

[START OF TRANSCRIPT]

Tania: Ladies and gentlemen, welcome and thank you for joining today's webinar, the NISPPAC meeting. Please note that all audience member lines on the phone will remain muted until the various Q&A portions of today's call. We will provide you with instructions on how you may ask a verbal question at that time.

You are welcome to submit written questions throughout the presentation and these will be addressed during Q&A. If you are connected on the web and would like to submit a written question, please locate the chat panel on the right side of your screen. Select all panelists from the send to drop down menu.

If you require technical assistance, you may send a private note to the event producer. With that, I'll turn the call over to the director of ISOO, Mr. Mark Bradley. Please go ahead.

Greg: Thank you. Good morning everyone, as you can see with the different venue that we had in the past. A couple of things, Mr. Bradley will give a lot of the administrative items. I would ask if you are a NISPPAC member, because we don't have a lot of microphones. We were aware of that, but the archives, believe it or not, this is what they had available.

These first two rows in the center perhaps we already have all the NISPPAC members that are present here. It's ironic, we did this because of safety concerns. On a day like this, a lot of folks are calling in, but who knew? I'll turn it back over to you now. Thank you.

Mark: I decided because the government is still open to go ahead and do it. Again, we apologize for putting anybody at risk. It wasn't our intent. What I will guarantee you is, we'll get you out here on time. With that, let's get started.

Let me just go through the usual administrative comments. Welcome to the 60th meeting of the NISPPAC. As you are aware, we've changed the venue for this meeting from the Archivist reception room of the McGown theaters. Greg said, we did that because of the fire codes. We were so popular that were running out of space.

Those of you who've been in the Archivist reception room, know it's a beautiful room, but it is compact. If we did have a crisis, it could be a real problem.

Move it here. It takes a bit to get used to. I feel like I'm either under the interrogation of the KGB or in Las Vegas. The lights are... I can just see orbs now. I'm not really looking at you. I'm looking at the light.

Anyway, we'd like to remind you, this is a public meeting. It is audio recorded. We are also using WebEx for the first time to expand our reach for enabling access to the meeting. You will notice this change throughout this meeting. Again, don't be taken back by it. This is an experiment for us too. We're trying to, again, expand our reach.

For those of you here in the room, please be mindful that we have people on the phone to teleconferencing capability. My guess is today, we have more than usual people on the phone. We need to be mindful of them.

There are three microphones in the first two rows for members use. Greg, if you identify where those are, those are handed out.

Greg: Yes. A few [0:03:27 inaudible] Carolina has one.

Mark: Okay, got it.

Greg: There's on the table. Dennis Arriaga has another one. We have a couple on the ends. We have some ISOO folks that will help out. If members that are not NISPPAC members in the audience have a question, you can either move over to the sides at the point where we ask for questions, or we'll try to get one of our ISOO folks to get a microphone to you.

Mark: Okay. All speakers must identify themselves before speaking. As you know, this is recorded and also transcribed. Again, in order to make a clear transcript to what this is, we need to know whose speaking. Again, please identify yourself. If I interrupt you again, it's not because I'm rude, it's because I'm trying to get an accurate transcript of who said what to whom and what the answers were.

The presenters will address a variety of topics today. At the end of each presentation, we will have a small question and answer session in which people may ask question as well as submit questions through WebEx.

The way it will work is after a speaker has completed their presentation, I will ask anyone in the audience, meaning those of you present in the room, if you have any questions. After answering those questions, I will then ask Tania Cianje, our WebEx moderator for this meeting, if any questions we're submitted to the WebEx chat function. If there are, Carolina Clink, of my staff, will read the

question so that everyone can hear it. Last, Tania will unmute the phone lines and ask if anyone calling in has a question. Please remember there will be a general question and answer session at the end of the meeting. I encourage you to take advantage of that.

Presenters other than those sitting here at table who don't have slides must use the podium at the front of the theater. Robert Tringali of my staff will assist those to use our presentations on the screen. Presenters will also have access to a remote where they can move the slides at their own leisure. Again, whatever you'll all prefer.

Some other additional administrative notes, we'll have a ten minute break during the middle of the meeting. The locations of the restrooms, when you exit the theater, they will on the left side once you enter the hall way, as is the Nara Café.

Also, for those with mobility issues, to my right, in front of the stage, there's a door that leads to an elevator which will transport you to the ground level. Regrettably, food and drink are not allowed in the theater, despite what you're seeing here in front of me.

Now, I'd like to welcome our newest NISPPAC members and express our appreciation for our outgoing members. First, I'd like to recognize Quinton Wilkes, who will now serve as our NISPPAC Industry spokesman. Quinton has served in NISPPAC in many capabilities for many years. He's proved himself to be more than up to this new challenge. We know that he will continue to make great contributions to the NISPPAC. We thank him for serving as the industry spokesman. Welcome, pleasure to have you.

We also have two new members from industry. First, it's a great pleasure to introduce Miss Rosael Borerro, who is the senior information security officer at Ensco, Inc. It's also a great pleasure to introduce Miss Sheryl Stone, who serves as a director of Corporate Security for the RAND Corporation. We are greatly looking forward to having you as members and sharing your thoughts and insights.

Our newest government members are Christine Gunning who I used to work with over at the Department of Justice. We welcome and thank you for your willingness to participate. Mike Scott, primary member of Department of Homeland Security. We welcome you and thank you for your willingness to participate.

Our outgoing members are Anna Harrison, primary member of the Department of Justice, now succeeded by Christine. Grateful for what Anna has done for us. Steve Lynch, Department of Homeland

Security. Thanks Steve. Heather McMahon, Department of Defense. We're grateful for her service. We have her here today as her **[0:07:27 inaudible]**. Wait, let's back up, that's not quite right.

Now, beginning with the table, I'd like each person to introduce him or herself, followed by the NISPPAC members in the first two rows. Next, remaining persons in the theater, last, we will go to the ones on the phone. For those calling in, they will receive a prompt from Tania, at that point, they will introduce themselves. This way, we will be able to provide people calling in and identifying themselves at the same time. Also, we would like to ask those on the phone to follow-up with the email of Robert Tringali at robert.tringali@nara.gov. Right.

Robert: To the introduction set-up.

Mark: Yes. I'm Mark Bradley, Chair of the NISPPAC.

Quinton: Quinton Wilkes.

Greg: Greg Pannoni, ISOO and the Designated Federal Official for the NISPPAC.

Valerie: Valerie Heil, Department of Defense.

Mark: Bobby, you want to start?

Male Speaker: I'll start right here. **[0:08:30 inaudible]**, NBIB.

Keith: Keith Minard, Defense Security Service.

Carolina: Carolina Klink, ISOO.

Bob: Bob Harney, NISPPAC.

George: George Ladner, CIA.

Dennis: Dennis Keith, NISPPAC.

Dennis: Dennis Arriaga, Industry.

Kim: Kim Baugher, State Department.

Christine: Christine Gunning, from the Department of Justice.

Roselle: Rosael Borerro, NISPPAC.

Kevin: Devin Casey, ISOO.

Glenn: Glenn Clay, Navy.

Fred: Fred Gortler, Defense Security Service.

Male Speaker: Excuse me Bob, **[0:09:09 inaudible]** could you grab the other microphone and...

Sheldon: Sheldon Soltis, NBIS.

Patrick: Patrick Hogan, DSS.

Cheryl: Cheryl Stone, NISPPAC.

Steve: Steve Demarco, DOD CAF.

Karl: Karl Hellman, DSS.

Steve: Steve Mapes, DSS.

Bob: Bob Lilje, Industry.

Lyla: Lyla **[0:09:34 inaudible]**, Industry.

Mark: Mark Riddle, ISOO.

Jim: Jim Ervin, DHS.

Mike: Mike Scott, DHS.

Justin: Justin Doubleday, Inside Defense.

Jane: Jane Dingle, Industry.

Sue: Sue Steinke, Industry.

Noel: Noel Matchett, Industry.

April: April Abbot, Industry.

Female Speaker: **[0:10:05 inaudible]**, Industry.

Jason: Jason Elder, DOD, USDI.

Donna: Donna McLeod, NBIB.

John: John Nicholson, NBIB.

BRyan: Bryan Macky, Industry.

Caroline: Caroline D'Amati, Clearance job.

Lisa: Lisa Reidy, Industry.

Dick: Dick River, Industry.

Jason: Jason Hager, Public Services in Vancouver, Canada.

Simon: **[0:10:41 inaudible]** Simon, DSS.

Chris: Chris Forrest, DSS.

Andrew: Andrew Parker, DSS.

John: John Massie, DSS.

Dennis: Dennis Newkin, DSS.

Amanda: Amanda McGlone, DOD.

Jason: Jason [0:10:59 inaudible], DSS.

Stanley: Stanley [0:11:02 Dave], NBIB.

Burk: Burk [0:11:08 Hamilton], CIA.

Tania: All the phone lines have been unmuted. If you're on the phone, can you please identify yourself and your agency? To our first caller, please go ahead and identify your line.

Carla: Carla Peters-Carr, Industry.

Dave: Dave [0:11:40 inaudible], Industry.

Ryan: Ryan Rainer, Industry.

Shirley: Shirley Brown, NSA.

Steven: Steven Cicirelli, Industry.

Tania: Catherine, please go ahead, your line is unmuted.

Catherine: Cathy Pherson, Industry.

Larry: Larry Piles, Defense Security Services.

Laura: Laura Aghdam, DSS.

Allison: Allison Rentzhaler, DSS.

Rick: Rick Ohlmacher, Industry.

Tania: Sharon, please go ahead, your line's unmuted.

Sharon: Sharon Dondlinger, Air Force.

Jennifer: Jennifer Skelton, Air Force.

Tania: To the other speakers on the call, please go ahead. Your line is unmuted. Olga, please go ahead. Your line is unmuted.

Olga: Olga Delgado, ODNI.

Tania: Patricia, please go ahead.

Patricia: Tricia Stokes, DSS.

Tania: Ryan, please go ahead.

Ryan: Ryan Deloney, Defense Security Service.

Sandy: Sandy Langley, DMDC Supporting Desk.

Tania: Finally, Valerie, please go ahead.

Valerie: Valerie Kerben, ODNI.

Tania: All phone lines have been identified.

Male Speaker: Does Tania have anything else?

Tania: All right. I'm just confirming that all lines have been identified.

Mark: **[0:15:09 inaudible]** not delayed then. Greg Pannoni now will address administrative items. We'll cover the status and action items since July 19, 2018 NISPPAC meeting. Greg?

Greg: Thank you Mr. Chair. I'm not going to look up as much either because these lights are tough. All the presentations and handouts were sent electronically to all the members and to those who provided in our RSVP, to the invitation for the meeting. If you didn't receive any of these documents, all the materials along with the final minutes and the official transcript of the meeting will be posted on the ISOO NISPPAC website within approximately 30 days.

Also, for your information, NISPPAC meeting announcements are posted on the federal register, approximately 30 days prior to the meeting.

I'm going to move in to the action items. Read off the action items from our last meeting that was July 19th. The first was involving Industry meeting with DSS. To see if they can get more clarity to some of the consultant and security services that continue to support small businesses. While there has been some informal discussion, the meeting between DSS and Industry is still pending.

Next, was the DSS and ISOO to discuss the directors and secretaries of federal executive branch agencies responsible to implement CUI. We, ISOO and DSS did have a meeting regarding the terms and what will be DSS' role in overseeing the implementation of the CUI program for the defense industrial base did on behalf of DOD. Yesterday, DSS has a draft plan that is very close to finalization.

Next, NBIB was to provide information on companies that are going to participate in a pilot program. To put some context on this if you

were here, you may recall from the last meeting this concern leveraging Industry as a trusted information provider or tip as appropriate. Some companies already have gathered vetting type information on their new employees, which may supplement the government's vetting program. Part of what is being considered is to establish base lines from what information is generally already being gathered by industry. Mr. Fallon, I believe a little bit of this with his presentation update.

Next, insider threat working group was to meet before the next NISPPAC meeting. ISOO is also involved with that with Paul, NISPPAC members to discuss ways to improve the insider threat programs. We did have that meeting on October 30th. It was a good meeting, productive. While ISOO did informally call members, some informal discussions at the meeting regarding program improvement were discussed. I will be providing an update on the insider threat working group meeting later in this meeting.

Next, Industry requested a debrief from ISOO on the meeting held with the CSAs and other government activities on the processing of leads. Due to business exigencies, the meeting was not held, but we will be doing that sometime in the next few months.

