but what is FBI doing?

MCLEOD: We had talked to FBI about... One of the things that we recommended, possibly having some additional resources from FIS to directly do the work for FIS. That was one thing we explored with them. But one of the challenges in doing that, of course, is the training that's involved or required to do the FBI work. The resources will have to be there physically so there may be a different type of investigation they'll have to undergo, which will take longer maybe to get them fully staffed to do that. I am aware that FBI is also looking to bring on additional resources. The same thing that we're doing internally with FIS, they're doing the same thing. But, again, it's a limited capacity. So how do you increase that capacity where more people are available to do the work?

F: Are they considering contracting that work out to industry?

MCLEOD: I don't know specifically but in talking... And our records research group that work directly with the FBI, we were told that they're looking to increase it. How they're doing it, as far as contract or federal workforce, I can't respond to that.

M: I (inaudible) for the records (inaudible) division at FBI just maybe two weeks ago asking this question. And they are trying to hire more contractors. They, of course, suffered the same issue when the contract went away from

OPM, which is why they're so far behind. One strategy that I thought was kind of interesting is she mentioned reaching out to retired special agents to bring onboard who don't require the learning curve that someone fresh off the street needs in order to look at the record and interpret it because they're already familiar with all the records there. And so there's a little bit of a -- you get two for one. Next exactly. But you hire one, you get a little bit more than you would of someone just off the street. So they're focusing on that. The real issue there is West Virginia and moving out to West Virginia and how many of that cadre of retired folks are there. But they're very aware of the backlog. They also would just like folks to... If there's at all a way to prioritize the request coming in to them, they are very willing to focus on the top priority ones that come in to the extent that people are able to articulate that.

MCLEOD: Yeah. And just to follow-up to that. That was one of the other points I wanted to bring up in terms of what FIS is trying to do to address the backlog. One was ask agencies to please prioritize the work that's coming in so we can make sure that we have the resources, focusing on what needs to be done the fastest or the soonest. And the other thing is if there's a need for cancellation, please

get that notification in as soon as possible because that, again, will allow us to divert resources from working investigations that are no longer needed.

M: Is that process an automated process or can it be automated or is that something they're doing by hand or a human has to take a look at it?

MCLEOD: From what I was told, and Dave, you may know more about this, but they have an algorithm that they're working to try to improve the process. But until that is complete there is a manual search that has to be done with their record check.

M: Right. The records are in paper.

MCLEOD: Yeah.

M: Well, I mean --

M: No, not (inaudible) have a lot of great initiatives underway to address the backlog. But can you give us a sense of... Do you have any projections on when, over time, it becomes eliminated? When do these things become so effective and you've got the workforce in place, you've made the changes, FBI is up and running. At what point do you really eliminate or start to crest?

MCLEOD: Well, we have projected, based on the ability to hire all the investigators and get everything on board -- and this was before the NBIB was actually brought up -- that it

would take us several years before we would actually be able to get better. We're trying to fine-tune those timelines as we achieve those initiatives to give us a more definite idea of when we could improve but I don't have an exact date to provide.

BRANCH: Just (inaudible) thank you for those (inaudible). It's a dynamic process, right. So we've seen unexpected increases in demand this year. Had we not had those we would have had a backlog but it wouldn't have been as severe. So while there's a question of does that continue or did we end up just sort of getting all the volume in the first half of the year? So it's quite a dynamic process. Unfortunately it will take some time and that's why we're sort of looking at what are the mix and the different levers that we can pull on sort of the demand side, understanding prioritization, as well as on the supply side with contractors, on the efficiency side with process changes. So the sort of forecast is so dependent on these different variables. But there is one. But it is going to take a while. It's taken us a while to get to where we are. It is going to take us a while to work our way out of this. The rebuild of the NBIB systems that we're working with DoD on, some of those things may help but some of those will improve other things and not improve this. So

not a very satisfactory answer, I understand. A while is appropriate but we are continuing to do this and the things about cancellation, understanding prioritization, all those things are the things -- is sort of the things we're focused on because we can actually do something there that will make real improvements and so that's sort of how we're trying to work our way through.

