NISPPAC 3-14-2018 audio

BRADLEY:

OK, shall we begin? One of the complaints last time was the meeting was too long so we'll try to move it along quicker this time, all right? So, welcome to the 58th meeting of the NISPPAC. Due to comments at last NISPPAC the three-hour meeting was too long. We've adjusted the slotted time, this time at two and a half hours. So we'll try to stick with that. We'll be having a five-minute break halfway through or you're welcome to take a break obviously at any time you wish. The rest rooms are down the hall. This is a public meeting. It is audio recorded. For those of you here in the room please be mindful that we have people on the phone through teleconferencing capability. Microphones around the tables can be repositioned in front of anyone who wants to speak so that anyone can hear. If you don't use a microphone others in the room and on the phone are unable to hear what you have to say. A floor microphone is also here in the room for anyone not sitting at the table, right there. Presenters can use the podium at the front of the room which is over here to my left. Before speaking, and this is critical because we have a transcript for this, please identify yourself each time so that information is captured in the audio recording of the meeting. So when we do the transcript we'll be able to

attribute the right comments to the right people who spoke.
Before we get to the introductions I'd like to quickly review
the role of ISOO in the National Industry Security Program and
then discuss the importance of the NISPPAC Federal Advisory
Committee Act, the FACA requirements. Per EO12829 ISOO is
responsible for implementing and monitoring the NISP formally
via the NISPPAC and its working groups and informally via
ongoing communications with government and industry. ISOO
strives to maintain an ongoing dialogue with both groups. If I
had a uniform on it would be zebra striped and I'm kind of the
umpire or the mediator.

As most of you are aware, the NISPPAC is a federal committee
comprised of government and industry members. As a federal
committee it is subject to the FACA. ISOO as the NISPPAC chair
must ensure compliance to maintain the viability of the
committee. One major requirement of the FACA for the NISPPAC is
the annual submission of financial disclosure statements by
government NISPPAC members to rule out potential conflicts of
interest. We appreciate your cooperation in meeting this
requirement and just recently completed this year's submission.
We've got some new government NISPPAC members and I want to also
thank some of the ones who are coming off. Let me welcome our
newest ones. Wait a minute, I've got something else to do.
However, I'd like to first recognize Ben Richardson, our primary

DOD representative. This is likely his last, right? Here with us?

RICHARDSON:

Possibly, yeah.

BRADLEY:

Ben's going off to a new work assignment. I might brag about it just for a minute. He's going to the War College. Ben has not only been a great colleague, but I've always appreciated his style of management and also his cordiality. He's a real professional and also, more importantly, a real patriot. So anyway I'd like to (applause). Our newest government members are Richard Townsend, primary member Department of Commerce. Richard here? OK. Good way to start, right? (laughter) Kishla Braxton, alternate member, Department of Commerce. She here? Good way to start, OK. Christopher [Hylig?], alternate member, Nuclear Regulatory Commission. Christopher? OK. Tracey Kindle, alternate member, Department of Energy. Thank God, OK. (laughter) Welcome. Our outgoing government members are Thomas [Peddon Breadmore?], Department of Commerce. No? And William Ewald, NRC, Nuclear Regulatory Commission. Mark Pekrul, NISPPAC alternate member for the Department of Energy, ended his service at the end of this past August. We welcome

all of you and thank you for your willingness to participate in this committee.

Now, beginning at the table I'd like each person to introduce him or herself and then we'll have those on the phone provide introductions. We'd like to ask those on the phone to follow up with an email to Robert Tringali at Robert.tringali@nara.gov. So let's go around the table. Mark Bradley, I'm the director of ISOO.

SUTPHIN:

Michelle Sutphin, industry.

PANNONI:

Greg Pannoni, ISOO.

WRIGHT:

Natasha Wright, Department of Energy.

MINARD:

Keith Minard, Defense Security Service.

LADNER:

George Ladner, CIA.

MCGARVEY:

Dan McGarvey, industry.

LOWY:

David Lowy, Air Force.

LYNCH:

Steve Lynch, Homeland Security.

STRONES:

Martin Strones, industry.

TAYLOR-DUNN:

Zuddayah Taylor-Dunn, NASA.

WOODARD:

Alegra Woodard, ISOO.

AGHDAM:

Laura Aghdam, ISOO.

TRINGALI:

Robert Tringali, ISOO.

WILKES:

Quinton Wilkes, industry.

HARRISON:

Anna Harrison, Department of Justice.

ARRIAGA:

Dennis Arriaga, industry.

PHELAN:

Charlie Phelan, [NGNP?].

KEITH:

Dennis Keith, industry.

BROWN:

Shirley Brown, NSA.

HARNEY:

Bob Harney, industry.

POULSON:

Kirk Poulson, industry.

BAUGHER:

Kim Baugher, State Department.

KERBEN:

Valerie Kerben, ODNI.

RICHARDSON:

Ben Richardson, DOD.

BRADLEY:

OK, let's go to the phone. Where exactly is the phone? Is it -
- OK, you got it. Who would like to start on the phone first?

BRADY:

Dennis Brady, Nuclear Regulatory Commission.

BRADLEY:

Next.

HYLIG:

Chris Hylig, NRC.

PLAY:

Glen [Play?], Navy.

JARVEY:

Vince Jarvey --

KYSER:

Lindy Kyser, clearancejobs.com.

BRADLEY:

Got to be a better way to do that.

JARVEY:

I think we stepped on each other. Vince Jarvey, industry.

KALEY:

Katherine [Kaley?], industry.

KELLER:

Trish Keller, industry.

RAINER:

Diane Rainer, industry.

FANT:

Liz [Fant?], industry.

DOCKINS:

Michelle Dockins, industry.

ZARELLI:

[Ethos Zarelli?], industry.

YEN:

Jocelyn Yen, GAO.

BRADLEY:

Anyone else?

BURNS:

Len Burns, industry.

BROOKS:

Mark Brooks, DOE.

BRADLEY:

Anyone else? All right. Greg Pannoni, my deputy, will address

some administrative items and will also cover the status of

action items from the November first, 2017 meeting, right?

PANNONI:

OK, thank you, Mr. Chair. Good morning, everyone. Just a couple of things on the presentations and handouts. They were sent electronically to all the members and to anyone that provided an RSVP to the invitation for the meeting. And for the rest, you will be able to get those materials on our website along with the final minutes of this meeting in approximately 30 days from today's date. Also, for your information NISPPAC meeting announcements are posted in the Federal Register approximately 30 days prior to the meeting.

Moving on to old business there were a few items. I'll cover those quickly. The requirement for government members to submit annual financial statements, we did finally get all of those and glad to say that action's been completed. Next was DSS to inquire on the capability of NISS to have best practices section for users. DSS is going to provide follow-up during this meeting for that. Next was DMDC to inquire on the capability of DISS to have a best practices section for users. DMDC to provide a follow-up for that during this meeting. The last item was DOE to determine releasability of the DOE/DOD MOU. DOD is to provide follow-up during this meeting for that one. And that's all I have. Are there any questions?

BRADLEY:

All right. Turn to our reports and updates section of the
meeting. First one, Charlie, will be an update on the National
Background Investigative Bureau. Mr. Charlie Phelan, well known
as the director.

PHELAN:

Thank you. I have my carefully prepared PowerPoints here and
I'm not addressing specifically these PowerPoints here. I do
want to give you -- take care of a couple of things here in my
time. First thing I want to talk about is numbers. Not
necessarily -- oops, that's not those numbers anyway. Not
necessarily the numbers that were up on the chart a minute ago,
but a nurse that I seem to have lost control of probably since
the day I walked in the door which is today 700,000. And the
mythology and the urban legend is that it's 700,000 people in
our inventory and those 700,000 people can't work until we
finish the work on them. Not exactly true. And so I want to
put some numbers around so you have a better sense of what that
is. And as we keep coming back to this meeting and other venues
I will keep everybody posted on what those numbers are, but just
to put it in simple terms, of that 700,000 or so 164,000 of
these are simple record checks. These are things that -- and
some very short fuse inquiries that we're making. These have a
half-life measured sometimes in hours, sometimes in single digit

days, occasionally double-digit days, but they go through pretty
quick.

What's left are those that are -- have some level of complexity,
field work, and that has been the long pole on the tent and will
continue to be until we get this under better control than we
have it right now. But again, to give you some numbers, of
what's left 209,000 of those are periodic reviews of either tier
three or tier five, occasionally a tier four periodic review.
And so these are people that are working and not a question
whether they can go to work. It's a question of are we keeping
tabs on them. We, the government, not we, me necessarily. That
leaves about 337,000 initial investigations. Breaking that
down, 230,000 of those initials are tier three, secret --
leading to a secret clearance. I know the question that this is
the NISPPAC, the I being industry, industry will say, "How many
of us are in there?" The answer is about 38,000 industry cases
are in that 230,000 tier three number. Oh, you're pointing to
chair. I thought you were pointing to me.

BRADLEY:

Excuse me. There is an extra seat if you'd like the seat.
There's a lady standing. Sorry, about that, Charlie.

PHELAN:

OK, I thought you were giving me the high sign like get out of here. (laughter)

BRADLEY:

We know it's bad.

PHELAN:

Go sit in the corner, Phelan, yeah. And then on the tier five side it's about 107,000 initial tier fives, 27,000 of those are industry cases. So of that total 337, again the question isn't how many of those people are not working, not all of them are not working if I can put it that -- that's two double negatives. I think, and I'll defer to the folks from DSS for more specificity, but I think the number -- and from DOD for specificity -- the number of interim clearances in the DOD world right now is about 170,000. So you take that off of that total and that still reduces the number of people who can't work. I will tell you that I don't know the precise numbers as to where they are, but I would conjecture that the vast majority of those interim clearances are in the tier three world, not so many of them in the tier five world, if any at all. But so this is, again, in the end this is still not a good number that I want of people that are in the inventory, but it is not quite as desperate as a collective as it is. But I am mindful of two

things. One is those numbers that are sitting out there, I

won't go back and dissect them all, I'm not either proud or

happy about what those numbers are and we are working to get

those numbers back to where they need to be, understanding that

this is an important thing to get folks and programs working.

So I think I will let those numbers stand for themselves.

How we're dealing with this, I would put it in the sense of we

are attacking this problem on three fronts. And you've heard

some of this before, but I'll give you some updates. Number one

is we needed to rebuild the capacity that we lost back in 2014

to do the investigations, the investigative capacity. I'm happy

to say that as of today we are at a little over 7,200 humans

within our staff and contract population that are doing field

work. That is about where we were three years ago. And three

years ago that was sufficient to keep us steady. We are keeping

steady right now although the top end is not where the

steadiness is where I want it to be, but I will tell you that's

not enough. It's not enough on two fronts. It's not enough

folks to deal with the changes that have come across in

investigative standards since we've lost the capacity and it is

not enough to deal with what will be attrition, with what will

be with some transition issues we'll talk about in a minute.

But we have told both ourselves and our suppliers they need and

we need to keep on hiring in that space because it is important

to bring this inventory number down to a much more manageable
level.

Secondly is better use of capacity. We have been -- we're
working within the confines of the processes that have evolved
within our organization. We need to make smarter use of the
capacity that we have right now. We began a business process
re-engineering study that concluded last year and we are -- the
study itself concluded last year. We are in the process of
executing many of those things. If we had another 35 or 40
minutes I'd go through all of them, but I'll touch on just a
few, not the least of which is defining what those process
improvements are that need to take place and working on the
technical support that is required to make those processes get
better. First and foremost is improving on our field work
logistics and so a couple of ways we're doing this. It's been
government focused now, but we are working with industry,
particularly through the industry groups AIA, NDIA, PSC, and
ISWG to some extent, to do what we have been doing with some of
our government customers more directly for the last year or so
which is to centralize and prioritize case work both in terms of
surging teams to various areas -- we started with the Department
of Energy a little over a year ago and are continuing that. In
fact, there's one that's kicked off I think in the last week or
so with the Department of Energy to surge into areas where there

is a crucial mass of cases that we need to close and that allows

us to better use the investigative time that we have and get as

much done working in that space, collecting the people that need

to be investigated, the people that are the source interviews,

and getting them in one place. And we've found that there's a

tremendous increase in productivity amongst the agents that are

doing the investigations when we get them into that environment.