Next, ISOO inquired about what the obstacle to obtaining sponsorship for eMASS training, and who is the authority of sponsorship. I believe, today, some of these was discussed as well. DSS stated that if an Industry partner is unable to access the eMASS training site, after being sponsored for access by their local ISSP, they should report this to DSS at the following email address, dss.quantico.dss.mdx.emass@mail.new. More detail on this will be addressed later during the NISA working group update that Karl Hellman will give.

Next, lead us to the last one. This one, the wording and the minutes is actually not quite right. This was about why some companies have been receiving notices that disestablishes their ATOs authorizations to operate. DSS stated that denial of authorization to operate letters are used, IBSS to inform Industry of the removal of the ability to operate. These letters are produced for variety of reasons as you may know, could be expiration of the ATO, increased risk, declassified information not previously known, change of security steps, security violations, unable to meet MIST or MS standards and others. Each DATO is an independent decision associated with the specific [0:20:12 inaudible]. That's a readout on the old action items. Are there any questions? Questions back to you Mr. Chair.

Mark: All right. Go to our reports and updates section of our program. The post here from National Background Investigation's head, Charlie Phalen. Charlie, please come up.

Charlie: Good morning. Hopefully, you all can hear me here. Now, I understand what you mean about the lights. I seem to recall earlier in my career, I would have been in the other side of those lights. Anyway, we'll do it again here. Thanks for the few minutes to share with you all this morning.

I went back and looked at what I had said when I was here with you all back in the spring. I want to get a sense of what promises I had made and how far had we come to some of those things. One of the sense of what I said is based on our inventory in the spring. One of the things that we were doing, I had predicted that by thanksgiving, we'd had about 15% in our inventory.

I'll give you a lot more of numbers in a minute here, but as of Monday, we are down 13%. Give it two more weeks, after Thanksgiving, I hope to be able to tell you that 15% is actually accurate.

In other news, I mean that in all senses of it, there had been some media reports that had gone both into the spectrum here. There was a couple of reports out last week that suggested that my inventory was extra ordinarily high much higher than it really is. At the same time, there was an article, that reflected that the principal deputy director in National Intelligence had predicted that I will have an extra ordinarily low inventory by the spring time of [0:22:11 inaudible]. I got a lot of people telling you what they would hope that I would do or what their numbers look like.

Let me give you a real sense of what these numbers look like here. As of Monday, the reality is that our total inventory of investigations sits at about 630,000. That is, as I said before, 13%, almost a 100,000 less than it was in the spring time.

I think more importantly for this organization, in particular for this discussion is, in that population, how many of these folks are waiting an initial clearance or in other words, may or may not be able to work in it.

Let me give you some breakdown in those numbers. In the two or three population, the secret clearance population, the total number in our inventory of initials is 190,000 of that number; 35,000 are in Industry.

Taking you to the next level, the tier five investigations, we are showing 90,000 in our inventory. [0:23:11 inaudible] initials, not for investigation's initials at 90,000 and about 25,000 of those are in Industry right now. You'd add all those numbers up, that's about 280,000 initial investigations that we're processing right now. Some part of that continues, but that is not 280,000 people that are not working. Based on the numbers we have at a minimum, about 114,000 of that 280,000.

We don't have inside to do every agency's interim clearance process, but that are the ones we can document. 114,000 of that 280,000 are at work on an interim clearance. That's not as bad a number as some other been out there, still not what we wanted to be, but it's not [0:23:56 inaudible]. Specifically, the Industry inventory itself, we can show itself down by 13% since just in June, based on some things I'll talk about in a few minutes here.

The other piece of these things which really is, the root here is timeliness, how long does it take to do clearances. I see behind me there is some numbers here that looking extra ordinarily unhappy. I am unhappy with the numbers as well there.

Two facts that I see here that may help a little bit. One is, that what we are seeing in the range of those times for clearances. We don't count them until they're actually finished. What we are seeing is, is what we sparsely narrow range it. Everything is coming in late. We're seeing a lot of stuff coming sooner, but at the same time, we're closing a lot of old stuff. The average has come out still about the same. I expect that as we get moving down, this inventory number that those times in these numbers will go down.

A leading indicator of this is in [0:24:54 inaudible] number that we use in our queue, our production in information. It's called field men hours. I wouldn't worry too much about what that defines. It essentially tells us how much field work is sitting out in our inventory. Field work, you guys know is the longest [0:25:09 inaudible] investigations.

That number is down about 35% since last spring. That's a good leading indicator of what we think these numbers are going to going here. Stay tuned, I hope to be able to come with our next session which is January, maybe and give you some better numbers here.

Male Speaker:

On March.

Charlie:

March, okay. I should bet some really good numbers by then. Okay. What's getting us there, I patched this out before, but really quickly

here, we rebuilt our investigative capacity. We're up to 8800 people that are doing field investigations for us right now, in addition to all the other folks that are working [0:25:46 inaudible].

That population has gained experience over the last six months. More importantly, we have put on top of that, a lot of our business process with engineering things, which are using these investigators far more effectively than we had been in the past.

I'm just going to touch on one here that you are probably familiar with this, our work on [0:26:07 inaudible] that is putting our investigators in having situations geographically so that we asked some of your companies have volunteered to be the footprint for us.

We did this with the government a few times. The government's organizations, whether it was Department of Energy, the Air Force, the Navy, Department of Defense at large and some other organizations. It's worked out pretty well. Our first two hubs with industry which were court pilots were going main stream with this stuff now. We pick a geographic location, one of you has hosted us, but every company in the area is welcome to come. Allow us to spend less time administratively, while the people we are doing the investigations on and the reference has come and talk to us.

In addition, we've given these folks some technology that we had if you guys are security officers, you know we're scared to death within like DTCs. Mark is using this stuff and using it under secure manner and extending our reach considerably here. That's all helping. Again, when we go to these hubs, all companies in the area are invited and we'll make sure that we are working on that stuff.

The couple of the cases, I think either Valerie or Olga, may talk about this when they get to the DNI stuff, but we are working on trusted works or the key elements of trusted workforce 2.0, which is rewriting the policies that are driving how we do investigations.

This is really picking up steam. On the last three weeks, we had an off of lot of energy into this thing from the Executive Steering Group. We've been working off some of the early decisions from this and that has also helped with our inventory reduction. All this stuff working together has been helpful.

Greg mentioned, the trusted information provide a program, it's a no brainer that I know a lot of you in the pre-employment portion of bringing people on board are gathering information that we can use later in the investigation. There's no point in us going back at and

recollecting that information, if we can trust that you have gotten it from a reliable source.

We've been working with a number of your companies, in a working group situation [0:28:07 inaudible]. We have put together a draft of how this would work. A lot of that comes from information provided by you. I have seen and know there's enthusiasm within our security executive agents to both the suitability and security executive agents, I'm sorry, to both for changing the policy and allowing us to broaden this out considerably. The front into this is doing some piloting work. We've got a lot of enthusiasm for that to [0:28:32 inaudible] and vision. This will come main stream pretty quick. I'm pretty happy about that.

Last topic here is changing T-shirts. Last spring, Michelle Sutphin said, after I talked about some of the things we're doing, "Are you going to share all these cool things that you are doing with the Defense Security Service when they do the 70/30 split?" The answer then, was yes. The answer today is even better it's, we will be the [0:28:56 inaudible] in some period of time. I guess we'll be sharing with ourselves.

Just a quick highlight here, back in June, the administration publishes the president's management agenda about the understanding that made notions to cut up the investigative organizations and the pieces but to keep it in tact. Move it from the office of personal management into the Department of Defense. That is still the plan.

We're waiting for the executive order. It will be imminent. I've been saying that for several months, but it will be coming out imminently. I've seen the last draft literally yesterday evening. We'll be able to close on this. It will start with that executive order.

Once that happen, we will work in earnest to get through that change of venue. That said, we've been working very close with the Department of Defense easily since last December, on some version of the transition. I would say the level of effort in engagement is both high and strong and pretty collegial given the fact that all the stresses and pressures that come into this stuff.

We really are working at this as we are... will be one team. I hate speed bumps. We're narrowing those down as much as [0:30:12 inaudible]. With that, we'll go to any questions? I should see a hand go up, that would be exciting. Yes sir?

Dennis: Dennis Keith, NISPPAC. The decrease in the number of field work hours, is there any correlation there between that and the increased use of CE (Continuous Evaluation)?

Charlie: Not yet. We didn't go to a lot of details about using continuous evaluation to supplement some of the periodically investigations that the department is working on it. The total number of investigations affected by that right now, is maybe ten **[0:30:56 inaudible]**. Those are avoidance at this point not taking things out of the inventory, things that were not put in to the inventory.

That said, because everybody is active out there, we are seeing consistently in the last few months a higher level of new work coming in than this time last year. We're actually working against a higher level of incoming cases. Still, we're making some good headway against it.

I expect in the long run a lot more wide use of continuous evaluation in as part of a periodical investigation program will have a much more dramatic impact. **[0:31:41 inaudible]** get a microphone.

Mark: Give the microphone.

Caroline: Caroline D'Amati, Clearance jobs. I was wondering though if the number that Hugh Gordon gave from ODNI, by the springtime, the number would be around 300,000. What would you say might be a more accurate estimation?

Charlie: I would say, probably, closer to 500,000; but I'm pretty conservative. I said 15% last year. Let's see what happens. Again, the key things that I really need to make promises about is, what will the time when this look like? I'm hoping that time when this is dramatically improved.

Mark: Questions for Charlie in the audience?

Carolina: I do not. However, some people joined after the attendance list. I'm going to list some really quick. We have Carla Peters-Carr; David **[0:32:43 inaudible]**, Dennis Bradley, Lindy Kaiser, Steven Cicerelli, Katie Timons, Diane Rainer, Jen Kirby, Leonard Moss.

Mark: Thank you. Anyone on the phone have a question for Charlie?

Tania: If anyone on the phone would like to ask a question, please press #2 on your telephone keypad at this time. We do have a few questions. Our first caller, your line is unmuted.

Leonard: Hi. This is Leonard Moss. I just have a question for Charlie on the hubs. Charlie, is there somewhere where you list those hubs, so if someone wanted to participate, they would know where to go?

Charlie: I don't really publish that list in the sense of putting out in the open, but where we set up a hub, I believe and I will ensure that we are reaching out to all the industries that have the locations within that hub area. All the companies that have locations in that area.

Leonard: Great, thanks.

Tania: Our next caller, please go ahead, your line is unmuted.

Lindy: Hey, this is Lindy Kaiser at clearance jobs. To Charlie, you're talking about me and I'm also reporting on your numbers. Why is the disparity between what you said today and what was in the secret act report that I got?

Charlie: Your voice is coming through kind of broken-up by I assume this is Lindy Kaiser?

Lindy: It's Lindy Kaiser, your number one fan. I'm wondering about the disparity with the numbers. You need to follow up with me later because I want to make sure I get them right because I'm interested in the number that you reported today, but they're different than what was listed in the secret act report.

Charlie: Lindy, I appreciate that. I went back and read the secret act report again as well. There's two things about this numbers. One is, they're numbers from June or July, I'm sorry, and not numbers from today. The numbers are different anyway from today.

The problem with that report is the way we were asked the questions by the legislation that said, "Please do this report," caused us to write the answers the way you see them in the secret act, but not all those numbers are discreet. There are some crosschecking that goes on where you can get counted [0:35:12 inaudible] information in that report.

We actually have come do very soon. The quarter we'll report on that. We're going to put a big caveat on that that says if it talks about the math problem with this. Because if you just look at it and add it up, you get a really high number. These are crosscutting in different ways, slicing in different ways. Again, the numbers that I talked today are the accurate numbers. We're going to actually suggest to find a different way to [0:35:44 inaudible] way that it's much more manageable. Lindy, we'll get back to you more directly and we can talk about that.

Lindy: Awesome. Thank you.

Mark: [0:35:54 inaudible] Charlie [0:35:55 inaudible] other call?

Charlie: Okay.

Tania: No further questions on the call.

Carolina: I just got a comment. I would talk to the speakers can speak louder to the microphone because the sound is faint.

Female Speaker 1: We just got an email from NASA. [0:36:16 inaudible] has been on in that, get off and turn to get back on. Is there some issue with getting back on?

Male Speaker: That one please.

Mark: Let's not hold up the meeting [0:36:33 crosstalk] let's go on.