M: I have sort of a question similar to Michelle's. But with non-federal partners and their assistance in the investigative process... Over the years it's been sort of spotty, uneven. In terms of their cooperation with providing information, investigative information at the state and local levels, is there a strategy that's been developed to get, you know, better cooperation among those parties?

MCLEOD: Well, one thing that I know we're definitely looking at is trying to work through those partnerships, to make sure that the provider understand the need for the investigation information. So in terms of... Say for a record provided for law enforcement. We have a dedicated group within FIS that will reach out to those providers to make sure they understand the importance of getting that information to the investigation.

BRANCH: We also, through actually some great bipartisan help in Congress, got some provisions in the last NDAA about, you know, the law enforcement status of investigators. So we're working -- we see real improvements in different pockets. It is something we're going to continue to work on and as we think about standing up NBIB, this capability to work with law enforcement, it was a piece of the work coming out of a 120-day review and the records access taskforce. That is work that is continuing. We see pockets of improvement. There's still plenty of opportunity to do more. The NDAA provisions are actually a meaningful help when folks are going out there.

M: Thank you. Thank you.

F: I don't want to beat this dead horse to death but I really want to emphasize the FBI portion. Right now fingerprints are not required to get an interim clearance and very soon they will be. And if we're having these delays on the fingerprints and we can't get interim clearances and we can't put people to work this is going to be a very serious issue very quickly.

MCLEOD: So just to clarify. The backlog that we're dealing with are not the fingerprints. It's when we do a check with FBI, the name based search, those are the ones that are delayed, not the fingerprint searches.

F: So the name based -- the name searches are not required for the fingerprint check to go through?

MCLEOD: So the name -- when we need to do a check of FBI based on -- it's called a headquarters check that we do. It's different from getting a technical fingerprint check. That is pretty much all automated and those responses come back fairly quickly. That is not the delay.

F: So the name checks will not hold up the interim clearances going forward?

M: I believe the (inaudible).

M: Yes, yes.

M: (inaudible) right.

M: (inaudible).

M: So yes.

MCLEOD: The name. Not the fingerprint check. The name. When we do a name based search, that is the delay, not the finger -- so we said fingerprint. I just want to make sure people know it's not the technical fingerprint we're talking about.

F: But it is delaying the NAC?

MCLEOD: Yes, because that name based search is part of it. Correct.

F: So we're going to have a major issue if this doesn't get resolved.

M: And at this time industry is based off of -- our interim's are based off of (inaudible) review only because DSS has a waiver. But once the waiver is up or they transition from the waiver and we have to do it that way, this is going to be an impact on us because if it's already a backlog it's just going to be worse. So our interim process is going to go from a couple of weeks to who knows how long.

CIRA: Anything else, then, Kathy? Are we...

BRANCH: Do we have time to hear through the ODNI? And we've got one other set of slides. Do you want to do that or...? We're at the twelve o'clock mark so defer to the group here.

CIRA: Go ahead.

BRANCH: OK. Gary.

NOVOTNY: (inaudible) guys. So I'll go through these very quickly then. My name's Gary Novotny and I'm just going to go over real quick the DoD industry timeliness data and the IC contractor data. So just real quick, we're using the performance accountability council security clearance methodology, where we're looking at the end-to-end timeliness, which starts at the initiate phase through the adjudication. So any of your pre-coordination or post-coordination is not included in these timeliness metrics.