The other is hubbing which is even more complex. We've had some

pretty good successes recently. I'll single out the Air Force

for one that we finished in Wright-Patterson Air Force base that

had a huge impact on the number of cases that we had sitting in

the inventory at Wright-Patterson. We also then moved on down

to San Antonio to do all the work down in San Antonio. That is

underway or soon to conclude. And then, again, in a government

focus but we'll still include some industry representation, we

are kicking off later this month, probably as early as next week

but no later than the end of the month, a hub activity at

different locations down in the Tidewater area to clear up a lot

of the work that is building up down there. So I think this is

-- what we have seen so far is it is making the agents more

productive, it is getting things cleared out faster and we're

going to work -- continue with our government customers, working

more with the industry customers, to do some of this. We've

identified five locations. I won't identify them here, but five

geographic locations. I'll make it clear that it is not
companies we're looking at, we're looking at geography to pull
things together and clear up work in a geographical area where
there's a lot of that critical mass.

And then within all that we want to also find more ways to
efficiently collect important data. Not interviews but data.
And so how do we verify employment, how do we verify -- how do
we do criminal records better, how do we get more and more stuff
electronically that today is not necessarily easily available?
How can we get it more electronically to free up the time of the
investigators to let them do what we really hired them to do
which is to have that conversation with subjects, to have that
conversation with references, and have that human interaction
where that human interaction is necessary and let data get
collected in a better fashion.

Saying all that, everything that -- the process that we do today
is driven by policy and I'd like to say that I can unilaterally
change policy but they won't let me. But I will tell you if you
were paying attention to the congressional hearings last week
the DNI rolled out the notion, and I don't know, Valerie, if
you're going to talk about this or not, of trusted work force
2.0 which literally kicked off day before yesterday over at the
ODNI and it was sponsored jointly by the ODNI, the DNI, and by
the suitability executive agent, the director of OPM, along with

the PAC principals and got about 40 folks in the room and we changed shifts on day one to day two, but it really is to start the process, to rethink a trusted work force. I have not yet broken the news to Margaret Weichert who just took over as the deputy director of OMB. She was wondering why we're not on trusted work force 27 at this point as opposed to 2.0 and I'm going to let somebody else break the news to her that trusted work force 1.0 was in 1947 (laughter) so we'll let her figure that out.

At one point Bill [Evanina?] said that -- as he was introducing the topic he said, "Charlie is looking for answers." My reply to that is I already have the answers. The answers are federal investigator standards. The answers are tiers. The answers are somewhat prospective, just go do social media checks. I have all the answers. I'm not sure I like all the answers. What we really need is the questions and go back and ask the questions. We have to fundamentally go back and ask from the very beginning what are those indicators that will tell you that a good person is starting to go bad or that they already are bad and you can't trust them? And then build that back into the process. This cannot be, as we have done in the past, a tweaking exercise where we continue to add things in or maybe pull something out. It'll be nice and we can do some quick fixes perhaps, but this really has to fundamentally go back and say in 2018 and for the

foreseeable future what are those indicators going to be that tell me, and tell an adjudicator more importantly, that somebody is not to be trusted or has a propensity not to be trusted, and then from that point forward how do we continue to understand whether that person is still in a trustworthy capacity?

So you know, I aspired to be an architect at one point. Didn't work out for me, but one of the basic tenets of all that is form follows function. We should not be rewriting the policies and the processes until we understand what the heck we're trying to write them to fix here. And you should know from the industry standpoint there was industry representation, fairly broad industry representation, from the various representational groups. Again, AIA, NDIA, ISWG, etc. And the collective message was from that group, in addition to the specific messages they delivered which was good, is we don't want to be complainers, we want to be contributors. And I think the stage is set to have industry be contributors in this. So I am excited about this prospect and I think it's one of those maybe not once in a lifetime but very few times in a lifetime chances we have to do something good here.

And so a couple of things that are dependencies in all of our success and I think ultimately in this ecosystem's success. There is the issue of a transfer of responsibility for the DOD cases back to the Department of Defense and, again, I don't know

if you guys are going to go into any detail about this. I will just simply say it is a three-year plan to transition that over, but that's a three-year plan, not a three-minute plan, and what that means is they're going to keep handing me cases in some volume over the next three years as this goes through. So you're stuck with me for a while if you're in industry. And this is why we're working with you on the hubbing and surging concepts we talked about. We are, everyone in this, involved in this transition is committed to a smooth transition and I would encourage you to hold us to that smooth transition. If you see hiccups you should let us know.

The other dependency is the development of NBIS, the National Background Investigation Services. We've talked about that before in this venue. I think this is more vital to the Department of Defense. It is picking up an activity, but it's not unvital to us. We will limp along with what we have if it doesn't come online when we need to, but it will be a great enhancement to the entirety of this ecosystem to get these jobs done better. So last thing, sort of what's our future look like? What does the future look like? So, putting those last two things aside, I believe that by itself the business process re-engineering and transition that we are going through right now is by itself going to start bending this curve pretty soon and you're going to see these numbers start to drop down.

I went out on a limb at a -- it was not an open hearing, but it was in front of -- actually I might have actually said this in response to a question in the open hearing last week as well, that I believe that by Thanksgiving or at least by the end of the year we're going to see the inventory drop by 15 to 20%. There are some folks that think I'm being pessimistic about that, it's actually going to be more. Some think I'm being optimistic. I'm trying to draw the line in the middle. I'm comfortable we can hit that kind of a number. So I'm looking forward to being able to do that.

I recognize the importance of what our mission is. What is really important for us to recognize and for me to recognize is the importance that we are in support of your mission. If we don't do this right your mission suffers and so we understand that. It's in foremost of our minds and I appreciate both the opportunity to sit here and chat with you guys for a few minutes this morning and our opportunity to be able to help make this be a part of the nation's national security and the trust that this government puts in people that are working in the environment. So I defer if there's any questions.

BRADLEY:

Yeah, right. I mean thank you, Charlie, for those -- that

update and thank you for coming. Please, anybody have any

questions for Charlie? Michelle?

SUTPHIN:

Michelle Sutphin. Charlie, I wanted to first express my thanks.

A lot of us in the room have had the pleasure and privilege of

working with NBIB on this transformation and suggesting ideas.

My question to you is, as DSS transitions to the investigative

model are you planning on sharing some of these new best

practices that you have learned from us with them?

PHELAN:

No, not at all. (laughter) It's proprietary. You told me

that, Michelle. (laughter) No, absolutely. In fact, we sat

down with DSS and with several members from the military

services maybe three weeks ago or so and literally went through

all of this BPR. We spent about three hours in a room with them

going over the process and our plan is to engage with them along

the way. There's no secrets here. We're protecting secrets,

but this is not a secret to protect. And our goal would be to,

as we get more and more involved with industry, because DSS is

the front end for most of our industrial work they've got to be

deeply involved in this as well. Absolutely.

SUTPHIN:

Perfect, thank you.

BRADLEY:

Anyone else for Charlie? My seatmate here has a question here.

KEITH:

With regards to the --

BRADLEY:

Introduce yourself please.

KEITH:

Dennis Keith, industry. With regards to the 15 to 20% expected

drop that you have by Thanksgiving, is that across the board or

is that in the records checks or is that in the PRs or the

initials, equally spread?

PHELAN:

So the short fuse stuff will probably stay at the same level

because it goes in and out pretty quick. So I would expect that

15 to 20% to drop off mostly in the cases that have field work

involved. And probably the ones that will have the greatest

impact on that 15 to 20% will be in the tier three world, but it will not -- they'll be missing out of the tier five world as well.

KEITH:

One follow-up please. With regards to the hubbing concept, about 65,000 industry members are awaiting their initial clearance. Will those cases be prioritized ahead of PRs?

PHELAN:

I can't unilaterally do that. We will work with the sponsors of those cases and say, "And what do you want to prioritize?" In fact, we do have a biweekly meeting with the Department of Defense within the cases that they have to ask them which ones would you like to put ahead, which ones -- and so that's sort of an in-flight prioritization that they can do. And then other agencies we work with have the same opportunity in a more aperiodic basis as they call in to try to reprioritize. So I would it to the department to decide -- to make those decisions about what they want to prioritize or not, but our focus, and I think everybody's focus, has been on getting initials to the extent that we can. Not to the demise of periodic reinvestigations, but initials are what folks want to get done.

That's the first and last comments I hear is, "I need to get

people to work."

PANNONI:

I actually do have a question too, Charlie.

PHELAN:

Yes, sir.

BRADLEY:

Identify yourself.

PANNONI:

Greg Pannoni. (laughter) Is it fair to forecast if the

projection that you gave is a 15 to 20% decrease in the overall

backlog, would that correlate to roughly a 15 to 20% decrease in

the timeliness of these cases [fastest?] 90%?

PHELAN:

So yes and no. One of the byproducts of clearing out a backlog

is, you know, these cases don't get counted until they've

cleared it out. So you're going to find some that will -- there

will be a period of time when the numbers you see reflected

there will show an increase. We need to find a better way to

say OK, let's look out over months starting from -- and working

backwards from today and say what happened to those cases that

submitted today or last month or the previous month? And we're

doing that and we're seeing better numbers. But that top line

is going to show something -- as old cases come out it'll

actually show it going up.

BRADLEY:

Anybody else for Charlie? Charlie, thank you.

KYSER:

Can I --

BRADLEY:

I'm sorry.

PHELAN:

Question on the line.

BRADLEY:

Is that somebody else?

KYSER:

Yeah, can I (inaudible) question now?

F:

Can you say your name please?

KYSER:

This is Lindy Kyser on the phone. So my question is about not the backlog, but just what you spoke to, the processing times. I think we overemphasize the backlog and as it pertains to industry the issue is that the top-secret timelines continue to go up. You kind of spoke to that a little bit. Why aren't we seeing -- we're seeing the secret processing times at least stabilize or improve. Why are the top-secret processing times literally going up by 30 days in Q1 of 2018? Do you have any specific insight into that?

PHELAN:

You know, Lindy, that's a good question because I went back and asked the same question when I started these numbers and they keep seem to be going up. Because those numbers are not the same as the overall government reported numbers for any of those tiers. They're higher in the tier five category. And the best I can determine without completely pulling out 500,000 cases and saying what the heck's going on here is that it is a matter of prioritization and who prioritizes what. And what we find on

the industry side is that the number that get prioritized is smaller than the number that get prioritized on the civilian side and on the military side. And that's the only number I can -- only thing I can point to that seems to have any dramatic effect on that number. There are probably some other sort of things in there. The other thing that has been proffered, and I have to do some more science on this to see if this is really true, is if you look at the average 18 year old who is entering the military service for the first time, their history is relatively short, particularly the history that we can actually cover because we're not going back seven years when you're 18, as opposed to a 35 year old engineer that has just signed on with Lockheed Martin and they're in for their first clearance. They're going to have more history. That case is going to take a little bit longer. But I don't have a good handle on how dramatically that affects the level of effort in the case because, again, that to me should be just a single digit day problem, not a 30-day problem. So I'm not sure I answered your question, Lindy, but that's about as much as I can come up with in the quick research that I did.

KYSER:

I think that would be an interesting nugget because I think the times industry is suffering a lot more with this than government

because the government time seems to be at least improving

anecdotally from I get and the industry is getting progressively

worse. I would love for Congress to start asking about that and

caring about that a little bit more. Forget this backlog

number. I don't care what that is.

PHELAN:

I appreciate that, Lindy, because you're right, I think the

backlog number has taken too much of a front seat in this

conversation and it really should have been all along. And I

think the thing -- nobody would care how big that backlog is if

I was delivering cases to you in 40 or 80 days as I'm supposed

to be.

BRADLEY:

OK, anyone else for Charlie before we go to the next speaker?

OK, Charlie, thank you again, appreciate it. We're now going to

turn to Michelle Sutphin, the industry spokesperson, to give us

an update on industry.

SUTPHIN:

Good morning, everybody. We've been very busy watching all of

you guys work and trying to catch up. So we're going to talk

about the NISPPAC MOU membership and then impacts of policy

checks as it pertains to industry. Next slide please. Our

NISPPAC industry team is staying the same. We have not made any

changes since our last meeting in November. Next slide please.

We do have one change for our MOU members and it is now Kathy

Pherson is our INSA representative and she is here today.

Kathy, you are somewhere. Here you go. Hi, Kathy. Thank you

for joining us today. So she is our one change. Next slide

please. As far as our overview on what industry is concerned

about, really this has not changed from the last meeting and

probably even the meeting before that. We are just focused

right now on the vast amount of change that keeps hitting us

fast and furious and we are just trying to ensure that we

understand what all of the policy changes are and that we can

implement accordingly back home in our corporations. We also

are of course concerned about the growing backlog of the

personal security investigations and long lead times, but it has

been good to be working with NBIB and working through that with

them. We have seen some changes, especially in the interim

timelines, so thank you to [PISMO?] and NBIB for that too.