Female Speaker 1: NASA's still trying to get back on.

Mark: What do you think Charlie?

Charlie: Okay, thanks. I'll be here all day, or at least until noon.

Mark: Okay. Thank you.

Charlie: Thanks.

Mark: Yes, you have the right. Right, we'll next going to here from Ryan Deloney, from DSS. He'll tell us about the National Industrial Security System and Employment of the NISP.

Ryan: Good Morning, this is Ryan Deloney. Can you guys hear me okay?

Mark: Go ahead, Ryan.

Tania: Ryan, your audio is coming through clearly.

Ryan: Okay, great. I just hold the plug, go for it. Great, thank you very much. Now, I wanted to give an update on the National Industrial Security System. We've had great progress on the NISP effort since last time this group met. I want to note that NISP did successfully deploy on the eight of October for industry and government users. I want to note that it is the system of records for DSS Industrial Security Oversight, those for the Department of Defense and those non-DOD signatories engaged with the DOD. ISFD and EFCL are two legacy systems that it replaced. Those are no longer available. NISP is the system of record to use going forward. You can see some activity notes on there.

Following yesterday's meeting with Industry, I went back and pulled some updated numbers. I'm happy to share those as well. As of yesterday, we are sitting closer to 6,500 users, of which there are about 5000 unique industry users, 800 government users, and still about 600 DSS users. Questions came up about how many companies that represents. I identified that that represents actually about 5,500 unique cage codes. There you'll see with that number actually bigger than the industry users. There are some users who do represent multiple cage codes either within their corporate family or there may be a multi facility at that zone.

Testing have been used currently over actually 13,000 clearance verification submitted so a high volume of processing there which is a good thing. There has been over 400 facility clearance sponsorship submitted. If you are either a government sponsoring an initial or a prime industry partners sponsoring this hub, this is the system you **[0:39:04 inaudible]** at.

We've seen a lot of benefits which produce rejection rates. Prior with our very manual process, you would see just for the paper forms submitted by email, missing documentation and issues that would cause a lag in the initiation of the FBL processing. The smart form and the system is reducing that. Ensuring that we have a package that has everything we need upfront, which has been beneficial.

Then, there were 500 conditions reported. Industry have been actually using that as required. User feedback has been a lot of feedback. I will say that. We received over 1000 comments either to our mail box, which you can see in the bottom right corner on this slide, as well as directly in system. You can provide that messaging.

We've really seen three main areas. One is poking for more training, or having questions, or needing education. We've been gathering that up. As those most common questions arise, we've been developing job aid, which we've been sticking directly in systems. On the screen here, you can see a staple dashboard forward where in that top area, there's the blue links to common functions, questions. We've been deriving tool tips, things of that nature.

We're also continuing to build and develop job aids based on user feedback. There had been many requests for enhancement, which is a good thing. I'll talk about how we're going to rack and stock and engage with industry and government to prioritize those on the next chart in a moment.

We have been receiving some bugs. On the initial deployment month for a major system like this, that was expected. The development team was in place mitigated over 30 critical issues upfront. Most of those same day and a lot of those again, came from that feedback.

Our initial triage of the feedback was trying to see if any trends and issues that need to be immediately resolved and that's been worked down where we're seeing pretty steady system used.

Looking forward on the training front, there is training available in step. The DSS education North Pole, if you go there, there is external training that is broken by user role. If you are a sponsor, clearance verifier on an industry security staff, you can just take those modules unique to you. They'll give you everything you need.

In addition, as I mentioned already to the in-system short in job aid, those are available as well. Also, on the screen here on the bottom right corner, our external webpage, dss.new/is/nispstudyhtml. We're maintaining that with latest information, FAQ's and resources just to keep pushing that education content available. Next slide.

Turned up there's late **[0:42:03 inaudible]** here. I haven't seen this slide push forward on my end, but I'll keep going just for the interest of time.

Key capabilities, industry and government, we did deliver, as I mentioned, this is where you can submit and track your facility clearance request. That's been beneficial. You can see, is it under review at our facility clearance branch? Is out with Industry to submit the facility clearance package? That's very beneficial. If you are the sponsor, either at a prime or government agency, one of the things that can get your people cleared and working fastest is, if you see that the company is still waiting, tending to submit their required facility clearance documentation, the sooner that is submitted accurately, the sooner we can initiate all the other activities, the FOCI assessment, clearance initiation as required on five surveys in order to get that company up and running so that's beneficial.

Clearance verification has been going really well. We've been seeing a lot of positive feedback on that. The system is much more proactive. It's been easier form to submit those. As mentioned, well over 10,000 of those have been submitted. That just goes to speak to that note as well.

In those automated notifications, be it whether you're involved in the clearance process. Once your facility is cleared at the interim or final level, the sponsoring company do get emails, updates on that information, as well as at the clearance verifications running. If there are changes, you'll get an email along those lines.

Industry, this is where they submit their facility clearance documentation as reference changed conditions required annual self-inspection certifications. They also have more transparency into the information in order to view their facility profile DSS content available that we can maintain the record on those companies making sure that that it's transparent.

Where we're going in FY19, we will be using this for the PSI projection survey that was prior done in EFCL, but with the system replacing that. That capability will be deployed out sometime early 2019. We are looking to update the system to further allow industry to provide updates for their profile and vulnerability mitigation. Again, getting off our current email process, as there any issues, or information request, all those are just handled in the system streamline and ensure accuracy.

We'll also be looking at the DSSs transition, related functions. Some of those are currently done by out of system email and other capability spreadsheet. We want to automate in streamline as much of that as possible to improve it for everybody.

We are looking at how we can enhance system reporting be it suspicious contact reports or security violations, both to receive better information upfront about the who, where, when, why of those types of incidents. As well as be able to report more timely and rapid information, both of the company and the data owner in the government. We're working on building those out in FY19 as well.

Key point as well, we're working to establish a myth operational requirements committee. As I mentioned, we are receiving a lot of feedback for enhancements. We've been doing some initial triage of that, but what we're really looking to do is gather participants from Industry, from government, from DSS to take a look at that backlog, rack, stack and prioritize as a community and then start delivering upon those capabilities. Which initial development within agile methodology starting out in FY early calendar year, sometime in late January is when we're looking to get that going.

We're currently finalizing that process. We'll be looking to gather participants in the month of December, to then start those meetings

to prioritize in January. We look forward to participation leveraging NCMS, NISPPAC and government stakeholder's groups. We're leveraging those types of vehicles to gather participants for that organization.

With that, that does run through the big summary. Some other questions that came up yesterday, that I'll just go on ahead and jump ahead of. As far as, if there are any access issues. You do access the system through EnCase, which is a separate application that DSS host. It's a single sign on portal.

If you're having any issues accessing that, call our call center. Which is available, their number is on the EnCase webpage. They have a full OCIO trained team to provide that support for access. If there are any broader agency level access issues, I know we've been working a couple issues with non-DOD signatories ensuring that their certificates can work with EnCase.

We do have a process to escalate those up to direct to the EnCase PM. If there are any issues there, feel free to send an email to dss.net [0:47:15 inaudible] work escalates and make sure those get result for the more systemic issues. If it's just one off individual, our knowledge center's been providing great support.

As far as turnaround time for accounts, the government side of the house should be quite rapid. Those goes to our knowledge center, which other folk team reviewing. Those should be within a few days. On the industry side of the house, as mentioned yesterday, those do go to industrial security representatives. That can be the same day or if your industry represent that maybe out in assessment or something like that, may take a couple of days. Always recommend... you can send an email to your rep when you do submit that. Just letting them know that that's in their queue, just to help remind in prompt. Then, we can get that worked as well.

The main technical issue we've seen currently that we're working is, there's some system latency. We've seen as people submit their sponsorship, SCO packages, etcetera may spend for a little while. That is our top priority to working fixed right now. We have dedicated team's really working full bore on that. We have an enhancement for that coming out. We're testing that at the end of the month for deployment in mid-December. You should see much improvement on that front.

With that, I think that covered a lot of the questions that came up, but I would be glad to take any additional questions on NISP, that the group may have today.

Mark: [0:48:40 inaudible] in to the [0:48:41 inaudible] or anybody in the WebEx?

Carolina: No, but we found the issue of [0:48:51 NASA] she's on the line, Diane Taylor.

Tania: If anyone on the phone would like to ask a question, please press #2 at this time. There are no questions on the phone.

Mark: Okay, lovely. Thank you, Ryan. We appreciate it.

Ryan: Sure. Thank you.

Mark: We're going to hear from Sandra Langley, from DMDC, who will now provide us with an update on the Deployment of the Defense Information Systems for Security. Sandra is calling in. Sandra, are you on the line?

Sandra: Yes, I am. Thank you very much.

Mark: Great. It's all yours.

Sandra: Thank you.

Mark: Welcome.

Sandra: I want to provide an update of where we are, with the deployment of DISS to industry. Give you some information on user provisioning and ask for assistance in continuing the efforts for user provisioning. Then, to remind you that, we'll continue to be in need for access to both JPAS and DISS as we go through a state's deployment approach.

As of October, we completed building DISS phase one which means, from an industry perspective, industry users are being provisioned and DISS for use of DISS. At this time, we have actively provisioned just over 5000 users. Just over 5000 users were auto provisioned. We are reaching out to those that were not auto-provisioned but within JPAS have an active account manager.

We have contacted all, but 8% of those users. The 8%, we're still trying to find email addresses, so that we can complete this effort. Just on they are 2000, have been recently contacted and provided directions on how to submit the PSSAR, the DD2962 for user provisioning.

I must advice that we are encountering a large rejection rate. Only approximately one third of those packages are approved. Request that users read the directions that are provide with them, yet they

very detailed lay those out of the PSSAR. What to do and to submit those training certificates required for user provisioning. DSS will put this information out also for industry. During a second campaign trying to assist in getting responses for user provisioning.

We also have this large group of security management offices that did not have an active account manager in JPAS. Therefore, we're working with DSS on a campaign to contact those security management offices to forward users for provisioning and to DISS in such a rate that we can effectively process those requests.

I'm sure that DSS will provide more information as we continue our discussions today, but just wanting to advice that we really need assistance in making sure when we send out a campaign requesting user provisioning. Instructions are thoroughly read. If there's any questions to ask them upfront so that the package will be successfully submitted and provisioned the first time versus the package going through multiple iterations.

In DISS today, DISS phase one is all about communication it allows to security management office to communicate with DSS, industry group for subject management, making into a higher within DISS. You can do a higher in DISS management. Meaning, you can define your hierarchy. Same, we'll have to continue to do that in both DISS and JPAS. Manage your security management office. You'll have to maintain the security management office in both DISS and JPAS and user provisioning. You have to make sure that users are provisioned correctly and maintain their access to both systems. We look forward to working with DSS to do an incremental phase transition, from JPAS capabilities to DISS.

Currently, within DISS can claim the subject make sure that they're associated with the security management office, other updates, foreign relatives, foreign travel, and establish owning and servicing relationships. Also, communicating with the industry team.

You can't [0:54:01 inaudible] management officers can submit customer service request. There are multiple customer service requests that they can submit for communications with the industry team. Beyond that, there's still a need to continue to use JPAS.

DSS will provide information as we transition capabilities. Provide information on continuing use of E-QIP, or when that will change, incident management is one of the first things that we would like to transition from JPAS to DISS. More information will come out from DSS.

When we're ready to do that, we're not ready to do that immediately because we're looking down range on interphases and how we share any information across the department. As we have finalized our strategy in our plan for transitions, more information will come from DSS. Until then, I understand that this ad is a pain point, but there will be a need to continue to access both JPAS and DISS for the foreseeable future. Any questions for me?

Mark: Questions for Sandra?

Kim: This is Kim Baugher from the State Department. I'd like to know, is there any plan in the future, at any point in time that you're going to brief regarding government access to DISS for non-DOD agencies and [0:55:34 inaudible] in DISS, because you only mentioned contractors at this point. That was the last time through that DMDC they didn't really address this either at the last meeting.

Sandra: Okay. DISS and JPAS are still limiting who will gain access to the systems. Based upon our current processes in the system of record notice, we did support the access to the system, however, predominate use for non-DOD agencies still screw the SRI Bridge with CBS.

Now, you will hear Sheldon talking about our transition of DISS into the NDISS construct. He may talk more about when we will add additional federal adopters and when additional federal adopters will gain access because of NDISS initiatives.