So just moving to the next slide. Kind of gives an overview of the timeliness metrics for, like I said, the DoD and IC contractor data. And it pretty much goes along with the slides that Donna had up there really quickly. From the end-to-end timeliness, for both the secret and the top secret, you know, the numbers have continued to rise. This is, remember, the first quarter of the fiscal year. So October, November, December. I think a good new story, though, is looking at those periodic reinvestigations. At the end there the time did go down. And if you look at the volume, the number of PRs did rise and the time went down. So I guess there is a good news story with the PRs. You know, one of the initiatives in the NDAA was for Director Clapper to, you know, get a hold on the periodic reinvestigation backlog and the timeliness. So, you know, that's a start there in that first quarter. So obviously we're going to analyze the second quarter data and reach out to agencies to see if this was just kind of a delta in just that first quarter or if there's something that we can work upon to help reduce that backlog.

So the next three slides just kind of break down the secret, top secret, and PR into the different initiate, investigation, and adjudication phase. So as you see for the secret clearance, obviously the background

investigation portion is missing that 40-day mark. Moving onto the next slide. Same with TS. Whereas, you know, the bulk of that end-to-end timeliness goal is that background investigation timeliness phase. So missing the mark there. But, again, moving on to the next slide. In the PRs, all three phases in that first quarter were reaching their goal. First quarter fiscal year '16, the adjudication phase, initiation phase. I'm sorry, no, the investigation isn't. I'm sorry, it's still a little bit above there for the investigation phase. But like I said, they kind of go along with OPM slides that are probably in your folders. You know, they're going to continue to rise as Donna said. But they (inaudible) plan and, as Director Cobert said, we're working. DNI and OPM and OMB are all working together, a lot of group meetings, a lot of coming together to try to tackle that backlog and the growing timeliness.

And then just one slide I have at the end here. Don't (inaudible). Just a few other initiative that I've spoken to in the last couple of meetings and that we've continued to see progress on. So not only are we focused on the timeliness but obviously we want to focus on the quality of the background investigation, as well. And just last week Director Cobert and Director Clapper signed the quality assessment standards and implementation plan, so those

quality standards were signed last year. We were able to get an implementation plan out to the heads of the agencies. That should have either been sent yesterday or we'll be sending today. Implementation plan on implementing those quality standards. And along with that we're creating the tool at the ODNI to collect those quality metrics. And this all just emphasizes the quality of the background investigation. So when it gets to the adjudicator you have a quality product. We're not just focusing on that timeliness, that we're getting you a quality product, as well. So we're continuing to see momentum with the quality assessment standards. And just a few other directives that we're working on.

The mandatory reporting requirements for your cleared population. So we have a directive that we're coordinating right now that we're trying to push out. That's going to be the minimum mandatory reporting requirements for your secret level population, your top secret, and your TSSCI. So there's different criteria in that directive that will be required to be reported to the security office. And Mary already brought up the social media policy and I think Director Cobert spoke to that, as well, is that, you know, you've got to work on the civil liberties and the privacy offices, you know, when you're working with that social

media policy. But, you know, I think we can all agree we're behind. You know, I mean, social media has been out there for a while. We need to use that as a piece of our background investigation. It's just a matter of working with those civil liberties and protection offices to... I think that final hurdle to get that social media policy out. But we're working on that. The policy is going to just kind of tell, you know, agencies what they can and cannot do with social media. And it does also give a kind of (inaudible) to these different pilots that Director Cobert talked about before, these social media pilots that are out there. And, you know, and to kind of repeat, it's all about the whole person. So social media is one piece that, you know, can be used during the background investigation and the adjudication but, you know, you need to corroborate that. You need to use that as one piece. Continue to use adjudicative guidelines and the training that is involved in the background investigations. So, you know, anybody can take a picture of Gary Novotny, make a Gary Novotny Facebook page. You know, you need to be able to corroborate that and use that as one piece of the background investigation. So sorry I went over that quick but I know we're still on time. So... Am I good?

M: (inaudible) question?

M: OK.

M: Thank you.

NOVOTNY: Thank you.

CIRA: Is that it then for the working group? CAF? We still have CAF?

_: DoDCAF.

CIRA: Yeah.