We are definitely willing to be responsive to all of these new

initiatives. We just ask we have enough lead time and that

things are clearly communicated to us so we can adequately

prepare. Next slide please. Yesterday industry met with DSS

for a few hours in the DSS stakeholder meeting and we received a

very good comprehensive update on DSS in transition from Gus
Green. One of the things that we were able to finally see is
how the DSS in transition is going to start being implemented.
We have learned that about 60 companies are going to be going
through the full DSS in transition review this year so we will
be very eager to be understanding the outcomes of how that works
with those 60 companies and if they are able to implement their
TSPs in a timely manner and what types of concerns will come out
of that. One of the things with DSS in transition that we're
going to also be continuing to keep an eye on is the impact it's
going to have on smaller companies and if they're going to be
able to handle all of the new regulations being put upon them
and if they're going to have enough time in house for their
subject matter experts to participate in DSS in transition. And
also, we are going to be keeping a close eye on how things are
going to be recommended that are outside the scope of the NISP
purview and how we are going to come to a satisfactory
resolution on anything that may be suggested.
Next slide please. Again, clearances, clearance reform, the
transition from NBIB to DSS. We did get a briefing yesterday
and that will be handled in a phased approach starting with
secret periodic reinvestigations and continuous evaluation. So
again, we're going to be monitoring that to make sure there's a
smooth transition. I think one of the big concerns that

industry has isn't necessarily who's doing the investigations, but is the mission properly funded and are we having enough timeliness during the transition. Also too with DSS and NBIB running in parallel for a significant amount of time we are curious as to if there's going to be enough investigators to go around for everybody. So we will be looking at that too. Next slide please. Another new business is small business. So this is a new topic we are bringing up this NISPPAC meeting. We have not addressed this last NISPPAC meeting. The NCMS security consultant working group put together and submitted a white paper very recently to DSS, and in all fairness to DSS we did not give them sufficient time to review that white paper for this meeting today, but we do want to bring up the topic. And the topic is this. Small businesses are starting to have a lot of new policies and procedures and regulations levied upon them. With insider threat and [state 100-171?], DSS in transition, RMF, clearance delays, and CUI it's becoming harder and harder for these mom and pops to continue to keep up with all of these clearance and security policy changes. It's hard enough for a company like mine at BAE to do this, but for the little guys who the FSO might also be the CEO or the FSO may be the receptionist, these things are much harder for them to implement because they don't necessarily do this as their 9:00 to 5:00 100% job. So what we are asking is that DSS take a

bigger look into how security consultants and security service

providers are assisting these small companies. We have seen

that it hasn't necessarily been handled consistently throughout

the United States in how security consultants are permitted to

participate in reviews and how security service providers can

handle things such as JPAS accounts and such for these small

businesses.

So these small businesses are going to have to rely very, very,

very heavily in the next upcoming years on these providers and

we just want to make sure that they're in alignment and that

they can continue to work. Otherwise there's concern that our

supply chain may start dwindling as the smaller companies start

to voluntarily relinquish their facility clearances and we are

also concerned of a counterintelligence issue if foreign

entities start purchasing these smaller companies with key

technologies who have relinquished their FCLs because they can't

afford to compete anymore. So that's one of our big focuses

that we're going to be talking about. Next slide please.

New business with systems. So lots and lots of changes with the

systems. I know we're going to be getting a lot of updates

today on these items so I'm not going to talk about a lot of

this in detail. NISS is going to be an official system of

record sometime soon. We still have a lot of industry that

doesn't fully have access and they're not able to get their PKI

cards working properly. So we are hoping that we don't go live
as the official system of record until we can work through those
kinks. With the DISS system we still really are going to be
emphasizing that we need to have available training for both
industry and government. As of right now there is not a
consistent training module available that encompasses everything
that they need to know in order to use the system from soup to
nuts. We're also concerned that starting in May DISS will go
live and we will be submitting SF312 submissions and using it
for RRUs. We're a little concerned about the mirroring and the
two systems mirroring each other as well as facility security
officers and security professionals being able to use both of
those systems at the same time and any potential confusion with
that.

NCCS is underway. We understand that there are additional
government agencies that are going to be mandated to come
online. I think you will see industry will start coming online
a lot more with NCCS when we see more of our customers
participating. And then with eApp we are awaiting a go-live day
and NISPPAC is very much interested in being able to see a demo
and provide feedback on that. Next slide. Seeds three and
four. We have gotten the opportunity to review ISL verbiage for
both seeds three and four. We provided the feedback on ISL for
seed four already and we are still collecting information,

Keith, on three and we will be getting that to you and Valerie shortly. Next slide please. We did participate in a fee for service survey a while back, 29, small, medium, and large size cleared companies were selected and interviewed for that. We understand, we asked the question yesterday what the status was on this, we understand that they are still looking into how clearances will be paid for after DSS takes over the investigation mission. Next slide please. Is that protesters I'm hearing? (overlapping dialogue; inaudible) They're not angry at me, are they? OK. (overlapping dialogue; inaudible) Yeah, me they're cheering. OK, yeah. Last slide.

So finally, legislation watch. There's the formation of two new committees that NISPPAC is going to be looking at very closely. The advisory committee on industrial security and industrial based policy. The charter was filed in April of 2017. We heard yesterday from Chris Forest that they are going to be moving forward on that. That is going to be comprised of both government and industry representatives. It's going to encompass multiple areas within security to include NISP but not just the NISP. So the NISPPAC will be looking at that very closely to see how we can help and assist and advise this committee going forward. And then finally we have been looking at and monitoring the defense policy advisory committee on technology that is also supposed to be comprised of both

industry and government in order to share technology and threat information. We don't know a whole lot more about this committee, but we would like to learn more. And I think that is it for my slides. Do any of you have any questions for me? Yes, ma'am, Jane?

JANE:

Jane (inaudible), industry. So we heard about the advisory committee yesterday from the DSS and I was just curious if they considered or potentially to put this on the table of how that organization will work with the NISPPAC. Perhaps they would have a subcommittee as part of the NISPPAC or vice versa so that they could share information more easily and the information would flow more freely.

SUTPHIN:

It's a good point and I'm going to defer to Chris Forest to see if he has a comment on that.

FOREST:

(inaudible) we're still in the process of standing up the committee. All options are on the table right now so I can't tell you exactly how we're going to set that up, but I can tell you that NISPPAC will be represented.

RICHARDSON:

So just to add to that, Ben Richardson, DOD. It falls

underneath the FACA requirements and so before we can do

anything with the committee to determine sub committees, how it

will interact with other committees, we have to go through the

process of identifying members and once those members are

identified and come together then they will make the decision

about how to -- what areas to focus on and how we should

interact with the NISPPAC. We have stayed engaged this entire

process with (inaudible) so we know that if the committee

decides to focus on areas that the NISPPAC either has interest

in or there's potential overlap, we'd want to work with them

very closely.

SUTPHIN:

Thank you. Any other questions?

F:

(inaudible), State Department. I was interested in what you

said about these security consultants because we're seeing that

a lot with our companies and gone are the days when an FSO was a

fulltime employee who lived at a company back in the day many

years ago. And it just seems like a lot of companies are

reaching out to these firms that are helping them and I'm not

one that's -- I'm like, I'm talking to the FSO and that's the

only person I'm talking to, but it seems to me that there should

be some kind of guidance or something to let us know what are we

supposed to -- how are we supposed to deal with these people and

how the companies are because I know the name sometimes and it's

like OK, that's great. Somebody's making a lot of -- a lot of

people are making a lot of money off of helping companies

tackled the NISP at this point in time and I just want to make

sure from a user agent's perspective how we're supposed to deal

with those people as well.

MINARD:

This is Keith Minard from defense security service. One of the

things we have to look at is we have to review the white paper

(inaudible) and discuss with the DSS, but keep in mind that

while we have to find a way to relate and support the facilities

security officers of small businesses they are a subcontractor

to your contractor. So the business relationship is between the

company and the security consultant provider. So what we have

to look at is what are the challenges, what are the issues, and

to determine how to best do that. Because we do understand that

in some cases the logistics person or the CEO or the spouse of

the CEO or somebody is the FSO (inaudible) official and in some

cases they don't have the technical expertise to fully benefit

from the capabilities of putting the right security program in

place. So the consultant or security service provider brings

that to the table for them. How do we find a way to best

integrate those while making sure that the cleared company

itself maintains responsibility for the security program?

SUTPHIN:

And to be clear, in no way, shape or form is industry looking to

circumvent the NISPOM requirements. We completely understand

the facility security officer must be an employee and we are not

looking to change that. What we're looking to do is have the

consultants and the security services companies be treated

consistently and also give them a rule book of how they should

be operating because right now it's very gray area and some are

doing it one way and others are doing it another way. And I

think if we can get everybody on the same baseline and have

everybody treated appropriately we can adequately support these

small businesses to be able to protect national security.

F:

Because it doesn't seem like some of them -- I mean some of them

seem to have facility clearances and we learn about that through

our companies, but some don't which if they're not having access

to classified, access elsewhere company, I understand they wouldn't need one. But it is just kind of a strange arrangement in some ways.

SUTPHIN:

We're not permitted to clear subcontractors either so you have lots of companies, for instance guard services companies, they never access classified but they have to have a facility clearance to provide cleared guards. So we have lots of different areas like that and there's really no clear consistent guidance. So, like I said, in all fairness to DSS we gave them this white paper late last week and we're looking forward to working with them.

BRADLEY:

Anybody else for Michelle? OK, with that I'll turn to Ben Richardson, the executive agent of the NISP. Sir.

RICHARDSON:

Thanks, Mark. So, thank you. Like Mark mentioned, this may be my last meeting here, but it's been fun and who knows, I may come back in the future. (laughter)

F:

(inaudible)

RICHARDSON:

So I want to highlight two quick things off the top. DOD
priorities as it relates to this committee. You know, there's a
lot of emphasis and SECDEF interest in personnel vetting and
critical technology protection. So those are two areas that I
think everybody in this room cares about and is interested in.
As Charlies has mentioned, the transition from NBIB to DSS has
begun. There's a lot of collaboration between the two
organizations as we move forward on this. DSS is really focused
right now on its DOD background investigations, the folks on
secret level clearances, reinvestigations using the continuous
evaluation model. So they're moving forward on that and they're
trying to start that in this calendar year, but as Charlie
mentioned, it's going to be really a three-year phased approach
to this but this is where it'll start.
On the critical technology protection area, it's always been an
emphasis for the department, but in the last couple of years
it's been increasingly important to the department. You can
probably see there's a priority in 2019. The most direct
manifestation of this for industry is probably DSS in
transition, but there are other ongoing efforts across the
department in the counterintelligence and security area that is

focusing in on how we can do a better job of protecting the department's critical technologies and collaborate with industry. As Michelle mentioned, there's a lot going on. This has been a theme over the last couple of years. There's a lot of activity whether or not that's NISP, DISS, NCCS, the seeds coming out. We appreciate this forum and the collaboration with industry. I've said it before that we did a great job of rolling out insider threat. There was a lot of collaboration with industry on that and so this dialogue and communication is the key to being successful in all these activities that are going on between government and industry.

I just want to hit a few items as updates. Many of these items have been hit by Michelle so I'll just kind of hit them wave tops and then open it up for questions. On the small business side, Michelle, I did get to see the white paper yesterday and it was good. I read through real quick and we're happy to work with you on that. I know DSS is reviewing it too so I agree with your concerns both from the security consistency side of things and want to work through those (inaudible) turns to, so we look forward to having more dialogue on that piece of it.

Last November we mentioned the DOD/DOE reciprocity MOU. We have been working on an industrial security letter to provide an overview to industry on that and do expect that we're going to reach out to work with industry on that draft ISL as we move

forward. We will be unable to release the full MOU, but we want
to make sure industry gets an opportunity to see some of the
details on that through an ISL.