I do look forward to continuing to partner with NDISS on the way forward for additional federal adopters. I do appreciate the State Department has requested access to the system and we continue to work with you offline.

Kim: I know I'm in the State Department, but really, I feel like I'm the spokesperson for non-DOD agencies. There's a lot of our agencies that when we have meetings addressed sustained, have the same concerns that they've not really been included in this. It's just not me, it's a lot of other agencies as well.

Sandra: I do appreciate that. That's why I believe there's going to be more conversations under the NDISS construct and DISS will be one of many systems. One of three system currently supported by DMDC, that will transition to the end of construct. We will be following their lead for federal adopters.

I do expect that Sheldon will speak about federal adopters. I can tell you that we are working currently right now with Social Security administration for federal adoptions. They recently published an

article in the federal register. They're identifying that our system will be used for adjudicative management. We'll be working with them.

I also expect that Sheldon will talk about the [0:57:55 inaudible] that is currently published and how that will support federal adopters in the future.

Mark: Okay. Thank you. Anyone else who have questions?

Male Speaker: Do you want to say that?

Mark: Yes sir? [0:58:10 crosstalk].

Quinton: Sandra, this is Quinton. Is it possible that you could set up a meeting in the future through the ISOO office so that you can collaborate with all of those non-DOD agencies?

Sandra: The answer is yes. There is a campaign underway by DSS for us to be reaching out to our federal partners, to have discussions on shared services and what they would like to take advantage of and getting to know the community better. Yes, we are doing that. I am just one of many partners in that campaign.

Greg: This is Greg Pannoni, from ISOO. I think that is a positive, but I'm not clear as to who takes to lead then on establishing such at least a--

Tricia: Hey Greg, this is Tricia. Can I give you a phone line... can I get in, please?

Greg: Sure. I don't know who this, go ahead.

Tricia: I'm sorry. Am I live on the phone?

Greg: Yes.

Tricia: Great. This is Tricia Stokes, from Director's Defense Vetting Directorate, DSS. We will be assuming the national background investigation mission, as soon as that great executive order is signed. To answer the questions in the room, the answer is, we are the functional requirements lead. Therefore, all of these questions, whether be the one that Quinton answered, whether it be the Department of State, should be coming through the Defense Vetting Office Enterprise Business office that I will brief on in a few minutes here. I can give the points of contact. It can be provided to Robert in a minute for this meeting, so you know who to contact for all of these questions. We shouldn't be going through DMDC, we shouldn't be going through the National Background Investigation system, or the IT provider. We should be going through the business office and that is the Defense Vetting Directorate.

Greg: Thank you, Tricia for the clarification.

Mark: Any other questions? Carolina, is there anyone on the web? **[1:00:16 inaudible]** for her?

Carolina: There are no chat on the web.

Mark: Okay, how about on the phones?

Carolina: If anyone on the phone would like to ask a question, please press #2 at this time. No questions on the phone.

Mark: Okay, thank you so much Sandra.

Sandra: Thank you.

Mark: Next, we'll just going to hear from--

Robert: Excuse me. Mr. Chair, I've been asked to specifically appear that we speak a little louder into the microphone. We're getting some response from those that who are on the line with the WebEx they can't hear.

Mark: Sure enough. I'll put the podium as well Robert.

Robert: Yes. Work on it.

Mark: Okay. Our Next speaker will Shelton Saltis, who will give us an update on the National Background Investigation System.

Shelton: I'm Shelton Soltis **[1:01:13 inaudible]** and I work in the NBIS in PMO PEO. Thanks to Tricia for answering the questions that was raised about where to go for the information about access. As she pointed out, we're providing the IT, not making policy decisions about who get access or requirement per se.

Little background about NBIS; the NBIS was stood up about two years ago to replace the NBIB legacy BI systems. As Sandy pointed out, we are sited about two years ago to use some of the DMDC systems that we're currently use for vetting inside DOD to give us a jumpstart, moving forward. Those systems are swift **[1:01:54 Mirror door]** and DISF.

If you look at slide, these are the term pipelines we currently have so you might be familiar with position destinations, the PDT, that NBIB, OPMS deployed. We also have what we called E-application subject, which is better known as EAPP, which is a replacement for the SF 86.

We have another application that we're calling NBIS agency that pairs with that or a replacement for EQIP. Investigation management that will be replacing the current investigation system of that [1:02:25 inaudible] I'll call tips. We're moving away from case centric to person centric. We're calling investigation management versus case management.

Then we have finger prints system. As I said, with DISS, the primary duty system we're adopting for that. One of the big things we are doing is on the record checks. Mirror Door is our current system for that we're enhancing that and moving that into the [1:02:49 inaudible] of NBIS.

Adjudication, that's currently located in DISS. That includes adjudication as well as continuous evaluation which is another portion of the Mirror door that we have adopted.

NBIS is a little bit different than most DOD applications. We are part of the agile project inside DOD. We are pilots. We're are designated. We did that for a couple of reasons. One, we want to use agile methodology to do the development for NBIS. We didn't feel that the current state of affairs inside the government with the DDI program, transition, transfer that a lot of form methodology would work well.

As we ever done waterfall to spend 18 to two years getting the requirements to the system this large, hand it to the developer and then the developer gives you something about three years later. Then, the users tell you, you basically built the wrong thing.

We also use an OTA to get us on contract as soon as we could, as part of the agile actions and strategy that we are using. That explains why we went agile and why we went with the OTA.

The channels we face, as I said, we have a very mobile and changing environment. We have TW2.0 coming out. We have the transfer, the transitions, a lot of movable parts. This is a federal system also, it's not just the DOD system which makes it more complex. We have to meet multiple stakeholders and multiple requirements so that we can meet the requirements for the entire government not just DOD.

We also have a very large project currently we chose [1:04:27 inaudible] for our agile methodology. We have 10 teams working on the IM portion of it. We have a team working on the front end of EAPP and what we call NBIS agency. We also have a team working on PDP. We have come up with a way to manage that across the

entire spectrum of all those teams. We chose a scale that will framework to meet that requirement.

As I said, agile is a methodology that produce software faster and direct to the users need versus building to documentation. We're really focusing in providing value to the owner. Making sure that we can change and we morph if we need to meet those requirements.

This is a comparison of the traditional practices of agile to waterfall or the methods. As you see, traditional practices makes to be predictable. You have post schedule performance. That's the iron triangle that most program managers will talk about. You can have two to three, you can have three to three agile. Try to make that a little bit by making trade out about functionality and stop the focus of agile. It's providing business value. This gave us stability to do what we need to do, to get NBIS where we need to go. We also have a very aggressive schedule, which another reason why we need agile.

This is the full safe. This is how to save construct works, to manage across workable teams. I'm not going to go to a lot of detail about it. It looks more complex than it is, because really, if you go up from the bottom, it's basically replicating what's in the bottom, but at a higher level. There's more inputs from the entire stakeholder as you go up and more over sight by the management team inside, the PEO PMO.

The basis is scam at the bottom where we're doing it. We make sure the scam teams have users and experts in place, so we can get what I consider real end user input requirements versus getting supervisors and/or higher level of deciding how things done versus how it's really done in the field or in the workplace.

We have program recommends every quarter, we decide what were the next thing that's going to be and how are we going to build that out. We meet with our stakeholders and our requirements. Just so you know, right now, we've been focused primarily on the IM capability. Also, what I call, in DIS agency, which is the replacement for the agency portion that used to initiate clearances inside the investigation process. That's the people we've been talking to, to get those requirements.

The other thing we did was. DISSs is to change with [1:07:14 **inaudible**]. We're going to what we call the DevOps or in our case dev set-ups. It's integration of the development security and operation environment. We can deploy to releases directly into the system and it moves to an automated process what we call,

pipelines to produce the software code that we need. We can pull it and get immediate feedback from the end user.

We had the set-up in the environment. We're moving forward into going into the problem primary with it. I'll talk about that a little more later, but this is important for us to be able to meet our schedule and to meet the requirements. Changes that we get based on changing priorities from our stakeholders and functional owners.

This is the road app we're going on. We're going into the cloud environment. We are hoping to get into the cloud environment in March of next year which will give us the dev set-up environment we need to operate. One of the big changes that we have is that choice to move into the cloud earlier versus later. I'll talk more about that in this slide.

This slide, just everybody knows. This slide is [1:08:22 inaudible] looking discussion. This is not stepping stones. This might be going to change based on requirements, changing in priorities, but this is what we believe is the best way to go forward for NBIS.

As I said, we have a release in March for the crowd and a couple other functionalities. The major release would be in June based on this work 21. That I said, this slide may or may not hold, depending on what kind of requirements we get and what kind of priorities change. Particularly, as we moved forward with any EC's coming out [1:08:53 inaudible] work initiatives and/or how the ER was assigned and went. They'll all text you with the schedule. That's basically what I have through NBIF. Any questions?

Mark: Okay. Carolina, any questions for Sheldon on the WebEx?

Carolina: I don't have any questions on the chat.

Mark: Okay, any questions for Shelton on the phone?

Tania: If anyone on the phone would like to ask a question, please press #2. You like it.

Tricia: Hi, this is Tricia Stokes again. Can everybody hear me?

Mark: Yes, go ahead.

Tricia: Thank you. Just one clarification from what Shelton just said on the June tier one delivery. We are working diligently to that desired goal, but I think we have a lot of work to do with the business office, with all the components of being able to deploy this. I just want to go on record and say the road map and the true capability and delivery schedule is under development. Thank you.

Mark: Understood. Shelton, many thanks.

Shelton: Yes, thank you.

Mark: Okay. Our next [1:10:29 inaudible] here from Valerie Heil, associate director industrial or USDI. We got an update as the NISPPAC executive agent.

Valerie: Thank you.

Mark: Welcome.

Valerie: Good morning everyone, several items to update you. The Department of Defense is establishing a personal vetting transformation office. The acronym for it as we do in DOD is acronym, PVTO. The PVTO will support planning and enable execution both for transferring background investigations to the Defense Security Service and reforming the personal vetting enterprise.

The PVTO will assist in coordinating and aligning recourses between the transfer and ongoing security clearance reform efforts or vetting efforts. The PVTOs planning support will leverage merger and acquisition best practices and data analysis.

Second item, the FY19 national defense authorization act, included the section 842, siding that by October 2020, the Secretary of Defense would have to require national interest determinations or access to prescribed information, which is top secret, SCI, SAF, COMSEC and restricted data for US cleared companies operating under special security agreements. Where the ownership came from what are referred to as National Technology and Industrial Based Companies.

When you looked at the supporting legislation about what is an NTIB company, those would be US companies owned by Canada, Australia or the UK. Right now, the Department of Defense is evaluating legislation on how we would implement it in DOD policy and consultation with ISOO and the other four NIS cognizance security agencies.

The third item, the NISPOM issuance, as some of you know, we worked informally with NISPPAC for several years on that. The draft, we issuance is currently in DOD coordination. Once we complete the DOD coordination, then, we must receive concurrence from the other four NISP cognizance security agencies to the diversion.

It's been confirmed to us recently that it will then have to go through the federal rule making process and become a federal rule. In that context, general estimate would be that we are probably at a year or two at least two years away from publication because, at this point in time, Department of Defense will not publish the NISPOM, unless the companion federal rule was also approved at the same time.

The last item I have is, we have talked about in NISPOM Change Three to incorporate the reporting requirements of the security executive agent, directive number three. We did provide some month ago a draft industrial security letter to the NISPPAC for comment. We appreciate those comments that we received. We are still evaluating how to proceed with the industrial security letter for the DOD contractors and those non-DOD agencies, for which we have industrial security agreements.

The issue that we are grappling with is how to handle the foreign travel reporting. We will keep you in the loop. It's still something we want to do. We just have some challenges in working through the details. With that, are there any questions?

Dennis: Dennis Keith, NISPPAC. Valerie, during the stakeholder speaking with DSS yesterday, there was some discussion about the newly established department [1:14:27 inaudible] technology protection taskforce.

Valerie: Yes.

Dennis: I'd like to ask if there's a way to clarify what the industries engagement would that taskforce might be.

Valerie: Yes. There is a critical technology protection task force that's been established to DOD under the direction of the Deputy Secretary. I know that came up yesterday about industry involvement. I will have to take it back. I'm not sure. I know it's just relatively new, as far as being stood up and how that will work. I will take it back and provide some feedback to the NISPPAC about what the taskforce considers about how it will interact [1:15:03 inaudible]. I think I understood yesterday that there was some indication that there might be some periodic round tables, but I don't really know if that's going to be the case.