_: We still have Dan Purtill.

PURTILL: (inaudible). I'm going to also be pretty quick. Good morning. Dan Purtill with the CAF. Most of you have seen these slides in one form or another in the past. Let me just go to the first slide there. Just showing our workload trends. CAF -- bottom-line with this is we're pretty healthy right now. We continue to trend in the positive direction, reducing our backlog we've had for several years and we're still hopeful that we'll see that completely gone sometime this calendar year. So we're catching up very well. We have a lot of unknowns coming up that are impactful to us. But like I said, we're pretty healthy. So I think we're posturing ourselves well to absorb those impacts, new FIS standards, CE implementation, things like that that will... But we're working very well with all our partners across the department, across the enterprise to prepare for those. So any question on

backlog at the CAF? I don't want to spend a lot of time since we're long. You, Sir?

M: Based on the slide can you talk about e-adjudication and what your process is as far as the tier threes?

PURTILL: Adjudication. Yeah, we are actually very close to -- I think to getting very -- to getting final approval on the e-adjudication implementation for the tier three. We are expecting that to be a matter of weeks to get that approval at this point. So far we've been able to absorb it. We haven't really had any real adjudications since the holidays basically. But it's not been hugely impactful. We're about -- we're losing about two adjudicators worth of work per month in efficiencies by that. So right now we're at about six or eight adjudicators basically if you want to look at it from a manpower perspective that we've lost. But it hasn't been huge to us. With the implementation of the tier three we are expecting a lower pass rate at the secret level but we are actually going to be looking at a broader range of people, because it's including not only the NACLAC but also the ANACI moving forward. So we're actually expecting it to be a bit of a wash for us moving forward. So it will be good when we get it but has not really hurt us too much.

M: Has the tier threes that are coming in -- you guys are at least trending upward as far as having to go to an adjudicator, taking longer to get done?

PURTILL: Yeah, we've seen a big shift. We're getting, frankly, next to no NACLACs in at this point and they're almost all tier threes coming in at the secret level, which is to be expected. That's the way that -- it's working through the system. But, yeah, all the tier three adjudications are manual at this point. Next slide. This just... This next slide just shows the ERPA compliance from the DoDCAF. And, again, we're looking pretty good. We've experienced some spikes in the past and we may continue to see a little bit of fluctuation but we're getting much more to a normal level, we think, as we work through that backlog. We don't really count a case until we finish it. So if there's an old case out there still, that's when we see the spikes in our [ERTPNA?] numbers. But bottom-line is, again, we're looking pretty good. Got the PRs finally back under the 30-day mandate there and we expect to stay there, although that's the one area where we might see a little bit of jumping around over the summer. But we don't expect it to be significant.

_: Sure.

PURTILL: So any questions on CAF workloads or anything else? Apparently everybody was waiting for me. Thank you.

F: We know time is short.

CIRA: OK. Let's go into the open forum part then.

F: Lunch is just a little later for everyone today. I spent a lot of time collecting my thoughts, probably eight to ten years, but really only the past week. So I don't want to miss any critical points on this point with JPAS access so I'm actually just going to read directly from this paper. Which, as I've come to need as of late, is in a nice 16-font, so it's not as bad as it looks, but I have to be able to see it. Obviously all of us here take very seriously the security of our nation's secrets and trust it to private industry. That's why the DoD and non-DoD agencies here today have worked so hard to establish effective industrial security programs and why the companies here today and across this nation have done the same. I take pride in the fact that the State Department has provided me with the resources to develop a robust industrial security program. After all, the State Department couldn't do our varied missions around the world without our contractors and they are critical to the protection of our classified information, the security of our domestic buildings, the secure design and construction of our embassies overseas,