Michelle mentioned the personnel security for industry funding
study. We first thank you for your support on that last year.
We did kind of brief that to our internal processes that we're
required to do. As we've kind of gone through that, and I
mentioned this yesterday during DSS's industry stakeholder
meeting, that the guidance that came back from that is to
continue to study it. I don't -- I would say don't interpret
that as they didn't agree with our results or anything else. I
would interpret that as it's a complex issue and there's a lot
going on with personnel security right now. And so putting this
at the forefront of everything else going on is -- continue to
look at that issue as we work through some other minor things
that are going on in personnel security right now, you know, as
we get through those issues and we'll get back to this. So
that's kind of where that stands so we may reengage with
industry as we continue to look at this issue probably this year
and next year.

As for seed three, we are -- we've provided a draft ISL to the
NISPPAC. We continue to work on feedback for that, as Michelle
mentioned. I've mentioned the last time I was here in November
that for seed three we are making sure that we are having a

clear understanding how we'll implement this for government before we implement it for industry and also make sure there's an automated way to kind of handle some of the foreign travel reporting piece of it. So that is still consistent with kind of where we're going with that. So we're looking for how we're going to implement that and some of that is system dependent as we kind of move forward. Ultimately, we hope to capture that through a NISPOM change three. The NISPOM rewrite, thanks for all the support from industry over the last couple of years working on this. Actually, several years working on this piece of it. And formal coordination on the rewrite with the NISPPAC will be happening throughout this calendar year so thank you for that and as we continue to work that piece of it.

Seed four, I think Keith will talk about it a bit more and we mentioned yesterday during the industry stakeholder with DSS that we are working on an ISL for that and there's some language out on the DSS website with guidance regarding the passport and returning the passports and other issues there. So open to answering any questions on that one. And last, the advisory committee, you've mentioned it. That has, it got kind of delayed in what was in the original NDA. It is officially assigned to USDI right now. We do have documentation to assign it to DSS to take charge of this advisory committee. That's what DSS is waiting on right now. That's up at USDI. Once

that's signed out and assigned to DSS then DSS can engage and

start establishing the committee members and then, as I

mentioned before, once that's established they can start

deciding what topics they're going to work on. There was like

five areas, personal security, information security, cyber

security, industrial base issues, and physical security. So

some of those areas obviously overlap with the NISPPAC here, but

there are some areas that may not be -- may not overlap. So

depending on what kind of a focus area and from the time that

this was conceived to the time that we're implementing, which is

probably a two-year difference, some of those issues may have

been shifting so we'll see where this kind of lands and as we

take it forward it's an opportunity again for more engagement

and dialogue with industry and communication. That's all I have

pending questions.

KEITH:

Dennis Keith, industry. Ben, is there any thought given to

being able to share a little bit more with the appropriately

cleared personnel the prioritization of the technologies?

RICHARDSON:

Yes, there's been dialogue on that. Currently the list is at a

TS level which is also challenging internally to the government

because this is kind of a group effort between the intelligence organization, security community, and also the acquisition community, and not everybody, especially out in the program offices, they don't even have secret clearances sometimes, you know, some of these contracting officials. And on the flip side of that even on the security side you can't always get the TS stuff out to the field, right? So we are working through versions of that. It's the aggregation of the list that brings it up to the TS level and so we're trying to figure out how we can de-aggregate it or find some other way to hand it out to both industry and -- you are seeing some of the stuff by the prioritization that DSS is going out. So obvious over time as you see DSS consistently coming back to you with certain technologies you're maybe going to be able to figure out which technologies we are prioritizing.

M:
I would submit too to the group that having some degree of visibility at the cleared board level with industry is a very, very powerful thing to assist the DSS in transition.

RICHARDSON:
Yeah, it's boiled down to about seven key technologies in the top list and getting that down to a level that can be briefed at

the board level, even if it's a classified briefing, is I think

a doable do. So we'll work on that.

HARNEY:

Just as an addendum on that, doing that -- it's Bob Harney -- is

not necessarily leave-behinds, but even if we have the briefings

and get C suite kinds of buy-ins into that I think it would be

applying the ability for industry to buy in --

RICHARDSON:

And we're having a conversation with Miss Lord on the

acquisition side so it's a consistent message both from DSS and

the acquisition community.

BRADLEY:

There was a question over here. Yes, ma'am.

DEAGLE:

Good morning, Jane [Deagle?], industry. So I've been involved

with the DSS in transition for industry groups and the process

has been rolled out to very few contractors so far, those have

been involved in the pilot programs. But we're already starting

to hear some concern from industry on the compilation of all of

this information in one location, identifying their key assets,

what they're doing to protect those key assets, the impact of

the loss or compromise of those key assets. So how is the

Department of Defense going to address those concerns?

RICHARDSON:

Do you guys have an answer?

GREEN:

So right now as a --

BRADLEY:

Identify yourself please.

GREEN:

Gus Green, DSS. This is part of our transition plan. We're

looking at the details of what the IT requirements are going to

be. In fact, we're building out a lateral level repository

where we can collect the information as a temporary measure, but

ultimately we have to build this into our capability for the

National Industrial Security System. So we are building plans

right now to elevate the classification of the data and bring

all that up to higher levels of classification with the tools

necessary to do that. But as an interim solution we're simply

going to have to have a repository on a collateral network where

we can capture the information and consolidate that information and protect it appropriately.

RICHARDSON:

This is Ben Richardson again. We've gone through this with CPI and some other data and this is more of the programmatic side of things where we collect that information in a single database and obviously we can't keep that at a classified level so we do need to, as we aggregate that information, move it up to higher systems.

BRADLEY:

Anybody else for Ben.

PANNONI:

Greg Pannoni. Just for my own clarification, maybe perhaps others, when we speak to the technologies are we DOD centric right now? Are we referring to DOD critical technologies or is this all the technologies?

RICHARDSON:

DOD has -- OSD, Office of Secretary of Defense, and the Joint Staff has come together with a combined list of our critical technologies and that is what we're providing out to DSS, but

we're also providing this to other government agencies to say this is what's important to us, but no, it does not encompass what DHS or DOE may consider critical.

GREEN:

NASA and what have you. OK, thank you. Just wanted to clarify that.

BRADLEY:

Anyone else have a question for Ben? OK. Move on to Valerie Kerben.

KERBEN:

Good morning.

BRADLEY:

She would give us an overview of the seed and what's the latest in the ODNI world on the seed. So please.

KERBEN:

OK, most recently seed six, continuous evaluation, was signed by Director Coates on January 12th. So hopefully our CSAs have received that and it should also have been posted on our public website. So for continuous evaluation that means that agencies

should be implementing this process for their tier five population, the 5% of their tier five population is the requirement at this point, but this is the policy for the whole entire continuous evaluation program. Seed seven is the policy for reciprocity. We have it in informal review right now. It's been out to our security advisory committee members and our next step is to get it from the DNI to OMB for the formal coordination process with departments and agencies. And we are also working on seed eight which would be temporary access. So that will be forthcoming soon too, but again it's in the informal review process at DNI. That's all I have today.

BRADLEY:

Anyone have any questions for Valerie? All right, we're now going to turn to Keith Minard, DSS, to tell us about what's going on in the world of DSS.

MINARD:

Keith Minard, Defense Security Service. First, I'd like to do a few introductions. Mr. Gus Green, director of industrial operations, already spoke briefly. John Massey. Many of you remember Heather Sims used to be the assistant director, deputy director for operations. John Massey now fills that role. Chris Forest, who will serve as the designated federal official

for the advisory committee once we're designated, and last is I've got a new staff member, Alison [Rosella?], that filled one of our -- she's here somewhere. She's moving over from our FOCI operations into the policy office. So I just wanted to make a few notifications first.

Real quick, those of you that are from FOCI companies knew last year we moved through -- we're moving from the ECPs, the phone log requirements, we've kind of finalized that process. We will remove the phone line requirements from individual ECPs at the next updates and for the changes. The next thing is actually insider threat implementation. I know this has been about almost a 22 month roll now. We're following the methodology of the national insider threat task force. The first step we did was move through to identified and implement the core requirements. The insider threat official, the plan, employee awareness training, staff training, and user activity monitoring or in many cases it's audit reviews because of the types of systems we have across industry. It's good to say that we have 99% of companies that have ITPs appointed, 95% have active plans that are certified. This is a good indication on industry's implementation of the core requirements. It's a very positive move forward and it just goes to show you that industry, when we work all together, we can make the right things happen.

So that's phase one. As with like the NITTF is doing at the federal executive branch, now we're moving into phase two. Phase two will take a little bit longer while we develop the processes and procedures to identify and evaluate the effectiveness of programs. So we've started the process and the goal is to develop a consistent approach for evaluating the different insider threat programs across the NISP. As everyone sitting in this room from a cleared industry knows, that we have everybody from what Michelle was talking about, a small business with two or three people to the Lockheed Martins, BAEs, Raytheons, and General Dynamics. So we need to make sure that we're able to provide the right consistency across the board to make sure we're doing effective reviews of these programs while they're in place.

So recently we had a tabletop exercise and there were four takeaways. Process must be consistent and simple. Reporting is not the only indicator of an effective program. As I mentioned, size and complexity is very important. And also, we have to understand that the variations and differences between local programs and those that are managed at the corporate level. When we rolled this out we actually put a lot of information and effort into making sure that we allowed for corporate programs to -- that a single program can be integrated at a larger corporation or company. So our way ahead is actually pilots are

planned in mid-2018. We'll be updating our resources and tools and job aids. We're working on internal training for the force and then we'll work on the socialization to industry. I think we found that was very successful when we rolled out change two the first time around.

So the next thing I have is actually Ben Richardson mentioned the seed four. Seed four is the updated [GPF?] guidelines. They came out in June of last year and one of the changes in that was it negated the requirement to have a disposition of a foreign passport for dual citizens. So along the way we've been looking at how do we make sure that when those cases were -- your cleared employees that were dual citizens had a disposition of passport and in some cases your security officers or FSOs maintained those passports to mitigate and allow adjudication for the final clearance. In January of this year the USCI signed out a memorandum to the Department of Defense that aligns with the same things we're doing for industry. While we're working on a seed for ISL this morning it went live. We have a posting and it gives general guidance on returning passports to individuals. It also gives information on what their employees need to be reminded of about their use. If they need to understand that they cannot use it for entry and exit of the United States and they have to report on official travel and its use. So there's some information in there. Right now you're

going to return it to them, you're going to remind the employees

any future use or effective use in or out of the United States

or for foreign -- unofficial foreign travel is an instant

report, but we removed the part where we had a lot of discussion

with industry this last couple of weeks about what do we do to

make it happen the first time around? So the trigger's been

pulled. It went live this morning some time so we can start

moving forward with that and by the end of the day today I guess

it would be all done. (laughter)

M:

(inaudible) Is the ISL going to mirror the guidance that you

guys are posting?

MINARD:

Yes. So the next thing is just a reminder, check out the CDSE

website on a routine basis. We've had a lot of new updates,

training material, webinars, shorts, briefings, and learning

activities that are posted there. Many of them relate to

insider threats. It's a good place to go for updated

information. And the last thing is some time in the next, I

can't say how many days or a month, I get the package final

signed you'll see the SF328 to go out for a 60-day notice.

Don't be concerned. The changes are administrative to the top

portion. One adds the requirements for DHS collection for the CCIPP program and it also addresses the defense enhanced security program as a collection for the 328. The questions have not changed. That's all I have.

BRADLEY:

Thank you so much. Any questions for Keith?

PANNONI:

Excuse me, Mr. Chair. Greg Pannoni. I have someone's parking pass for the garage on 7th Street so if you want to see me at the break (laughter) to get your car. (overlapping dialogue; inaudible)

BRADLEY:

Yeah, right, exactly, make sure you validate it. We're now going to hear from Ryan Deloney. Going to talk to us about an update on the NCCS implementation.

DELONEY:

Morning. Ryan Deloney, Defense Security Service. I have two updates for you this morning, the first on NCCS, the enterprise (inaudible) form 254 system. That is live within wide area work flow. We have over 40 agencies and offices currently registered

and using and over 150 industry partners as well. The largest

update is on February 8 USDI Kernan signed out an implementation

memo mandating that all components must begin using NCCS by

September 14th, 2018. So in line with that we've been working

with the different component points of contacts looking at what

is their implementation plan and assisting them to be successful

to meet that deadline. In line with that, as Michelle mentioned

during the industry update, as the services get in and use

that's going to drive up industry need to have access as well.

So we've been working with the industry concern looking at

scalability for onboarding because once you start bringing in

10,000 companies that becomes a big lift. So we are working

with specific web-based training and job aids for most of the

sessions in stand-up process and we're also working establishing

technical and functional help desks if you have a technical

issue with the system or if you want to set up your agency's or

your company's account management structure, how to do that from

a functional side of the house. We'll have call center support

for that as well. Those are the big updates on NCCS. Any

questions on that before I move to NISS?