Dennis: Okay, thank you. The second question is also from yesterday with regards to new DFARS requirements that might be under consideration further deliver on compromised [1:15:23 inaudible]. If there's a way to advise.

. industry as to the path for consultation on what those DFARS commerce might look like.

Valerie: I will take that back to our acquisition colleague who handles the DAR process for DFARS classes. I'm not sure where things might stand with any process for that at this time.

Bob: Bob Harney, NISPPAC. Valerie, back to the taskforce, has there been any movement as the taskforce is being stood up, whatever, as far as how to reign in some of the variations to the theme that are coming out of the Navy or the Air Force, or whatever on **[1:16:09 inaudible]** plus X and things of that nature as there's a lot of reaction on how to handle the cyber threats and those kinds of activity? Is that part of the task force mission is to get that kind of vague. There's something consistent across DOD and what is being pushed out in the industry as new requirements?

Valerie: I would have to say that the task force is still relatively new. Some of what you're asking, I don't have the exact details other the initial task or memo that was send out across the department. They are spilling the **[1:16:47 village]** as far as the task force members. I can take that back also to one of my colleagues, who's been detailed **[1:16:54 inaudible]** have any details at this point.

Mark: Anyone else have any questions for Valerie? Anyone on the WebEx?

Carolina: We don't have--

Mark: Anyone have questions for Valerie on the telephone? Okay. Thank you so much. Quinton? Industry spokesman, new industry spokesman. **[1:17:37 inaudible]**.

Quinton: Good morning. We have two new industry NISPPAC members. Roselle Barerro and Sheryl Stones, we want to welcome. We have one change on the MOU, Kyle Hanson is now the chair. You can do it. Go ahead.

With the vast amount of changes in security policy and procedures, the implementation of these changes is enhanced when industry expertise's is leveraged collaterally early in the process. Industry is interested in learning more on the delivery on compromised initiative and the possible impacts for industry.

We want to thank the ISOO facilitating dialogue with Director Evanina to discuss information sharing and collaboration on Sec EA policy issues.

When it comes to DSS and transitions, we're still working with the collaboratively with the working groups, but we do feel that, if

continued upon an enhanced understanding of the threat and vulnerability, which is not supported by the current information sharing infrastructure. We're concerned about variances in implementation from one field office to the next. We're still unclear as to the corporation with the GFAs and concern about the impacts of introducing vulnerability information to the GCA outside the scope of the contract. Next, we're interested in how CUI governments will be distinguished from--

Male Speaker: [1:19:30 inaudible].

Female Speaker: [1:19:35 inaudible] microphone.

Quinton: Okay, sure. Under DSS and CUI, we're interested in how CUI governments will be distinguished from this government. Industry continues to be [1:19:51 inaudible] to describe the forest compliance for the CDI on unclassified networks.

Under new business for NDAA, as DOD investigations transitions from MBRD to DFF, we're looking forward to learn more about trusted workforce 2.0 as industry engages in the trusted workforce working groups.

When it comes to small business, with all the changes, industry is concerned about small businesses and the impact on supply chain. We're still waiting for comments from DFF on the NCMS security consultant white paper, concerning use of security services providers.

Next slide; there's a lot of new systems out there, think like they all [1:20:46 inaudible] at the same time. The industry is concerned with the ability to obtain access to these systems in a timely manner. Seeing that with certain systems we're applying and is taking weeks to get access to use systems. We're still concerned when it comes to lax training for DISS.

Next slide; Industry is still waiting the implementation information regarding travel reporting under C3, that was already talked about earlier. Where we received seven and eight drafts are under coordination and have requested the ability to provide input, but we're still waiting for response.

Next slide; Industry is waiting more clarification on information of the evaluative committee on industrial security and industrial base policy. We're also waiting for the slide.

Mark: Maybe waiting along.

Quinton: The last slide is on the legislation watch. Industry is waiting more clarification on information of the advisory committee on industrial security and industrial based policy. We're also waiting for program information on the defense policy of evaluative committee on technology as well. Questions?

Mark: Just an observation from the Chair. It seems to me you're still waiting on a lot of things.

Quinton: Yes, we are.

Mark: I've been Chair for almost two years. I'm hearing still the same thing over and over again [1:22:27 inaudible] we do a year estimation to actually do something about this. Still having these quarterly meetings where I keep hearing the same thing. Need more working groups, do we need more meetings like we had with Bill Evanina in the SCIF?

Quinton: We need more engagement. When we were talking with the government, and we're speaking with the government, once we lead the meetings, we need them to come back with this.

Mark: The answers?

Quinton: With the answers. We have the meetings. We tell them what we need or what we want, or where we [1:22:56 inaudible]. We're trying to collaborate with them to help them help us, but we give them the information, but we don't get anything back in return.

Mark: Greg, maybe what we ought to do is start holding some meetings ourselves and maybe just pick a topic and try to have a meeting about it. I don't know [1:23:12 inaudible]. I am getting tired of hearing the same stuff.

Greg: I agree and I appreciate as Quinton alluded to. There is a lot of different things going on in terms of a lot of systems and what have you. At the same time, it is troubling that things are, I'm not sure what the right word is, percolating, but not resolved. Yes, I'm open to other ideas, but that seems reasonable. I mean, this is a partnership. I'm not trying to throw anyone under the bus, but I've said this so many times. I think most people agree.

There's so much expertise on both sides, industry and government. That's where the real value, I think lies in a committee like this is, not just hearing about that expertise but then, putting it to good use, putting it into practice. I think so, if that's the direction we need to take.

Mark: I think that's right. We actually need to do something. Again, I'm getting a [1:24:25 inaudible]. I understand too. We all take lead, DOD take one minute challenge and task here with this background investigations. It's a time of enormous transition and uncertainty. That said, if this committee can't resolve things, then I wonder what the point of it is. I think we need to do a better job actually getting some answers. Again, maybe the answer is, you don't like, but at least get you a new [1:24:51 inaudible]. I mean something. Okay, exactly. Let's see what we can do a better job on that.

Valerie: I would say on behalf of the Executive Agency, this is Valerie Heil, that DOD does, because there have been a number of speakers today from DOD. It's [1:25:05 inaudible]. There will be additional [1:25:08 inaudible] we do to the utmost of our ability. The information and the processes that are ongoing provide as up-to-date information as we can.

Mark: All I can say again is we're a team. We need to work together, because obviously, why we're here as security of United States. I mean, we're on the same side. We just need to do a better job. I think about listing what you need and then hearing [1:25:37 inaudible] legitimate concerns on both sides.

Greg: I would suggest that we'll reach out and call it a program resolution meeting, because we're at a point where we got a lot of things that are on the table. I think we need more clarity definition as to, like you said, some things Mr. Chair, we can't resolve in a way that industry may find favorable, but they deserve a response. I know there's some things out there about this. For example, I mentioned in the beginning, the use of the consultants and the small businesses. We'll frame it as a resolution type meeting and see where we can go with that, if you agree.

Mark: I think that would be a healthy thing to do and as long as this is done collaboratively and obviously [1:26:30 inaudible]. Okay, anyone have any questions for Quinton? Anyone on the WebEx?

Carolina: No questions on the chat.

Mark: Anybody on the phone for Quinton?

Tania: Once again on the phones, please press #2 on your telephone keypad if you wish to ask a question.

Mark: Okay, no one on the phone for Quinton. Quinton, thank you. We're going to hear from Keith Minard from the DSS, to give us an update on their initiatives. Then we'll take our 10 minute break. Welcome Keith.

Keith:

Good morning. I give him all of the breaks though. Mr. Chair, part of the discussion previously, I think we have to deal with this prioritized actions and look at accurate expectations on timelines to accomplish certain things. Some things do take a little bit longer with 12,200 clear facilities and 900,000 cleared employees, as we work these processes. That being said, first welcome to Quinton as the new Industry Chair and also, the new members of NISPPAC.

First, we'll talk about NISP contract classification system. It's been a slow roll, but we're moving forward now. Hopefully, decent pays I think start service partners out there; army, air force and navy. We're really looking again for implementation place. It is a flow down system. If we talk to industry, keep in mind that, this all starts with a prime contract 254. Bear with us as we move through the process. We want to make sure that we got the effective capability in place, to ensure that the optimal use of the system is there for Industry.

Speaking of Industry, one thing I like to know for the smaller companies out there, that unless you're sub in contract in NCCS, down to a sub as a prime. The system itself will generate 254 from your prime and sent it to you by email. Now, in industry, you actually have NCCS as we deploy out.

Quinton, in regards to helpdesk information, we do have the DLA helpdesk. It does support contract account management and Kim, services for your contract account managers. Either you can go there directly from the information or website, or you can actually dial the DSS knowledge center and be referred there. We do have an email address on our website to help address operation issues outside to what DLA provides.

What we really need to know now, Quinton is, what's the services that we don't have right now available, and what's the issues that we need to address in the future through helpdesk or knowledge center? Make sure we provide the right services to cleared industry partners and also government industry.

Second is, the advisory committee that was up. We're actually in the process of working nominees for both government and industry, primary and ultimate. It's a little bit of a process that we have to go through for approvals and nominations, so bear with us. We're tentatively scheduled to have... again, I say, tentatively scheduled to have a first advisory committee meeting in late... second quarter.

Actually, today, Chris Forrest is actually the designated Federal Official for the committee. He's present in the NISPPAC. As we go along, we'll keep industry informed in that process.

One thing I would like to note is actually over the last couple of NISPPACS, we've been working with our operation side of the house. Also, field personnel on the issues addressed in the NCNS white paper. It took us a while to find out what's in the field prospective. What are issues were from our side, to make sure we can have a collaborative effort with industries to move along.

I understand that our operations inside of the house is planned in early December meeting with Michelle Sutphin and about 12 industry partners to further address those issues for small businesses, security consultants and security services.

Just as a note, you may have seen it in public comment, DSS 328 certificate pertaining to foreign interest without her comment. The fundamental changes, the document, just 10 questions in a change. The form was updated to provide each use for the defense enhance security program. As well as DHS as a kind of security agency for their classified critical infrastructure protection program. Again, no questions, no change to questions, just for its use.

You heard Greg mentioned earlier about CUI, I'll just give a quick update. We're on the final stages of recommendations and plan. Plan of action that will go to the USDI based on the May 2018 memo. We're working with our government partners right now. As we move along, we actually went to get a head nod and approval on the recommendations. We'll begin the process of engaging industry.

I want to make a point for industry, this is about 10% of the entire defense industrial base, which puts DSS as the functional manager for and lead. Keep in mind when we start reaching out for CUI and industry as partners, then this will be a component of that, but we have much of a 90% that we have to manage into the integration process to make sure that we're engaging in the entire community.

We see that over the next probably, 30 to 60 days. If we have an opportunity, start looking for the right industry partners as we work to this process.

We have had very good success working with our service partners in acquisitions and the DOD CIO in this process. We look forward to engage over the next period of time as we implement these processes in DOD.

The last I have for you before your break is, reminder, USA learning is a transition from step, it's out there CDSE post new training all the time. Take a look at the CDSE website, to see what's available for training. Does that answer your questions?

Male Speaker 1: [1:32:06 inaudible] our break.

Male Speaker 2: [1:32:09 inaudible].

Mark: Anyone on the phone for Keith?

Tania: No questions on the phone.

Mark: Thank you so much. Okay, let's take a 10 minute break. Restrooms are here to the left. If you please, be back in 10 minutes.

Male Speaker: 11:45.

Mark: Yes. 11:45, we can wrap it up. Okay, our next speaker would be Patricia Stokes in DVS, will update us on the transfer of investigations to DSS.

Patricia: Thank you--

Mark: [1:32:48 inaudible]?

Male Speaker: Yes.

Mark: Patricia?

Patricia: Yes. Can you hear me?

Mark: Yes, ma'am.

Patricia: Okay. As I mentioned earlier, I am the Director of the Defense Vetting Directorate of the Defense Security Service. I updated your forum last time. As Charlie suggested, I went back and looked at the notes. I'm here to bring you up the speed on where we've been since then.

As Mr. Phalen indicated, we are all anxiously awaiting the incoming executive order, which we expect to be imminent, but that has not deterred us in any fashion on moving forward with our planning, with our NBIB partners. We are engaged daily on many facets of the transfer. I think you could probably imagine. There are a myriad of them, but I can tell you that the Defense Security Service defense vetting director team is really focuses on the transformation aspects of the transition.