and the security of the lives of our personnel and other agency personnel, to include scores of DoD, civilians, and military personnel, visiting or assigned to our missions abroad. Particularly in these difficult times it's even more critical that we all have the tools we need to ensure the security of each of our facilities, personnel, and information, and that we do so expeditiously. A huge part of all of our jobs is ensuring that contractor personnel have the requisite security clearances before they are afforded access to classified information or areas. That is why it is hard to understand why an agency like the State Department and the 30 other non-DoD agencies in the NISP are restricted from direct access to JPAS, the system of record for verifying security clearances in the NISP. All DoD components and the over 13,000 contractors in the NISP have JPAS access but the 31 non-DoD user agencies do not, except by exception. According to DMDC regulations, JPAS accounts for non-DoD agencies "are issued by exception due to the lack of insight into non-DoD subjects, employment, security clearances, or oversight." I truly do not understand this premise, especially as we follow the same national standards as DoD for processing clearances and hiring personnel. I have offered time and time again, as many in this room know, to provide whatever information

is needed to facilitate our access to JPAS. Two years ago I had all of my personnel take all of the training and follow all of the steps required in DMDC's JPAS account requests procedures manual. I even included the required full explanation as to why OPM CVS does not meet our operational needs. But according to DMDC at the time my request was not processed at the request of OUSDI, although we were issued a waiver at that time allowing us to continue to request JPAS person summaries from our contractors on an interim basis. As an agency which has taken very seriously its role as a user agency and a member of the NISPPAC and the GISWiG, I do not understand this restriction and have a difficult time in explaining to my deputy assistant secretary and assistant secretary why we are treated differently with regard to JPAS access and how that could have a direct impact on the security of our missions around the world. Given the issues that we have seen time and time again, as my staff has continued to review visit letters and JPAS person summaries from our contractors, we cannot go back to simply accepting the information contained on visit letters submitted by our companies. Somehow we have to continue to verify that the information provided by our companies is accurate, as my office is ultimately responsible for ensuring that each and

every contractor who walks through our front door, especially at our embassies and consuls abroad, have the requisite personnel security clearance. CVS, though I'm sure as designed could be a tool for personnel security professionals, verifying clearances on an intermittent basis, is not a useful tool for my industrial security professionals, as they work diligently to verify the clearance and investigations status of over 25,000 contractor personnel supporting the Department of State on a yearly basis. Though there have been some improvements to CVS over the past few years with the addition of cage codes, I'd ask OPM looking forward how CVS could be made more user friendly and less onerous so that if non-DoD agencies continue to be denied access to JPAS we can do our jobs more effectively and efficiently. Also, relying on CVS versus JPAS to verify the current status of contractor clearances will at least triple our processing times for the review and approval of visit letters, which will result in significant delays to both domestic and overseas contract performance for our contractors, especially when you consider that we must review over 2,000 visit letters per month. It will also equate to thousands of additional man-hours being expended as a direct result of our not having JPAS access. So my point today was to ask DoD if

there is any possible way that an exception can be granted and State Department industrial and personnel security professionals could be brought more in line with DoD and contractor security professionals and be granted access to JPAS. So I was happy when you mentioned it but this is a lot of years of frustration that I decided this would be the best venue to bring it up at. So I appreciate looking forward maybe I don't have to bring it to -- I'd rather talk directly with you all than have to go all the way up my chain to the undersecretary. But...

M: Yeah. Happy to have the conversation.

F: And I think there's other non-DoD agencies, if they're not here, that have the same issue. It's not -- might be as large an issue for them as it is -- has been for us. So I appreciate your time. I'm sorry for making lunch later but...

CIRA: Is there anybody else who wanted to bring something up? OK. We better wrap this up then. As you all know the next meeting is going to be Monday, June 6th, from 2:00 to 4:00 pm in the Gaylord Hotel in Nashville, Tennessee in conjunction with the annual NCMS seminar. And the NISPPAC will be on day one of the conference. So thanks again to everybody and hope to see you in Nashville.

M: Thank you.

CIRA: We are adjourned.

M: We're adjourned. Thank you.

END OF AUDIO FILE