BAUGHER:

Kim Baugher, State Department. I had a quick question on the

hard copy of the DD form 254, that I forget -- I mean recently

it was revised and there was a certain amount of time, I forget, I don't know how long, before we're supposed to use [ISIT?]. I think it's 60 days or 90 days, but I'm just wondering because different reps seem to be like warning us or telling us they're not going to accept them or whatever if they're not on that form and ours is right now, State Department, ours is done through a system and with monies and stuff we're trying to get it changed but we also aren't high on the list of priorities at the State Department to change certain things right now. So I just want to make sure that, is there a drop-dead day on the 254, the old one, that someone's going to say, "This isn't valid" because in my mind it still will be.

DELONEY:

So our facility clearance branch is looking for the new revised DD form 254. If yours are generated through the system and you have technical requirements that's something we could partner with John Massey on who oversees our facility clearance branch to see how we can work with you if we need to set an exception for specific cases, but we are looking to transition to the updated form.

BAUGHER:

Yeah, because I just don't want reps out in the field saying, "This is not valid" and when it goes to our contracts and goes to our contracting folks because, again, I'm not sure when we're going to get the resources to change it in our system.

DELONEY:

Yeah, we'd be glad to work with you to ensure that that's clearly and consistently executed.

BAUGHER:

Thank you.

DELONEY:

Question? Good, thank you. Shifting gears now to the National Industrial Security System. This is a system that will replace the industrial security facilities database, ISFD, a system of record for facility clearance information as well as the electronic facility clearance system for submission of facility clearance and FOCI related documentation, be it for an initial facility clearance or a changed condition where those apply. That is in a test state. It is live now. There's about 2,000 combined industry and government testers using the system and providing good feedback which has been appreciated. So, working with that. The biggest concern that Michelle brought up as well

was the registration error. That impacted about 10% of industry

users. That was set as the priority. It was a disconnect

between our single sign-on system and our NISS itself. That was

resolved as of last Friday. We reached out to a sampling of

those users who reported that issue who then all reported they

could access the system, so that was good news. There are some

outstanding one-offs that we're working. Those are more end

user configuration issues and as those come in we directly work

those, provide updates to our knowledge center for technical

support to ensure that they know how to consistently remediate,

but as there are any issues that continue to rise we encourage

industry and government personnel to continue submitting those

to our call center or through dss.niss@mail.mil.

Additionally, as we finalize those last issues that we have from

the soft launch state we will identify a deployment date. We

expect to identify that date this spring. So once that date is

identified there will be at least 30 days advance notice to all

industry and government partners through the DSS website, Voice

of Industry newsletter, and direct messages to all current ISFD

and EFCL users that that transition date is approaching and what

that transition will entail of. So there will be clear advance

notification when that cutover date is identified and we move

towards that. Additionally, coming up from the action items at

the top of the list, it was to determine capability of NISS to

have a best practices section for users. We took that back,

evaluated it. It is technically feasible. What we'll look for

is more specific requirements of what that actually is needed by

the community. So to that end we are looking to stand up and

operationals requirements committee comprised of DSS, industry

and government users of the system to adjudicate and prioritize

those system requirements to make sure that the delivery

capabilities are what the community is looking for. So we'll be

looking for, requesting, through industry and government

stakeholder points of contact to establish that body to

participate in that committee going forward.

The last note on the PKI issue that was addressed in the

industry concerns, NISS is behind [Incase?], our single sign-on

system that we've been using for years. You use it now if you

access ISFD, OBMS, it's also another way to access step for the

education side. So we haven't seen any specific PKI issues

because if you can access [Incase?] and you have been for years

you should be able to access NISS. So if there are any specific

things we do look for industry to provide those to us so that we

can troubleshoot those and remedy those as quickly as possible.

With that, that is the update on NISS. Are there any questions

on that side? Everyone's excited for a break. (laughter)

BRADLEY:

OK, yeah. OK, thank you, Ron. I appreciate that. It's time

for our five-minute break. Men's rest rooms are behind me. The

women's are down the hall. Please be back within five minutes.

[break] Please take your seats. This is what we have. In

order to keep this thing under two and a half hours or right at

the mark we're going to have to go. It's, what, 20 after 11:00

now. OK, the next person we're going to hear from is Nick

Levasseur from DMDC who'll provide an update on the deployment

of the Defense Information System for Security. Nick?

LEVASSEUR:

How you guys doing? So I know there were two questions that

came to us from the NISPPAC (inaudible). I'd like to address

those first. So I'm going to give you a little bit of a status

check real quick on this. We have (inaudible) and we've

successfully deployed to the components, Army, Navy, and Air

Force. The next deployment will be industry and that is still

scheduled for late May. One of the things that we were going to

address is the ECA [piv?] issue. I know that that has come up

recently (inaudible) cannot get into the system of the industry

working group. We have elevated this up to our senior

management and they are also (inaudible) to DISA so that we can

resolve this ECA issue well before the 30 days when industry is

supposed to go on. And the second topic that I think was

requested was the quick tip sheet. Same thing with this. So the two items that we have, we do have frequently asked questions posted on the webdocs page and I believe the last time it was updated was sometime in May of 2017, I believe. But what we're working on is with the small deployment that we've had so far we're receiving from not only the JVS users but also some of the other [catchers?] and so on and so forth.

So we are going to be updating that FAQ once we have some trends and some analysis in terms of what the questions that are being asked are on a recurring basis. We're going to take those top questions and make sure that we answer them on that document. It's twofold. To help you guys out, but also to reduce the amount of resources it takes for us to answer those phone calls. So besides that, I also did submit a change request to see if we can get more of a pinpoint identifier within the system to the user guide. So if you're doing let's say visit requests there should be a link that will take you directly to the user's guide on that. That is a change request and it's going to have to go through the priority and the funding review through OESDI. I think that's where I'm at unless I think I might be missing one more bullet. I'll rely on you guys to let me go.

BAUGHER:

Kim Baugher, State Department. (inaudible) other agencies
(inaudible)?

LEVASSEUR:

We do. So as of right now we are introducing Social Security
Administration into the system and we're working with the PAC in
order to identify all the other agencies that are coming on
board and the timeline for them to do so as well. I want to say
there are a number of them identified so far, but I'll have to
get back and let you know exactly which ones there are. All
right, thank you very much.

BRADLEY:

No questions for Nick? All right, we're going to hear from
another Nick, Nick Morin, on DISA.

MORIN:

Good morning. Nick Morin, I'm with DISA. I'm working on the
NDIS project. I was told that you guys were interested in eApp
so I'm here to talk a little bit about that, but more
importantly I've got a short video to show you that will --
somebody was asking (inaudible) and provide some feedback to
everyone. So I've got a short video that's going to talk more
about what we're doing. What I will say right now up front is

that we're very far removed from the development (inaudible)

interface. We spent a lot of our time -- a lot of the effort

has been focused on better research hearings and getting better

data. We hope that if we can get better data up front then that

moves the investigation a little quicker on the flip side.

Knowing that's not the only solution, but that (inaudible). So

we're doing increased validations on addresses. You're able to

improve teletypes. You'll see in the video it helps text next

to every single field to kind of give you more in-depth

knowledge about what's being expected. There's autosave.

There's also an ability to save as you go because there's a lot

more -- we've gotten -- there's more clicks -- it chunked up the

form more, so rather than just looking at 1,000 questions on one

page we chunked it up into logical sections so it gave you the

ability to save (inaudible). We went through a lot of user

feedback, user testing sessions, a lot of user feedback,

incorporated almost all of those went. So there was a lot of

cycles where we'd build something, we'd pull back, get user

feedback, come back and rebuild, and a lot of that back and

forth. And that seemed to work really well.

So where we are now seems to be a place where people are

seemingly quite happy with it all and we're looking forward to

getting out to a wider audience. But anyways, before I go too

far can we show that video? Because I think it talks a lot more about what we're doing. So this is one of our developers.

VIDEO:

-- is going to cover some of the new features in the eApp prototype. A lot of what we're doing is improving user experience, making it clean, really easy to use, simple, and improving the user flow throughout the form as well as improving the data that's collected from the form. We've been doing a user centered design process where we are testing this with users, recording their feedback, and working those suggestions and findings in throughout the form as well as getting a lot of good feedback from them. For example, with the reorganization of the navigation on the left, the different spacing and styles of elements, we've gotten feedback that it seemed straightforward, seemed more modern, current. One person even said it's the most painless experience for a painful form. (laughter) We're also reworking the navigation here to improve that flow and we're condensing it down into 10 top sections by grouping like subsections. So for example, in information about you we've included your identifying information and other names used. And the goal for this is to make it less intimidating where they're only looking at 10 sections as well as allow them to jump around really easily. They can go in and hop around

from section to section as well as give them an overall idea of where they are on the form with this sections counter here. One user that we tested said, "I like this counter style. It's nice to know, nice touch." Meaning that it was nice that they knew where they were on the form and how much they had left to do. Here's a screen where five of those 10 sections have been complete so five out of 10 is shown at the top. The sections that are good have our green check style here as well as the progress bar at the top that goes throughout the form and indicates how much left you have to do. There's a lot of user feedback on the form, not just in the navigation with these green complete styles, but also in the inputs themselves. So this one here, we've filled it out and we have our green check verification style. If we make an error somewhere that error message is very prominent and in your face. It comes up, we read what the issue is, and when we fix that we're shown that the form has confirmed that that fix has happened. Within each of these sections we have these accordion items. So rather than jumping to a new page each time we had, in this example a new bankruptcy, all of that happens on one single page. So this one has been filled out. If we wanted to add another one we click yes and it adds a new bankruptcy. We can start filling that out as well.

So however many bankruptcies you have they can all be added on one page and it's easier for the user to go back, edit things. This one is incomplete so we can go back in and finish it. If it turns out it was added in error we can delete each of these. Within each one of these, mimicking the style that we have up here at the top of the screen that lets us know where we are, right now we're in financial record and bankruptcy, that is carried through into the accordion where as you go down if this was really long and deep branch within this accordion we've found in testing that occasionally a user would kind of get disoriented and forget what they were filling in so we have this sticky header here that's the no, OK, you're working on petition number one, here's the [porthouse?] where this is stored and the date. So that way they can glance up at any point and it's like an anchor for them to let them know what they're filling out. Each of these top-level sections includes a review screen. So the flow throughout each one of these is you fill out a section, you're going through these next buttons, eventually you will get to the end of that section and that takes you to the review screen. So what that does is it stacks all of those items in one page where you can go through. It looks like this question was missed, we're calling out that this is required for you and it needs an answer. So it gives you the ability to change these live on the review screen. If there is an issue in here it gets

called out, we can fix it, and then jump ahead to the next

section. Another piece that's worth calling out is the way

we're handling the history section. So that's where you live,

employment activity, schools, and formal federal service. A

couple of the pain points that we've heard was address issues

where something as simple as spelling out circle instead of CIR

would cause kickback and we'd have to push this back to the user

and get that change made. So we're bouncing these addresses off

of USPS and their lists now. So if I go in here and I'm typing

my address and I, for example, spell out circle we're running a

check against USPS, it verifies it, and then it proposes a

suggestion. So in this example we're shorting circle because

that's what USPS wants. We give the user the ability to use

this address and it changes it live here.

We're also recognizing that a user might need to enter the same

address multiple times. For example, they lived at home, they

go to school, and then they live back at home again, and they

need to reinput that address. That's where this personal

address book style comes in. You can select that and preload

one of these addresses. So if I needed to switch this to this

address, one click and that updates that address. If I did that

in error I can go back. So those are the improvements within

the address block itself. We're also adding a tracking tool

here where we're telling them we have 10 years that must be

covered. There's a visual gap here and we can see that there's
only seven covered, but we're also dropping these error messages
in that tell a user where the gap is and how to fix that. And
they can fix it by adding an address here. That's carried
across through where you went to school.