The other heavy lifting of the acquisitions and the people, the HR component and the facilities and all of that is under of important things are being handled by our headquarters with a joint team with NBIB. Certainly, with support of the personnel vetting transformation office that Miss Heil briefed you on earlier.

The other thing that the Defense Vetting Directorate is doing is, in all the transfer activities, this includes, I don't want to leave this out, the transfer of Department of Defense consolidated adjudication facility, small portions of the defense manpower data center, few of their people and certainly all of the systems that support the vetting enterprise. Then finally, the defense information systems agency, program executive office for the National Background Investigations system.

All of those entities will be transferring to the Defense Security Service soon to be renamed, the Defense Security Counter Intelligence Agency. The Defense Security Counter Intelligence Agency, let me make sure I get the acronym right.

Progress since the last meeting is, we're working very-very closely in the DVD directorate with our National Background Investigation System partners. Also, the Personnel Vetting Transformation Office again that Valerie mentioned.

We're very-very much aligned and supporting and participating in the trusted workforce 2.0, because that is defining our future. We sit on the Executive Steering Group committee that meets monthly. That will culminate at the end of this year with the eighth presidential draft, a presidential directive and many other artifacts revision to federal investigative standards, revision to the adjudicative guidelines, and a myriad of other reform.

The heavy lifting on all of this work has been completed by the pack PMO, the Performance Accountability Council Program Management Office, they have done an extraordinary job. I believe maybe the DNI may address some of this when they have the podium next. Everything that they are doing, we expect to be documented. We'll get some actually relief early next year.

In another executive correspondence, as we all know in this town, it takes a while for presidential directors, executive orders and policy to be amended, but that is not stopping the leadership of the pack in reforming efforts and giving us some immediate **[1:36:49 inaudible]** early next year to another executive correspondence much like the three that they previously issued to get started on some of these reform changes.

The Department of Defense, DVD, is ready and were poised to start executing this changes in the executive correspondence. That is anticipated again early next year.

What we have done since I spoke with you last is, we've established something that I mentioned earlier, when I cut in on the phone call. We've established our enterprise business support office. Now, what that is for simplification for the group, is really the support office. The customer support office and the system development on the business side support office that will fit side by side in the agile acquisition framework that Sheldon described in his briefing with our developmental operational counterpart.

It's really the subject matter expert that I bring to the table that sit with the Dev Ops to actually build capability, provide the requirement, as the developers build the capability, test out the capability. At the same time, we'll have business units that are attached to that that addressed to the other parts of the things, of deploying enterprise capability such as this. That will be a strategic communications team that will be able to communicate with our customers early, before this deployment was coming, what you expect, building the training that's necessary to understand how that execute, when the capabilities are deployed in small increments.

Addressing the policy issues with the policy issues whether it be the SecEa or CUA or our own policy makers within the Department of Defense as we assume this mission. Making sure the policies are aligning to allow us to execute these new capabilities and these new deployment [1:38:56 inaudible]. Then, certainly a performance in metric shops that will be measuring our every action to make sure that we are making progress in the right direction, that we are executing data driven decisions and that we say the continuous improvement mode.

Secondly, we've been working very diligently on the execution of the last executive correspondence which is provided as significant activity and I would say relief. What that did is it allowed us to defer or clean periodically investigations and put them directly into continuous evaluation program.

To date, we have deferred over 35,000 cases. We started this on July 31st this is a very good news story. Why? Because we are not adding to Mr. Bailey's backlog or inventory. It's also allowing us to really kick the tires and test reform in realistic ways.

We continue to refine those business rules. [1:40:08 inaudible] every week, our staff keep growing. We are working with the executive agent, the security executive agent to further refine our business rules so we can increase our deferment thresholds and our way of cases that we're putting in deferment by sending into the inventory.

I would like to remind everybody in the room right now, because this question always comes up and variably I would get asked, is that the executive correspondence that was issued that allowed us to do this said, that these cases will be reciprocally accepted by all agencies.

I understand that the system of record doesn't reflect that and that's a challenge, but we we're not going to hold up this very-very important authorization and ability to not add to inventory and start testing our transformation and reform waiting on a system change.

Perhaps Miss Langley could give us, the group some in refer to fidelity as to when that system changed will be realized. It will be reflected on the system of record, but in the meantime, I know industry is struggling greatly with this support multiple customers, I can tell you that your best course of action would be to touch base with your government sponsor when you get pushback or call the vetting risk operation center industry division probably previously known to most of you as [1:41:35 inaudible] office for industry and bring the issue up to them, so we can provide some assistance. That's my update. Any questions?

Mark: Any questions? Please, yes. Can you give the microphone for...?

Kim: I just have a quick question. This is Kim Baugher from the State Department.

Mark: Identify yourself please.

Kim: I did. Kim Baugher

Mark: [1:42:06 inaudible]--

Patricia: I heard you Kim, thank you.

Kim: I just want to make sure from a user agency standpoint. I don't really know who to call anymore at Defense Security Service, to be honest with you on issues. Are you saying that, you kind of are the whole kit and caboodle, like we're supposed to call you for every [1:42:22 inaudible] subject matter experts? You have the policies, you have all this stuff?

Patricia: For the background?

Kim: For whatever that we're supposed to contact with questions or concerns?

Patricia: For the background investigation mission, if that's what your question is, yes. I am the kit and caboodle for the background investigation mission. What we are going to do in this calling or and your questions, ma'am, have also enlightened me to: A, we need to put a person from the website and we also probably need to actually quickly establish an enterprise business support office box where we can actually entertain your questions and then get back to you.

I would not take responsibility for the critical technology program, or the counter intelligence program, but anything from the background investigation and vetting mission, yes, I am your single point of entry.

Mark: Does that answer your question?

Kim: I guess I'd like an old chart of DSS right now.

Patricia: The old chart with DSS is under development. It is with our director. Once our director gets it approved through the Department of Defense, I'm sure it will be shared.

Kim: Okay, thank you.

Mark: Okay, another question?

Mike: Yes. Hi Tricia, this is Mike Scott from DHS.

Patricia: Hey Mike.

Mike: We understand that the system is going to take a little while to build out the JPAS, whether somebody's in the CE that's not going to do that. We're going to go into this, so we can do the reciprocity or the **[1:43:53 inaudible]**.

In the previous meeting, their response about is going to be interim guidance on exactly where to call to find out that information. Do we have a timeline when that guidance is going to come out for us as an agency so, we could use that to help **[1:44:06 inaudible]** partners and ourselves, for people transition?

Patricia: Mike, I'm going to take that for action. I think I have members from B-rock there who might be able to address what is on the website for them right now, but we certainly need to get the message out.

Do I have a B-rock member in the audience who might be able to address what's on the site for industry? I know that your homeland security might, so we certainly need to address that at the DSS website, for the DOD as well.

Patrick: This is Patrick Hogan with the B-rock. We do have the information on our website. We posted a frequently asked questions related to the deferment. On there, there's an email address for those kinds of questions about enrollment in CE especially for the government customers looking to have verification while we wait for that technical solution that patch up.

Mark: Any other questions? Carolina in WebEX?

Carolina: No questions on the chat.

Mark: Okay, any questions on the telephone?

Tania: No questions on the phone.

Mark: Thank you so much.

Female Speaker: Can I have the--

Mark: Yes, go ahead.

Female Speaker: Were you going to...

Keith: Keith Minard, Defense Security Service. Over the next probably period of time, we're going from a few mission states to a large, multi-mission agency. There would be a wide range of changes that go along. I'm sure as we go along, those changes will be formalized and socialized, but just a few years ago, you think about the CESC mission, the NIS mission and some intelligence services post the previous background investigation mission. Now, with a wide range of CUI, CTP, NISP background investigation.

As we grow, we will have to evolve and get the right organization structure with everybody to make sure it's understanding that we no longer have what used to be single point to contact in to, potentially because of the multi mission space, a wide range to point of contact.

Mark: Okay, anyone else? All right. Thank you so much. Our next speaker will be Valery Kerben, ODNI. To provide a Security Executive Agent Directive, SEAD policy update. Valerie, on the phone?

Male Speaker: Yes, she's on the phone.

Valerie: Yes. Good Morning, can you hear me?

Mark: Yes.

Valerie: Okay. Good morning. Thank you, Mr. Chair. On behalf of the Security Executive Agent, I'm pleased to announce that SEAD seven, reciprocity of background investigations and national security adjudication has been signed by the DNI as of November 9th. At this point, it's being prepared for distribution, to executive departments and agencies. Of course, our websites will be updated shortly thereafter. There will also be a push to our Security Executive Agent advisory committee members. It will be forth coming to you all for your information and for implementation within your agencies.

For an update on Security Executive Agent Directive eight the temporary eligibility, it is still in draft. We have received our comments back from all of the agencies. It's finishing up in the adjudication process. We received many comments which we are considering a lot of those in the revision. We are hopefully going to have it submitted to OMB for formal interagency review by the end of the year that is our goal.

I know Charlie and Tricia spoke a little bit on trusted workforce 2.0, but for those of you unfamiliar with it, this effort will lead to an overhaul of the security clearance process. The security and the Executive Steering Group does include, ODNI, OPM, OMB, DOD, NBIB, DHS, FPI, DIC and industry partners. They're engaged and meeting frequently. The first step on everybody's agenda was of course to take those substantial steps to address the backlog investigations.

Phase two, which is what we're working on now, is to revamp the fundamental approach and supporting policy framework to ensure the lines. We're overhauling the business process plans to improve timeliness, quality, and effectiveness of the process to help further reduce the inventory. We're modernizing or plan to modernize the information technology architecture, to expedite the migration of continuous vetting model.

These are the things that are being worked on from the Executive Steering Group. Also, the pack which has the lead on ensuring all of these decisions are brought forward to the Executive Steering Group. That is all I have to provide.

Mark: Okay. Anybody have any questions for Valerie?

Greg: Yes, I have one.

Mark: Go ahead.

Greg: Greg Pannoni, ISOO. Thank you, Valerie. A lot of good progress I appreciate that. As you may know, many of us were at the AIA and DIA conference in San Antonio last month. We had to opportunity, [1:50:04 inaudible], for all industry folks to meet with and I was [1:50:07 inaudible] too. We had good discussion. I would characterize it as far as the back and forth flow of exchange of information.

One of the items you'd mentioned on the trusted workforce 2.0, that there are industry members on that group. I understand there are two, I believe Dough Thomas and [1:50:25 inaudible]. Is it the other fellow? Evidently, from what I've heard from my industry colleagues is that, they're not allowed to share information that they are learning about and participating in the working group. I'd ask that you take that back to Mr. Evanina, to see if there's something we can do here, to barge the aperture just a little bit. When we're talking about the eight NISPPAC Industry members, as far as being able to share and utilize their expertise to have more input from industry on that group.

Valerie: I will take that back. I just also want to caution you that a lot of the information is pre-deliberative and they're making decisions. Some information is not even being shared outside of this group, at this point. There will be the opportunity for some stakeholder inputs. I'll let the pack know and also Mr. Evanina, that you're addressing that concern.

Bob: Yes, Bob Harney, NISPPAC. Valerie, in the same thing as Greg's question, but with the SEAD that is about to be published, since Industry had no view into that at all or ability to input, is there any language in there in regarding CE and reciprocity? For SEAD date, now that it's in its infant stages, is there any chance as Bill had alluded to having the NISPPAC be able to have some level of review and comment on that as [1:52:11 inaudible] addressing through the approval process?

Valerie: Bob, in regard to SEAD seven, it does talk about different ways of accepting reciprocity. You'll all be seeing that. I don't want to get into all the specifics, but, for SEAD eight, we're just at the process now. It can be ready for OMB. As far as I know, OMB only goes out to agencies for formal comments. We're still looking at ways to possibly share it with you through the process, but at this point, we're still moving ahead to get it to OMB still in draft.

Mark: Are there other questions for Valerie? Carolina WebEx?

Carolina: No questions.

Mark: Okay. Anyone have questions for Valerie on the telephone?

Tania: A reminder to those on the phone, if you wish to ask a verbal question at any time please press #2 on your phone. No questions on the phone as this time.

Mark: Okay. Thank you, Valerie. We'll next hear from Mark Riddle of my office, on the implementation of the control on unclassified information program.

Mark Riddle: Hopefully everybody can hear me. This is going to be a pretty short update. I know we're usually pretty long when down in the CUI side of thing. This will be refreshing, right?