This one doesn't have gap tracking. It's more of a counter
where we're counting schools and degrees and diplomas added.
Employment activities is more of that gap style where we have
three out of 10 covered here and then our visual progress bar.
Once that gap is covered this turns to green letting the user
know yes, this is good, and they can continue throughout the
form. The last piece to touch on is the way we're handling
different screen devices. We acknowledge people are going to be
using this on tablets and maybe even phones. This is in
progress right now. We're still working out solid break points
on this, but it does break down to mobile now and you can go
through and fill this out. Again, it's in progress. This will
be continually refined, but our accordion items add here. One
more element is the save icon. This was brought up a lot in
usability testings where users expressed concern that they
really wanted this information to stick around and the form does
autosave but they would feel much better if they had a physical
save button. So the autosave feature now doubles as a physical
save button. You can click on it at any point and it saves the

form, giving the user that kind of added peace of mind that they can leave and come back and none of this information will be lost. And that covers some of the base features here. Thanks.

MORIN:

So (inaudible) an EFS video. Several more (inaudible) there's been some more [refinings?] on the (inaudible). Every time I've shown that the same questions always get answered (laughter). We're doing a couple thousand users this fiscal year, primarily on the military side and the civilian side, to test the form, see if people like it, how it works in the larger community. We'll do some testing of the data to make sure it's validated properly, it's going to flow through the system properly. This will be released to the larger community some time in FY19, hopefully as far left as we can get that. [NDES?] as a whole has a target of full operating capability of October first of 2019. We're going to try and be releasing things incrementally as we go. This hopefully will be one of the first things. Any questions?

WILKES:

Quinton Wilkes, industry. Is EF going to be part of the new DISS system?

MORIN:

No. So just -- it's all going to be rolled into the same suite
essentially of NDES. So this is going to fall under NDES, it's
going to be one of our products. We're going to try and as with
EFS (inaudible) management tool. So we're going to try and make
it -- in the long run make it all as seamless as possible. In
the short run you're going to be kind of going through the two
different systems.

WILKES:

Right, because the reason for the question because right now
industry goes into JPAS still to do their investigations. They
don't go directly into E-QIP like the rest of the government.
So moving forward it'll be the same or different?

MORIN:

So going -- I'm not sure of the exact (inaudible). We haven't
hammered out all the exact (inaudible) functionality. So it's
either going to be going through to JVS to initiate a queue. It
will go through a different agency functionality. I'm not sure
we've hammered out that detail quite yet in terms of what that
initiation will go through.

BAUGHER:

Kim Baugher, State Department. I'm assuming this whole new

system, is it not going to populate -- I mean people like it now

because their old E-QIP populates. Are people going to start

from scratch or will it populate it? I may (overlapping

dialogue; inaudible).

MORIN:

That's one of the challenges we're going to work out between now

and the larger release is that we want to make sure that to the

extent we're able to we want to make sure that the existing data

is available for users. We're starting off the first couple of

thousand users are entering initial forms because we don't have

that solved quite yet, but we want to make sure we do solve that

before we push it out to the larger community. We recognize

that. That would be fun for everybody if we didn't have that.

BRADLEY:

Anybody else for Nick? Michelle?

SUTPHIN:

Michelle Sutphin, hi. One of the pain points in E-QIP currently

is any time that there is a correction for an applicant they

have to go back in and not only do the correction, but they have

to redo all the yes/no questions. Has there been any discussion

as to how to make that process easier, for example, showing them

a list of their responses and just having them validate, is this

correct, to speed that process through?

MORIN:

I know we've had discussions on it. Chris, do you know where

we're at on that? I'm not sure where we're at on that, but I

know we've definitely had discussions on that process and it

seems to come down to some differing philosophies on what you're

doing with that. Some people seemed to think it was more of a

gotcha type of idea. You know, you said no before, now you said

yes or you said yes, now you said -- so I think I need to

understand the policy around it first. Technically, a piece of

cake. I just need to understand the policy around that first

and I don't think we have that (inaudible). We might, but

unfortunately (inaudible), but he's unavailable today so I'm

kind of filling in. But yeah, I think we're going to look at

that a little more closely and see (inaudible).

SUTPHIN:

Thank you.

WRIGHT:

I have a question. I'm sorry, Natasha Wright, Department of Energy. I have a question about the frequency or the periodicity for how often the system automatically saves the form. I think it's going to be important for users to know that interval so then if there's a power outage or if there's some issue then they will know that they need to actually manually save the form as they go along.

MORIN:

At a minimum it's every time they click one of those next buttons or whatever thing. Do you know if we have the autosave -- I don't think we have an autosave like timewise, but the form is chunked up -- you saw it. It's a fairly small section so if you're (inaudible) a section, hitting next, we also have that save button on the right here that kind of hovers and floats with you as you scope it down. So yeah, potentially you have a power outage you'll probably lose that page, but you're not going to lose everything because every time you click next or previous or click to a different section it automatically saves as you go.

WRIGHT:

OK, awesome. Thank you.

MORIN:

You're welcome.

PANNONI:

Greg Pannoni. And if I missed it I'm sorry, but the security

features, I hope, consider what's happened in the past with this

type of data being sensitive, that the correct moderate level of

confidentiality, security controls, have been incorporated into

all of this. Is that --

MORIN:

So we're working on some of the authentication and security

right now. And so one thing that I said before the presentation

was that we spent a lot of time focusing on the presentation

layer, how it's going to look, how it's going to perform,

getting better data validation. The next step after -- so we're

going to roll with this and we're going to secure it and make

sure everything is locked and loaded, ready to roll. The next

step is we want to actually rearchitect the back end of it to be

able to handle some additional forms, but to also be able to

handle any future (inaudible). So if we want to have a closer

investigator to applicant type of interaction we could support

that. I'm not saying -- that's a policy question, but we want

to be able to support that should that come down the line. As

part of that rearchitecting of it is we're introducing even some

more security controls that go above and beyond. Probably

getting away from a database model and going to more of

individual encryption, individual key for every single file. So

I think it's -- we're there now. It's going to be even better

in the future. I have a lot of confidence in our security

posture for this.

BRADLEY:

Anyone else? You had a --

HARNEY:

It's kind of a follow-on on that. You showed kind of a link --

it's Bob Harney -- to the address thing and that sort of thing.

How is that from a security standpoint being handled? Is that

out to the web or --

MORIN:

It is out to the web. So there's a -- the US Postal Service has

a (inaudible). So we're passing it to that web service and

retrieving the data. It's a very like point to point connection

where we're going straight to that service.

HARNEY:

Yeah, this can sort of open this to the web or whatever privacy

protection aspect?

MORIN:

Believe me, we've got a whole team of security people that are

concerned too. So that's the reason why it's not out yet.

We've got to go through a whole raft of cyber security testing

and vetting and making sure everything's -- that will be passed

on the test and everything. That's one of the things they're

going to be looking at closely to make sure that that point of

entry in (inaudible) is essentially secure. Absolutely, but

that was one of the key features we're trying to implement so

we're hoping we can make it work.

BRADLEY:

Any more questions for Nick?

M:

(inaudible)

MORIN:

(inaudible) discuss it with the [program office?]. I'm not sure

how -- I'm not sure. (inaudible) I've just got to doublecheck

with that.

BRADLEY:

OK, anyone else? Thank you, Nick. All right, now we're going to hear from Pat Viscuso, my staff, on the status of CUI, particularly its implementation and where it stands. Pat?

VISCUSO:

Well, it's nice to see a lot of familiar faces and I'll give you a status on where we're at right now. So there's a sequence of phased implementation. By the way, I should note everything about this program is pretty open. All the guidance is open, all the notices are open. They're all on our website, www.archives.gov/cui. And so there is this CUI notice that was co-admitted with OMB and affected agencies that sets out the sequence of phased implementation. Because we're talking about a very large program that's going to affect a lot of -- most of the executive branch. And based on that phased implementation, for example, establishing governance first, establishing policy first within the agency to implement the program, then training the employees, then making an assessment, for example, of the IT systems to see whether they need to be brought up to certain standards in accordance with the federal regulations, so on and so forth. Based on this and the reports that we are receiving from agencies, because we asked for a status report and we've

asked for a submission of an annual report, we are projecting a
three to four-year timeline for the implementation of the
program.

Right now we have received a number of completed policies that
agencies have been able to finalize, but we are -- throughout
FY2018 agencies are projecting that they will be issuing their
policies. On November first, 2017 agencies were required to
submit their annual reports on the status of their
implementation. For the first -- for the past three months we
have engaged those agencies that have -- that had failed to
submit their reports. We've also engaged agencies that have not
established the governance for the program within their
agencies, namely the controlled underclass flight information
senior agency official without was sure that there would be
adequate resources for the program to be implemented and the
program manager who would actually run the program within their
agency and interface with us.

And so we are in the process of compiling our report to the
President based on those that have reported to us. And we will
be submitting our assessment and analysis based on the data in
the third quarter of 2018. We plan to revise the CUI registry.
The CUI registry, as you may recall, is the central location
which lists all of the categories of controlled unclassified
information that agencies will be controlling and marking. And

what we've done is we've attempted to make it a bit simpler.
What we've -- we've replaced the CUI categories and sub
categories with CUI categories falling under groupings so that
all of the legal authorities that will be listed under the
categories will not be split between categories and sub
categories as they are now. In other words, it'll be a more
user friendly and simpler arrangement. We've been careful
though not to affect anything that will deal with the markings
of the categories and we've been very careful in this revision
not to affect anything of the agency policies that have already
been finalized.

I might add though that the CUI registry, actually the category
listing, is really not for the average user. It's really for
the program management officials. But nevertheless, there are
tools on the registry which are very useful for the average user
and can assist agencies and industry in understanding the
program. What I'm referring to are a whole series of training
videos, associated downloads of scripts and PowerPoints, and
other resources such as the CUI marking handbook. Speaking of
which, we are revising. We're revising the CUI handbook for
better readability and presentation of the markings, but I must
emphasize that we are not changing the marking schema. Why
would that be? Because it is rooted in the federal regulation,
the 32CFR for 2002. So what we are trying to do is we are

trying to produce a more user-friendly product and we expect to

release that sometime in early spring 2018.

We have a very active CUI blog and if you go to the registry

site, www.archives.gov/cui, you will be able to access the blog

and get updates on all the products that we are publishing.

Useful recommendations and guidance continue to be produced in

the form of CUI notices and since the last NISPPAC we've issued

two. One is a guidance on drafting agreements with non-

executive branch entities involving CUI, but I must emphasize

that this is not the federal acquisition regulation. These are

the types of agreements that more or less -- that are used for

state and local governments, this sort of thing, not with

industry for procurements. That's a separate complete effort

and I can talk to that in just a minute. We also have a CUI

notice that deals with recommendations on basic training. It's

a highly professional document that deals with training

objectives and methodologies. For those of you who are

interested in the development of learning objectives and

curriculum I do recommend that you take a look at it. And as I

say, all of the guidance for this program, all of the policy for

this program, is completely open and available on this website.

Regarding the FAR which does affect industry sitting in this

room, we are part of a technical working group since June headed

by GSA and under the auspices of OMB's office of federal

procurement policy. And this group has been working on a draft

FAR. And we have -- I would like to just note something here.

We've made hundreds of presentations throughout the country at

industry events, NCMS events, as is -- I'd like to publicly

thank NCMS chapters for providing travel expenses for my staff

in providing these briefings. At these briefings we receive a

lot of input from industry about their concerns, about the real

situations that they have to deal with, about the

inconsistencies that they have to deal with regarding the

protection of the type of information that will fall under the

CUI program when it is implemented. We have listened very

carefully and this has informed our development of the FAR draft

and what we bring to that technical working group. And we are

looking forward to the fact that this FAR draft will go through

a public rulemaking process where industry will be able to see

the results of our work and comment on it. We expect the

conclusion of that process to take place some place in 2019. We

expect the initial draft of the FAR to be completed within the

next two months and then it'll be going through this FAR federal

rulemaking process which will involve submission to the defense

acquisition regulations council, the DARC, and the civilian

agency acquisition council, the CAAC, and then legal review and

public comment.

Now, regarding outreach, our outreach efforts do continue. I've

mentioned the large number of briefings that we continue to

provide. Please, if you would like to invite my staff to

provide a briefing we would be more than happy to do so. The

larger the audience the better. We want to reach as many as

possible. In that vein though, we have produced a whole series

of training videos that have been very well received and they

continue to enjoy a great deal of popularity in terms of

download. Our -- and as I said, the transcripts and the MP4

videos can be brought down to your -- can be used by your

facilities, can be used within agencies, and they have been. We

do invite participation in our blog which is quite active.

Since October 2017 we've had 449 followers, 2,218 visitors,

6,513 views from 28 countries. Regarding the YouTube videos,

767 for the overview, over 2,000 for the introduction to

marking, over 800 for decontrol, close to 2,000 for the

controlled environments, over 800 for destruction, 1,000 for

marking nontraditional media, close to -- well, over 5,000 for

unauthorized disclosures, and six and a half thousand for an

overview of the program in detail. And about 600 for lawful

government purpose.

We are open to all of your suggestions as the CUI executive

agent for this program. We are the center for the -- and we

have the responsibility for the establishment, maintenance, and

overview of the program and we will continue to exercise a

robust role in doing this. Any questions about this update?

WILKES:

Quinton Wilkes, industry. Pat, how many agencies have

implemented the program?

VISCUSO:

Right now in terms of full implementation, no one has fully

implemented the program. But in terms of agencies that fall

under the program we have a number of agencies that have

submitted their completed policies. You know, these are huge

organizations so you've got to first complete your implementing

policy and coordinate it. Then you've got to design your

training program and train all of your employees. And that's

just for starters. So the implementation began with the CFRs

effective date which was in November of 2016. Agencies then

were called upon to revise their policies and took most of -- a

lot of them got a -- were able to move out and begin to revise

their policies 2017. So we've gotten quite a few that have

submitted to us, taking advantage of what we've been doing,

submitted to us their policies to review even before they began

to coordinate them internally. And then they have to do their

components of course. So if you're talking about a huge

organization, for example Department of Agriculture, you're

talking about a very large number of components which then have

their component policies to do. So that's why we've projected

it three to four years, because it's a complex thing.

MOSS:

Leonard Moss, industry. Pat, this is a big program obviously

which is why you're taking your time and trying to do it right.

My question --

VISCUSO:

Well, it's not only us taking our time and trying to do it

right, but it's the sheer practicalities of the thing. In other

words, we can move with the development, we've moved with the

development policy. It took quite a bit, by the way. You know,

it took about five years to do the informal and informal

development of the federal rule. And we can put out -- we're

pretty quick in putting out CUI notices clarifying. Not putting

out new policy, but clarifying the policy through guidance and

also making recommendations. If you want to really see an

insight into the complexity of the thing I recommend CUI notice

201701. This is something to take a look at because you'll get

the full breadth of it, you know, from an agency perspective.

MOSS:

So my question really revolves around oversight. I'm just -- I
know this is probably early, but what thought are you giving to
who's going to oversee this and how are you going to -- is it
going to be one overseer like ISOO or (overlapping dialogue;
inaudible).

VISCUSO:

So the way we want to approach this is actually from the
standpoint of overseeing agencies, we would oversee their
programs, their programs of oversight to ensure, and this is why
we're working with them in working groups, to ensure that we
have common standards by which we're going to evaluate their
oversight programs. Now, the thing that industry should be
paying attention to is the fact that we are, and this is
something unprecedented for the control of sensitive
information, is that there is one CUI executive agent to whom
you can address concerns and issues. You can bubble up, for
example, the NISPPAC MOU members can bubble up issues to us and
there is a central place where they can be addressed. So the
governance of the program is pretty interesting. It's the CUI
executive agent and then you have, what? The CUI senior agency
officials and program managers. Now, we have a CUI advisory
council, but note it says advisory. That is the means by which

we get advice, we fulfill the functions of the 32CFR2002 and the
executive order on consulting with affected agencies, but it is
not part of the governance structure. So there is a CUI EA that
is the center for these types of issues with regard to the
government and the consistency and implementation of the program
consistent with the program's requirements.

WRIGHT:
So I have a question. This is Natasha Wright, Department of
Energy. I really appreciate and love the fact that you are
having an outreach program with this reaching out to the
agencies or at least having information available so that they
can go and get additional information and assistance. You
mentioned that you have YouTube videos available. Is that via a
specific channel or how do we find that information?

VISCUSO:
So everything -- the CUI registry by its definition is not just
simply a listing of the categories of CUI but is in fact a
clearinghouse for everything related to the whole program,
including all of the training, outreach materials, everything is
on the registry including access to our blog. So it's one
central place, it's very simple, www.archives.gov/cui, and you
see the CUI blog specific address, but you can access it right

through the registry site. What agencies have been doing is downloading the training videos in their component forms, the PowerPoint slides, the transcripts, and the empty port videos, and incorporating them into their own training packages. We also, that notice that we just issued on training is no small thing. That is a very professional product. I want to thank the Department of Defense Security for Defense Security Excellence and also I would like to thank the intelligence community. They brought their -- and Department of Homeland Security. They brought some of their best professionals involved in development of training, learnings, and objectives and curriculum and they produced a truly professional document of standards by which a training program can be developed by an agency and any other large organization such as a major company in developing a training program.

WRIGHT:

Thank you.

VISCUSO:

Thank you.

BRADLEY:

Anyone else for questions for Pat about CUI? OK, I thank you,
Pat.

VISCUSO:

Thank you. It's been a pleasure.

BRADLEY:

Next we're going to turn to another one of my deputies, Greg
Pannoni, to give us an update on the NISPPAC implementing
directive 32CFR part 2004. Greg?

PANNONI:

Thank you. I'll try to go quickly to get us back close to being
on schedule. The 32CFR is closer to publication. We did review
a second round of comments, a limited number of comments, from
agencies. We, ISOO, did that and adjudicated them and just
recently submitted them back to OMB. We are anticipating OMB
will approve of our adjudications and if they do the document
will come back to NARA for NARA senior management to take one
last look at it. Then it goes to the federal register for a 30-
day public comment period which includes anyone, Congress, to
look at it. And then it will be published. So that's where we
are on that. Is there any questions on the 32CFR2004? No? OK,
well. I'll move into my next one.

BRADLEY:

We're moving into the working group section now. So Greg will

give one on the insider threat working group.

PANNONI:

It's not specifically, I don't think, called out on the agenda.

The insider threat working group we're considering as part of

the clearance working group. There's really not much to report

right now. You heard earlier in our meeting what is going on

with insider threat and the Department of Defense, meaning phase

two, the beginnings of the evaluation of the execution of

insider threat requirements. And so this group, with that

starting to evolve and develop, piloting starting to take place,

we will probably try and meet sometime this summer, industry and

government, to talk about mutual concerns as to how this is

evolving. Obviously scalability is something that needs to be

considered. The smaller companies where in those situations you

may have one person wearing a lot of different hats, doing a lot

of different functions versus a large corporation where you have

a separate legal department, you have the information systems

folks doing their things, you have financial people doing their

things. So there are differences in how this thing is

effectively executed, not its scalability. So I think everyone

is mindful of that and wants to be a party to having those
discussions as we move forward. Are there any questions on
insider threat?

OK, so now I'm going to ask Laura Aghdam as we move into the
clearance working group to give a brief overview of the
clearance working group and then we'll move into the individual
presenters.

AGHDAM:

The clearance working group is our largest group and is pretty
much a precursor to what we're going to discuss here and what
you've already heard today. So I'm just going to kind of read
the list of topics to you and if you have any questions you can
let me know. Of course, we always receive updates on personnel
clearances and the timelines. We talked a little bit about
NISPOM informing change three status, talked about seed three
guidance for industry. We got an update on the setup of the
DISS working group which really hasn't gotten going yet, but
they're working on it and that should be within the next month
or two. We got an update on the NISS deployment which you
already heard today and industry provided a list of the topics
it proposed to discuss today. Any questions? Thank you.

BRADLEY:

OK, going to move into the metrics and statistics. Gary

Novotny, ODNI SEA.

NOVOTNY:

Good morning, good afternoon. My name is Gary Novotny. I'm the

chief of the security oversight branch at the ODNI. So just

very briefly, as Laura said, our role here is to just go over

very briefly the national security timeliness metrics and a few

other things. And I'm waiting for the PowerPoint to go up but -

-

AGHDAM:

It does work. (laughter)

NOVOTNY:

But what I wanted to mention, and similar to what Mr. Phelan did

with the 700,000 backlog, it's just kind of real briefly talk to

you about the timeliness metrics and what exactly we're

measuring when Mr. Phelan puts up some timeliness charts and

when we put up some timeliness charts. So the hockey rink

there, I want to focus everybody's attention in the hockey rink

because when we start the timeliness for the national security

timeliness that we present it's from when the applicant or the

contractor or the individual signs that standard form 86. So at

the beginning of the process is that initiation phase when the
individual certifies SF86 and sends it off to security, all
right? And then at the end of the hockey rink there is when
that adjudication is made and that adjudication decision is
uploaded into the repository. So all that stuff outside the
hockey rink there, the pre-submission stuff, any kind of
prescreening paperwork, things like that that you would do in
industry or even in the government, that prescreening and pre-
paperwork, and then any post-decision coordination and
documentation, things like that, is outside the timeliness
metrics that Mr. Phelan and myself will provide.

So I just wanted to make sure that we understand that when we're
looking at national security timeliness it's everything in the
hockey rink there, all right? So the next couple slides is just
going to be DOD industry data and IC data timeliness. But real
quick I just want to go over the methodology. You can replicate
this slide if you want. Remember the Intelligence Reform and
Terrorism Prevention Act of 2004 created the investigate and
adjudicate time frames. The metrics and measures subcommittee
in 2008 kind of added that initiation phase on the front as well
as the periodic investigation timeframe. And then Director
Clapper in 2012 expanded that investigation timeframe for the
initial top-secret clearances from 40 days to 80 days because

obviously those top-secret background investigations take a
little longer.

So, as a few people here before me, I want to preempt a question
when we're talking about timeliness goals and if we are
relooking at those. We are taking look at the end to end
timeliness goals right now, but we need the data, right? We
can't just create a new timeliness goal without really looking
at the methodology and the timeliness metrics across the
government. So we are continuing to gather that data to see if
maybe the [ERFA?] goals need to be relooked at. So but that's
methodology on where we got to where we are. Robert, if you
don't mind going to the next slide. Just briefly again this is
DOD industry data and IC data. The first quarter of fiscal year
'18 is shown in the purple bar and at the bottom is the volume
there and it's similar to the slides that Mr. Phelan had up.
The secret seems to be steady there along with the periodic
reinvestigations. Top secret did show an increase again in
quarter one of fiscal year '18.

The next couple of slides just kind of break that out in the
secret, top secret, and the periodic reinvestigations, but what
I want to focus on is a new slide that I have, I believe it's
slide seven or eight, Robert? Eight. And it's a new slide,
response to the clearance working group. What we were wondering
we could get is just the industry data just in the intelligence

community. So this is across the intelligence community. The industry data and the goals are kind of in the background there shaded. And again, for secret, top secret, and periodic reinvestigations you'll see exactly where just the contractor data in the IC lies at 119 days for secret and right around 170 days for the top secret and periodic reinvestigations.

BRADLEY:

Any questions for Gary?

M:

Gary, you know I asked this before, that is the fastest 90% or --

NOVOTNY:

Yes, I'm sorry. Yeah, the methodology is fastest 90% of the background investigations for your niche.

M:

OK, thank you.

NOVOTNY:

And with that said, I was just informed earlier this week that I'm actually being transferred to a different position within

the ODNI doing some different IC stuff so there will be somebody
else probably presenting the hockey rink slide and some
timeliness slides. But I just wanted to mention that. We'll
still continue to support it, but I appreciate the last three,
three and a half years you've let me come and provide some
(inaudible).

BRADLEY:
Thank you. (applause) OK, next will be Heather Green, DSS.

GREEN:
Good morning, Heather Green, DSS personal security management
office for industry. So as that pulls as well I'll highlight a
few items regarding industry front end investigation processing.
The personal security investigation budget is fully funded for
this fiscal year, but we have been continuing to meet our
investigation submissions to stay within the continuing
resolution constraints. We continue to prioritize initials,
then PRs. Once the CR is over, keep our fingers crossed, we
will be processing at a steady state. That means that the
investigations will be processed within one to two days of being
received into the system. So that left-hand chart, that's not
the stock market. (laughter) It's not my blood pressure. It's
actually the inventory of investigation submissions that we had

to meet or in hold back due to the constraints that we're having with the budget. But, as I mentioned, the good news is this fiscal year we are fully funded so once we get over that CR budget constraint then we will be back to that steady state. We posted guidance on our website regarding the T5R deferment. We do need industry to submit all T5Rs over the six-year periodicity. Currently there are over 16,000 T5Rs that are over the six-year periodicity for industry. So we would like you to begin submitting those as soon as possible. We have been maintaining interims on an average of 30 days. We understand the importance of getting the trusted individuals to work in a timely manner so we're going to continue to maintain that 30 days and strive to improve that as well as we continue to look through our processes to ensure that we can meet those needs and the goals. Next slide.