Generally, right now, of course we're in the middle of agency implementation and agency reporting on their efforts to implement the program. Majority of the agencies in the executive branch have reported to us on their status. Already a number of agencies are serving full compliance with the CUI program. This means that they have policy, training that they've transitioned their physical environment and also information systems to the standards of the program, which is great.

Now, it's going to start the work of validation or what we **[1:54:26 love to hear]**, inspection. ISOO oversight in our role in the part of CUI program. We are going to be going out in evaluating and accessing very agency that deserves total completion all our miles as long as related **[1:54:42 inaudible]**. Also, if any agency out there has a complete policy training module, you're going to see **[1:54:49 inaudible]** stepping out into the executive branch. Validating and making whatever course corrections are necessary. To ensure that there is alignment with the program **[1:54:59 standard]**. Of course, the results of the annual report submissions from agencies will be detailed in our annual report to the president.

Generally, based on what I'm seeing, compared to fiscal year '17, we'd have seen a lot of movement largely because money has been flowing. Agency **[1:55:16 inaudible]** sources in the way of implementation of the CUI programs. As a result, we've seen a lot of movement among a lot of agencies. Also, been out for two years, so they got some momentum, but, what you can expect and what we're predicting is that, once agency is issued that agency level implementing policy, everything seems to follow pretty aggressively. The system transition, physical environments **[1:55:42 inaudible]**, we had to come on that of course.

Now, the CUI registry is what we protect in the CUI program. If you haven't been there yet, I highly recommend that you do a visit to the CUI registry page. It lists all the categories of CUI, along with guidance documents that we issue to help agencies and other stakeholders, industry, state, local, tribal, academic institutions who have subjects to the requirements of the program. Guidance to help them understand and implement the program as best as they can.

Also, what you'll notice, it's been a while since we've been out here. ISOO has developed a number of training modules to assist agencies and stakeholders. Train the workforce on the standards of the program. These training videos are posted on our page, also posted up on YouTube. They're free for all to use of number of cabinet level agencies. Also [1:56:37 inaudible] are using these to satisfy the training requirements of the program.

We highly recommend that you take a look. You don't have to use them, but they will save you on the development of these training modules. We address everything from [1:56:52 inaudible] to document one thing. [1:57:00 inaudible] concepts of law for government purpose and of course our relationship with freedom of information act.

In regard to notices, one of the things that you'll notice about CUI program is that, we issue a lot of CUI notices clarifying guidelines or policy points on how this program is structured or how it should be implemented.

Over the next 30 days, you're going to see a number of new notices hit the street that are going to assist agencies [1:57:28 inaudible] program. Every [1:57:31 inaudible] document disruption to provisional categories, to even the process [1:57:35 inaudible] control markings.

Moving quickly to my third bullet here, about the federal acquisition regulation. What this is going to do for the government, once it officially takes hold, this is going to standardize the way that executive branch agencies convey safeguard and guidance to non-federal entity.

Right now, there is some inconsistencies of course, as you know. Whenever an agency enters into an agreement with a non-federal entity, they're often times referencing their policies and procedures. They're naming convention associated with sensitive information. Once the FAR hits the streets and by our estimation right now, should be sometime in the summer [1:58:14 inaudible]. That message would be consistent.

Everybody in the room is familiar with the DV-254, which is that form that agencies right now to convey the safeguarding requirements related for classified information. The CUI form will have a similar type of form, our company, where agencies when they issue a contract that the CUI is involved, they will be required to complete this form where the categories of information, the safeguarding standards dissemination controls will all be conveyed.

One of the goals that you will see, one of our goals of course is to make things better. We believe that the federal acquisition regulation will make that process and bring a lot of clarity to how agencies convey that safeguarding guide.

One of the things you can expect of course is that the public will get an opportunity, industry will get an opportunity to comment on the federal acquisition regulation. Right now, we project that the form will be out to public comment sometime on the end of January of 2019.

If you subscribe to the CUI blog, you'll get an update about when that regulation is out there for public consumption. I encourage everybody to take a peek at it and provide some comments to make it better. Like with every regulatory process, the more hands that we have in that process, the better the product will be. Since it's going to affect you, sure, we highly recommend you take a look and provide those comments.

My fourth bullet here speaks to our regular update that we perform to stakeholders. Every quarter, of course CUI program has a webinar for all stakeholders into CUI program. This is state, local trial, but everybody tunes in and ask questions, in regard to the program. It's also laid for us just to convey the general status of things. Like the federal acquisition regulation. New training modules that we developed awareness products, but, it's also just a great form for Q&A or even just for us to solicit suggestions from the stakeholders in the CUI program initiatives that we have underway in the CUI program that eventually manifest themselves [2:00:27 inaudible] notice coming from the stakeholder discussions.

If you haven't participated and tuned in to those, I highly recommend you do. Also, as the executive agent for the program, we have a very open door as far as communication goes. Literally, anybody can contact us through our inbox. Ask a question, offer suggestion. I guarantee you, every one of those will be reviewed and you will get a response. Due to the volume, it does take us some time to get back to everybody, but somebody will get back to you and incorporate those things.

Now, we have one yesterday. There's stakeholder briefing. The next one will be February 13th. One to three, of course the [2:01:10 inaudible] that will be available on our CUI blog.

Also, lastly to close out, on December 10th, we're planning a CUI, Industry day. That is exactly [2:01:20 inaudible] sounds like we're at... for two years in the implementation, a number of industry folks and agencies want a form where they can get out there and talk about the products and services that they developed to assist agencies and other stakeholders how they implement the program.

It's a free event. The schedule of all the vendors and also the presenters are posted to the CUI blog. We encourage you to spread the word, if you want to attend, of course just shoot a quick email to cui@nara.gov. Let us know that you're planning to come and that you're planning to bring 50 of your closest friends with you. It should be a great event.

If we have a good turnout, which already looks like we're going to, we'll probably do this again [2:02:04 inaudible] the summer. Keep that in mind. Everything that we do on regard to industry days is first come, first serve. Meaning that, as soon as we drop the notice to our CUI blog that we're having this thing we get flooded with request to be a presenter or to even have a booth at the event.

Our only criteria is that, whatever you're presenting, or whatever you're going to present or do for this event, has something to do with CUI. I think that industry really [2:02:31 inaudible] provided a really great agenda for us. We have folks who were talking about automated marking tools for the electronic environment, of course, destruction requirements. Folks who are out there who are [2:02:44 inaudible] companies and agencies with compliance to the standards to the standards of the CUI program for the electronic environment. This [2:02:50 inaudible] 153 for the government folks really good stuff out. We're really hopeful [2:02:58 inaudible] just a word of caution.

We have to say this is that, of course ISOO, we have not evaluated any of these products and services. Agencies are using some of these. They conducted the evaluation. We always say, evaluate with caution always do your own evaluation before you start signing out these checks. I think at this time, I'll open it up for questions for everybody on the WebEx, on the call, in the room.

Mark:

I'm going to make a comment. I assume responsibility for CUI end of July. I really want to commend Mark Riddle in particular and the entire CUI team in general they've done a fantastic job. Probably

many of you know, it's been [2:03:46 inaudible] process getting this CUI program implemented. We're seeing some really good progress. A lot of that goes to Mark and the team.

I also want to put this out. I did check with the boss. It just occurred to me, we have CUI advisory council which is all government right now. We'll check the chart on by-laws, but I don't believe there's any reason why we couldn't extend at least an observer role to a non-federal entity on that advisory council that meets about monthly. We're going to look at that and put that out. You don't have to keep it just for the [2:04:22 NISP], because it's much bigger than that. That's all.

Mark Riddle:

One of the great things of course is that, we share it to CUI advisory council, which is comprised with about 26 cabinet agencies. Also, some of the suspect that you would expect to see there. This is something that we'll definitely raise in our next council meeting, which is December 13th and possibly open it up for industry.

Right now, of course, some of the things that we talked about at the CUI advisory council that would be appropriate for industry to be there, because we are talking [2:04:59 inaudible] changing markings and standards. We don't want to get [2:05:01 inaudible].

Absolutely, I think that when we meet in probably as early as January. We might open that one up. Probably, we also have a pretty open phone line. We have to have you RSVP, but keep an eye out for that. If we do open something up, at the next council meeting, we'll probably post it to the blogs. Again, subscribe. It's really great. Are there any questions comments?

Tania:

As a reminder to our virtual audience, if you wish to ask a verbal question, please press #2 on your phone and your line will be unmutes. If you prefer to submit a written chat, please use the chat panel and send questions to all panelist to be readout loud.

Mark:

Okay. It sounds like there's no questions. Thank you, Mark.

Mark Riddle:

Okay.

Mark:

We're going to move rapidly into our working group reports. Greg, you're going to start with the insider threatening. Karl Hellman will give us the one on the NISS update.

Greg:

Yes, thank you Mr. Chair. I'll try to be quick. Insider threat working group, we did convene a meeting on October 30th purpose was to evaluate the process. The government will use to evaluate the effectiveness of contractor insider threat programs and in general to

provider forum for NISPPAC members to discuss ways to improve the program.

The group received two briefings. One on the DOD ITP policy and foundational documents and one from DSS, which is an overview on insider threat effectiveness. The primary principles for the program effectiveness conveyed, were program management, awareness training, information system's protection, collection and integration, and analysis and response. Each of these principles have associated ITP requirements and corresponding assessment factors for determining the effectiveness of their implementation.

Other points in evaluating effectiveness discussed including consideration of the whole program, as well as the size and complicity. Compliance, not necessarily determining effectiveness. The ineffective program may impact the overall security rating. To some, there are three steps to evaluation of ITP effectiveness, review program requirements, assess program implementation and determine effectiveness.

The group plans to meet again sometime in mid-January or early February. We encourage in particular the other CSAs. DOD was terrific. They were well represented as I say, in these briefing's came from them, but I asked the other CSAs come join us and discuss their approach to evaluating the effectiveness of insider threat. Are there any questions?

Mark: Carolina, none? Anyone on the phone for the insider threat working group?

Tania: No questions on the phone.

Mark: Right. Karl Hellman, please? Step up. Give us a latest on the--

Tania: I do have one comment on here. They're saying, they have ten minutes left on the call.

Mark: What was it?

Tania: They only have ten minutes left on the call.

Mark: Okay, yes. Karl, go ahead.

Karl: Thank you, Mr. Chairman. Moving rather quickly, just want to update on what the NISP working group is working on and what DSS is working on. Since our last meeting, one of the things that we were talking about is our transition to eMASS. It's our system of record per assessment and authorizations of classified systems. We had initially been looking at a launch date of that transition date of that

is October 1. We ran into an issue with the access to the training site, which is maintained by DISA.

We're working group and some other [2:09:29 inaudible] AIA, NBIA, and NCMS. We delayed our transition. DISA was able to fix issues with access. We now have dates for our transition to eMASS as the system of record. March 18, 2019 will be our training date.

We will also have a new version of our process manual available in mid-February. Which will allow people by the month to read it, comment and comprehend it. We used the NISP working group as a point of records for industry to get comment and feedback on the process manual. We already completed that, because we were scheduling to do that in October. Probably in late December, early January, we will use the working group to send out what is going to be the final draft for one last comment from industry, some of our government stakeholders. As always, any information we have on the NISP risk management framework process and our eMASS process falls under our dss.mail/ourmap.

I don't know if we can go down and see it. One of the things that we are working on within the working group is a proposal systems initiative. We've got a lot of feedback from industry on the ability to get proposals systems authorized and up and running quickly to work with the speed of business. We've asked our industry partners who's [2:11:04 inaudible] a couple of different items. Ways, so we can look to expedite this. Industry owes us some feedback by the end of this month through the working group.

We've been working with the other CSAs on this also. I know that currently we've been working with the daft CIO. On this effort, we've been working with the CIA, their industrial security. Folks have a very good proposal system template. We're not going to try to reinvent the wheel. We're going to try take best efforts that people have already done and come up with a more consistent way of having those be submitted throughout, from industry, throughout all the folks with accreditations so that we can get those done on a little quicker basis. That is our big top topic from the working group.

Let's see, maybe it will go maybe we won't. My last slide is to talk about the metrics. For those of you from industry who were around that the industry stakeholders with DSA [2:12:17 inaudible], just a little bit about the DSS metrics. We are measuring workload in resources currently for our senior leadership both in the field and at headquarters. The idea of being that, where we're doing it by regions, is to figure out where we have the most workload, where we have the most impact and direct resources to that.

Currently, on a rolling 12 months basis, we received about 450 submissions for classified systems. We are currently producing about 350 authorizations to operate from those systems. About 15% of the submissions we received, we return back to industry for corrections of the plan whether it's lacking some detail or information. Just a little on their 10% of the overall systems that we received, are either denied by DSS straight away or cancelled by industry so that reflects some of [2:13:17 inaudible].

I could have shown you is that, we receive bubbles and receive it attempts that to leverage band with. In northern region, we had a gobble of work. In the capital region at DSS, we had some availability of resources. We are in the middle of a 12 week effort of sending post in the capital region, to the northern region, to work down that bubble.

We are using our current inventory of plans that we're reviewing. We're also looking at what's coming due, what things are expiring, the next 90 and 180 days, so we can do some workforce planning. They're subject to your questions?

Mark: Any questions on the phone for Karl?

Tania: No questions on the phone.

Mark: Okay. Thank you so much. Greg?

Karl: Thank you sir.

Mark: You're welcome Karl. Thank you.

Greg: Sir, I'll go see my time, because it's really a summation of everything that's been talked about already from the SEADs to the other things. The interest of getting us stats and whatnot, I'd suggest we move forward.

Mark: I accept that. All right. Move into the statistics part now. On the personal security clearance performance methods. We'll start with Olga Delgado, ODNI.

Olga: Hi, can you hear me?

Mark: Yes.

Olga: Wonderful. Hi, I'm Olga Delgado. I'm just going to provide an overview of where we stand with the ITs and DSSs security clearances at this time.

The data and the sec next line, we're on slide two, really identifies security clearance timeliness processing for contractor cases. At the data for industry, for DOD is provided by OPM and IT contract data is provided by the following agencies; CIA, BIA, FBI, NGA, NRO, NSA and the Department of State. The timeliness data is being provided to really report the length of time that contractor cases take, not contractor performance.

We don't account for pre and post case works. Unless, otherwise testified into the initial secret data, is a combination of legacy investigative type to align with and also, the tier three investigations.

Next slide; this slide three highlights, the timeliness methodology and evolution. You could see as how this has transformed since 2004. We're currently using the methodology established in 2012. We're currently in the process of evaluating what elements should or should not be changed and modified. This is a part of the trusted workforce 2.0 effort.

Next slide; slide four, highlight by quarter the average days of the fastest 90% of reported clearance decisions made for the IC and DSS. In comparing FY18 quarter three which is the orange bar and the FY quarter four which is the purple bar. If you take a look across the spectrum, you'll see for secret confidential cases, there was a slight increase in time. If you take a look at the top secret cases, you'll see a slight decrease between quarters three and four. Then, of course for PR, you'll see a slight increase there as well.

I do have a little caveat here on this slide. This data is all inclusive. However, we've only included a summation of two quarter three. We are still missing a few submissions from agencies to complete quarter four, so that get back to that item highlighted there.

Slide five; speaks to secret clearances for the IC and DOD. If you take a look at that as well between quarters one and quarters four, you'll note several differences. If you take a look at quarter one, it took 31 days to initiate an investigation. Currently, in quarter four, it's taking 39 days. To get after this, we are encouraging both Industry and executive branch departments and agencies to assist with that process to ensure timely submission of investigations.

For those that having contacted the same Q-four, your support and giving after that processing come to final decision phase. Also, if you take a look at quarter one and quarter three, you'll a slight reduction in these.

Next slide; projects, here we have the highlights that speaks to top secret clearances of FBIs and tier five. Again, if you take a look down for quarter one and four, the initiation day is we're doing better for top secret clearances by few days, but on the top end, you'll see a slight reduction of days as well in terms of processing. We're hopeful that we'll continue to see that defined.

Moving on to slide seven; periodically investigations as well as tier 5. If you take a look and compare quarters one and four, quarter one for initiations, it took 62 days to initiate a PR. Now, we're down to 42 days. Again, different strides have been taken to reduce these days and to find those decisions to the front to ensure the complete submission of the PR as well. Those are required for work. Of course, the slight increase in day is overall.

Next slide; if you have any questions, feel free to send us an email at secea@dni.gov. That's all I have.

Mark: Any questions for Olga? Patrick Hogan, DOD DSS.

Patrick: I would like to just provide you guys with a year review for FY18. We don't have the numbers up on display. I'll just go ahead and read those through to you.

Due to continued budget challenges, DSS with metering investigations at the end of the year reaching that high of 23,855 cases in August of 2018. We did receive end of the year budget reprogramming, which enabled us to significantly reduce the EQIP front in inventory and end of the year with our smallest inventory on record of 2,980 cases.

Our FY18 metric included more than 253,000 industry case submittals. 95,000 in terms of determinations processed, averaging 20 days on 108,000 knowledge center calls.

FY19 is looking positive. We continue to drive towards the steady state of EQIP submissions, customer [2:21:13 inaudible] and internal report processing. Questions?

Mark: Steve Demarco, DOD CAF.

Steve: I will be giving you the status of the CAF inventory for Industry cases right now. As you can see from the slide here, the inventory has doubled to the end of the third quarter. That's due to a number of factors. The factors are; NBIB has put additional resources in processing or investigating their cases. That has caused a surge in the number of cases were getting in. They have also implemented

some additional measures to close their cases out. Again, that's also causing the surge, that's one reason.

We'd had in just issues as far as the communications between NBIB and DMBC. Making sure we're getting all the cases in. They do the reconciliations. They find large numbers of cases that were not adjusted the way they were supposed to work with DMDC and NBIB. We get those cases and they put them in a large block. It can be tens of thousands of cases. We're not coming in a consistent level as well.

I had the longest pulling [2:22:52 inaudible] for us right now is network issues or actually application issues. DSS or DISS, I should say, is not operating optimally for us. There's a lot of challenges with the workflows in DISS. We are seeing a reduced capacity in putting cases through the system. We are working with DMDC every day for change request to try and get those workflows to be optimized are extremely rigid. We just can't process cases as quickly.

While we work with DMDC on their changed request, we are also looking internally as well. We are looking to optimize our own internal processes. We are looking at potentially restructuring the way our divisions are set up. We are going through and trying to change our processes to work with the system. It's better having the system work for us.

Now, it's set as backwards, but that's where we are. That's what we're doing to try and change the situation. Fortunately, the trend you're seeing here are going to continue to Fiscal year 2022. We expect our backlog to grow tremendously over the next few years. We are programming for additional resources, but as usual, resources take time to get. We have the program for them. They have to get approved. We have to go out and hire them. Then, to train a fully functional adjudicator takes us two years.

We have a lot of obstacles. We're working to overcome them every day, but that impacts our inventories, which will go up. Our backlogs will go up and our timelines are going to grow. You can see here in September, we were still... while we are above the mandated timelines, we were actually not doing so bad. The other good news is the industry portfolio is the healthiest portfolio right now within the CAF. That's a good news story, but that story is going to progressively get a little [2:24:53 inaudible] as we get more work in.

When we shut down the legacy DISCO CAF, we had some issues with the document migration. Those have been fixed. Now, we can request those documents. We have [2:25:13 inaudible] issue again

with our network [2:25:14 inaudible] to see your application [2:25:16 inaudible].

We do not have access to legacy CAF any longer. Anytime we do have missing documents, we have to put a request in. It is a button. DMDC has been pretty good about getting those in within 24 hours.

Again, we continue to work in partnership with USDI, DBD, NBIB. We are trying to set up successfully to work these challenges but it is going to take us some time to work through this inventory, but we will work on it. We'll continue to get reports to let you know where we are on this. Other than that, I'm just going to open up for questions and see if I have anything.

Mark: We thank you for your candor no matter how depressing.

Steve: It's a story. Not necessarily good news story.

Mark: That's true. It's a story. Questions? Thank you, Steve. That was good.

Steve: [2:26:18 inaudible].

Mark: I appreciate that. Again, bleak but true. All right. Perry Russell. [2:26:28 inaudible] op Perry.

Perry: Good morning. Thank you very much. This is actually a brief good news story, because DOHA does not have a backlog. It depends [2:26:39 inaudible] POs obviously is the authority for denials or revocations in industry.

Right now, we have less than 900 active cases NS Included among those are the [2:26:50 reps] 830 cases [2:26:52 inaudible] current in legal reviews and current in getting cases [2:26:57 inaudible] hearing. We recognize that as over the summer, there was authority for granting the ability for NBIB to close cases short and with the introduction of much larger populations in the continuous evaluation. It is likely that the work load hitting the DOD CAF is going to, as we said, continue to increase.

The good news for us at DOHA is, one; we're ready for whatever increases coming at us, because we do not have a backlog. The other good news is that, historically, over the last 30 years, the number of denials and revocations that have come out of either the clearance application process or background investigations has been less than 2%.

As I've often said, the purpose of the personnel security process is to look for the needle in the haystack the bad actor that after who either is insider threat or it's somebody who should not have

eligibility for access the classified information. As long as we don't make the haystack bigger, the number of needles we're catching is going to remain relatively constant.

I am optimistic, especially because we're working with the DOD CAF. Whatever problems you've heard about with DISS, they are not affecting us at DOHA, because we work with the task, to work around that with all our due process cases directly from the CAF immediately. They're [2:28:23 inaudible] with no change to going cases. In that regard, industry is not only the healthiest portfolio at the CAF, but DOHA is healthy in how we're working with capital handler.

Mark: Any questions for Perry? Quinton?

Quinton: Perry, this is Quinton. In your process, the CAF is not going to be out of trouble until 2020. Do you foresee to your organization [2:28:59 inaudible]?

Perry: Well, DOHA receives what we receive. I would say it would be impossible to not have some of that, but as of right now, because of the way we're working with the CAF on getting the statements. The statements are reasons to get a legal review of the [2:29:19 inaudible]. We have an early warning system there, because we can see when we see an uptake in graft statements of reasons that tells us that we're going to be seeing more of [2:29:29 inaudible].

While some number of people after they get their statement of reasons may decide to not go forward with the process. It's still a good early indicator. In a sense, the statement of reasons are like canary in the coal mine. We have not yet seen a major up-take in that. When we do, we'll know that we need to look up for what's coming next.

Mark: Anyone else for Perry? [2:30:01 inaudible].

Perry: Thank you very much.

Mark: Thank you. Okay, now we move in to our open forum discussion, which my favorite part of the show. Anyway, please grab a mike and say what you want to say.

Greg: I'll put in a quick plug. December 6, right here in this room, ISOO is having a 48th anniversary, half-day celebration. The primary focus is information security. We'll have all the living ISOO directors present for a panel, as well as a key note speaker. You're all invited. You can go to the www.archives.gov/isoo or you could email Alegra A-L-E-G-R-A alegra.wooder@nara.gov, if you would like to attend. It will be

in the morning. We'll have some cake, coffee and punch afterwards. It should be a good show.

Mark: Keith?

Keith: This is Keith, NISPPAC. I want to get back to... just quickly, a comment the chair made earlier before we broke with regards to the relative utility of this group. I feel pretty strongly that this group has a very important function to perform for industry and US government. The primary purpose of that function is transparency. We have a governance problem right now, with regards to how efficiently we tackle the issues, but the most important thing we do, when we get together quarterly is to be transparent with each other **[2:31:39 inaudible]** all solutions that have been official both for the government and for industry.

[2:31:44 inaudible] that we're not doing that right now, we can fix that. It's our choice to fix that. I want to just attest to the leadership we have at the table in their ability to address these issues collaboratively and productively for industry.

Mark: Well said. Yes, I agree. Okay, there's no point in keeping us here on a snowy day. I assume it's still snowing. I don't know. Anyway, first NISPPAC meeting for 2019, tentatively, the date is March 13th. It was in our national archives. We're going to try to acquire this day in July and November. Expect to have dates lined up in the next two weeks. You can imagine the reservations on this theater or top.

As mentioned earlier, announcements are made in federal register about a month before each meeting. That's where you can always turn to. About that, without any further comment--

Male Speaker: Just one thing. We know we have a few hiccups today. We appreciate your feedback. We would like to be more efficient to this as best possible. Feel free to send me an email or Robert Tringali or Carolina Clink.

Mark: Thanks. Please drive safely on your way out of here. Meeting adjourned.

Female Speaker: Nicely done. I thought your staff did a great job.

Mark: Thanks.

Tania: Thank you to all those who joined today's session. This session has concluded. You may disconnect.

[END OF TRANSCRIPT]