In light of our timelines please keep in mind that you can do things to reduce the delays. Ensure your E-QIPs are required for performance of classified contracts. Conduct thorough review of the E-QIP for completeness. The eApp technology system will help us in the future, but for now we are looking at -- it's very manual in nature so as much that you can do on that front end to ensure the accuracy and completeness of the forms certainly help. Use click to sign. And extremely important for electronic fingerprints for initials, please submit at the time

or just before an investigation request is released to DSS and

JPAS. Especially once we get back to that steady state that's

going to be very important. We will not be releasing initial

investigation requests to NBIB unless we see that the [SAC?] or

the fingerprint results are actually in the system. So that

helps us on a couple of fronts, but certainly will help with our

timeliness for the interim determinations as well as ensuring

that the fingerprint results have been received and the

investigation continue to move forward. Any questions? Thank

you.

BRADLEY:

Thank you, Heather. All right, next is Ned Fish, DOD.

FISH:

Morning, everybody. I'm Ned Fish from the DOD CAF. I'm going

to try to go quickly. I'm not sure if it's good news or bad

news, but the CAF continues to be a bit boring. Not as

interesting as Charlie and DSS and all the other moving

investigative pieces. So if you look at this slide this again

shows you where we see the backlog as we measure it at the CAF.

The blue is steady state in the norms and the red is outside of

the norms, whether that's the timeliness piece that Mr. Novotny

was talking about or norms go back and forth between suspense

and review. I think we've achieved a bit of a steady state

here. The good news is when I started talking to you in 2013

there was 8 to 9% of the annual workload that we did for

industry for the NISP was in a backlog and now if you see that

green circle on the bottom right it's somewhat less than 1%, but

there is a bit of a pesky backlog that we're working off.

Again, that shaded area is where we were able to then not just

talk to you about collateral cases but SCI cases. Just as a

reminder, sometimes people think -- you go back to the disco

days those cases were just collateral. We adjudicate about

130,000 SCI cases per year and probably about 30,000 of those or

so are for the NISP community.

Bottom left there you see that's some of the points that I would

like to highlight since I last spoke to you at the last NISPPAC.

This backlog, a slight increase of about 300. I don't think

it's much to worry. That's the evident flowing. With that SCI

workload we actually are in DISS with the [NASH?] for the

industry. So all cases are coming to you today with an SCI

determination are actually being adjud8cted in the DISS system.

When we talk about the deployment to industry in May that's

actually for the collateral aspect of the workload for PSMY and

for the subsequent portal that it will work with you all in your

security offices. I think we have a good steady state work flow

with DOHA in the legal sufficiency review, around 400 cases

there. However, it is important to note that as we saw with the
military department in January we can expect an uptick in the
work in progress, an uptick in this backlog slide. The next
time I brief you as we deploy the system and get folks trained
and spun up and consolidated on the new DISS system to be
deployed in May. Next slide.

Our timeline is a little bit than what DNI reads because of
course I'm not talking about DIA, NSA, and NGA adjudications
here. This is just duty cap. I think the good news is if you
watch those lines at the top right and look at the comparison of
'17 to '18 to date we're actually improving some of our
timeliness as far as timeliness. An uptick in the PR line back
in August was due to about a two to three-week period where we
had no in just of cases so therefore there was a timeliness
issue once we did start adjudicating them. So I think we're
fairly decent as far as the norms and where we need to be.
Again, these timelines will probably be growing. You'll see
some spikes next time I brief you given the pending deployment
of this in the May timeframe. Next slide.

Key takeaways. I think we're at a relatively steady state
today. Hopefully we can get through the DISS deployment and the
follow-on DISS deployment in a healthy way and find a better
normal in the future. Some of the impacts you've seen are
actually those SCI adjudications we're doing for you so I think

there's some good news where that unlike when we deployed to the military departments the industry adjudicators at the CAF are working cases in DISS today. They're just not working the collateral cases in DISS and so we're a bit further from the CAF perspective along with industry as far as knowing what it looks like than we were with the military department deployments in January. But again, as I pointed out, the next NISPPAC expect to see some tick-ups. Last thing is we're looking forward -- we're forward looking towards the investigative shift and I do foresee I will have -- I'll be -- I'll have two hoses turned on me, not just the MBIB hose, but as DSS picks up their mission there will be the DSS hose. So we're going to work closely with both DSS and MBIB and USDI and the chief management officer of the Department of Defense to make sure we understand how that's going to come at us and so that we're postured whether it's -- to adjudicate whether it's e-adjudication or manual adjudication, but if you all remember back in '05, '06 they moved -- the investigative backlog just moved in to become an adjudicating backlog. That pig just moved down the snake and so we're working hard to posture ourselves so we are -- that pig is gone. That pig is not coming to the CAF. But that's going to take some work in the coming months as we look at what's happening and how quickly, whether it's CE and all the different changes in the coming years. That's all I have.

BRADLEY:

Thank you. Any questions for Ned? Actually, I have one behind

you. Valerie?

VALERIE:

Valerie (inaudible). I was a little confused for a second

there. So the SCI adjudications for industry are being done in

DISS? But does not JPAS also then reflect that an SCI

adjudication has been accomplished on Joe Doe from --

FISH:

Yes. I mean the JPAS is still the system of record. So the

reality is you're -- NISP industry adjudicator is at the CAF.

When we moved all SCI cases as well as collateral cases to them,

had to operate in two versions of CATS, Army CATS and DISCO

CATS. So, but yes, it's still seen in JPAS. Thank you for

clarifying that. They're done in DISS but it floats to JPAS.

BRADLEY:

Anybody else for Ned? Thank you, Ned. Appreciate it. All

right, now we'll hear from Perry Russell-Hunter, DOHA. Hey,

Perry.

RUSSELL-HUNTER:

So I felt like a baseball player stealing second because I've been moving up the room to get to here and so that I would save time. (laughter) I promise I'll be brief which is something you almost never hear a lawyer say. I have good news which is that the numbers awaiting decision, cases awaiting decision by an administrative judge are down from the last time I talked to you. Also, the number of statement of reason legal reviews that we have actually remains below 200. The ones that -- the number Ned gave is the full process including what's also still at the CAF to be sent to us. So the good news there is that 200 is a month's worth of work. So we're getting stuff done within the month that we get it as far as the statement of reasons reviews and my only caveat for the future is, as Ned pointed at the looming investigative backlog, is that we hope that issue resolution can still be a priority in resolving those investigations because that helps us. To the extent that we have delays in the downstream process it's when we have to resolve an issue that has not been resolved earlier in the process. And so I join Ned in pleading for careful resolution of that investigative backlog.

The other thing I would say is that because in Gary's hockey rink we're very much at the tail end, we're kind of clustered around the goal, I would hope that as a larger policy matter we

look at making e-adjudication more robust. One of the reasons

that Ned and I feel so strongly about that is because

adjudicators can spend more time on the real issue cases

resolving issues if they're not having to worry about cases that

really have nothing in them. So in that regard I hope that when

we next meet we're talking about having made e-adjudication more

robust. And that's all I have.

BRADLEY:

Thank you, Perry. You're a man of your word. (laughter) Any

questions for Perry? All right, next we're going to hear from

Karl Hellman who's going to tell us about the NISP information

systems authorization working group report. Karl?

HELLMAN:

Good afternoon, Mr. Chairman, and it is afternoon (laughter) so

I will be brief. Just a couple of updates from the DSS

perspective of our NIST authorization office just as a -- for

our government partners, beginning January 1, 2018 we began all

industry submissions for classified information system

authorizations are using the NIST RMF framework. We released a

new process manual back in November to support that transition

so we are moving forward in that transition and we continue to

mature and grow those NIST risk management framework processes.

And obviously I always make a plug for dss.mil.rmf. In 2018 the other thing -- big item that we'll be working on in the -- with the NISA working group will be our transition to eMASS. eMASS is a DISA system of record for conducting RMF authorizations. So we will transition our -- from our current DSS built business management system over to a DISA supported system. Next slide please.

I have a couple of metrics that aren't about personal clearances so just -- and this is just by our four DSS regions the number of authorization decisions that we issue on a monthly basis. As you can see, the months of November and December and January we started an increase. This was for industry submissions ahead of our formal transition to all systems. So they spiked a little bit and, Robert, if you could please go to the last slide.

Thank you, and here is our timeline and, again, what we would have assumed based on an increased number of submissions before the end of the year and before that final transition, we'll have a small spike in what our timeline is of getting ATOs delivered. And our normal goal is 30 days. Our January metric was right about 40 days, but we expect that to dip back down to under 30 days as that spike dissipates. Sir, pending any questions I would like to thank NARA for providing leadership and support to the NISA working group. I think we've done a lot with industry

and the government folks doing that. So for Alegra and Robert

to support us, we appreciate that.

ROBERT:

You're very kind. We appreciate your appreciation.

BRADLEY:

Yes, sir.

MOSS:

Karl, Leonard Moss, industry, just real quick, what do you

attribute the spike to? Is there a reason?

HELLMAN:

So January 1, 2018 was the transition of all systems. We had a

set of systems that were still being worked under the old

certification and accreditation process. So people were

submitting for either new systems or reaccreditations in late

November/December to beat having to go to risk management

framework. So we had an increase in those. Which we expected

and in our phase one we had the same thing last summer. Thank

you, sir.

PANNONI:

So, Karl, Greg Pannoni, I really don't want to call that a region, but looking at the chart from June through January northern region is always above the target and they really jumped in January, but yet looking in the prior chart their numbers really aren't the highest. The western region and the southern region overall seem to have higher numbers as far as actual volume of ATOs. So why is that? Why is the northern region having a bit of trouble?

HELLMAN:

So we look at a few things. One is the length of experience of the staff. Our summer spike -- the northern region just this summer, probably in August, they got to basically a full staff function even though for us full staff isn't, as with anyone else, isn't enough folks. So along with big -- so they are fully staffed, but they have the least experienced staff. So the timelines for newer ISSPs, and those are our boots on the ground folks doing these planned reviews, is longer for our newer folks than our more experienced folks.

PANNONI:

So I assume DSS is taking steps to address that?

HELLMAN:

Yes.

PANNONI:

All right, thank you.

HELLMAN:

Thank you, sir.

BRADLEY:

Thank you, Karl. We appreciate it.

HELLMAN:

Thank you, sir.

BRADLEY:

OK, moving on to the open forum who would like to say what to

whom? (laughter) Within civility, of course.

F:

I have a question. Is there an update on the states' request

for access to DOD's personal clearance information?

F:

There actually is. I mean a few weeks ago we actually out of

blue -- so I was pretty happy -- got stuff from OSD and we're

still reviewing it, a draft MOU between State Department and

DOD, to get 20 -- yeeha -- JPAS accounts for the entire State

Department. So some of those I've just spent the other day with

our personnel security folks to talk about -- I'm taking most of

them, but they're going to get a few. So but we still have to

go through the MOU process to make it kind of happen. So we are

-- it was a nice surprise. A long time coming, but I appreciate

it. So hopefully other non-DOD agencies who have the same need

will get that as well when they need to. So again, we're

working it through -- it's an MOU so you know it's State and DOD

so you've got to play that little MOU game, but it is on the

forefront so we're pretty excited about that. Thank you for

asking though. And thanks for your help too. I know industry

was a big fan of mine, I think. Or not fan, but backer of mine

(laughter) to try and get this for us. So it'll be very helpful

for us, so appreciate it, thank you.

BRADLEY:

Who's next?

STRONES:

This is Martin Strones. Could I see you, Charlie, for a moment afterwards? (laughter)

BRADLEY:

That sounds ominous, Charlie. I don't know whether I'd accept it or not.

PHELAN:

Is there a lawyer in the house? (laughter)

BRADLEY:

OK. Anything else? I'm sorry, yes, ma'am.

F:

(inaudible), industry. With the [crowd deceits?] is there anything planned to provide them in draft form, similar to what we do with the ISL, at least to industry if not just to NISCAF.

F:

ISOO has asked DNI for a conversation and we're working through coordination on that and we'll see what steps could possibly be made for more involvement.

BRADLEY:

Anyone else? Yes, ma'am.

F:

One final go-back for me. Ned, in terms of DSS has there been

any discussion about the DOD CAF falling under DSS with this new

transition of investigations?

FISH:

So the NDAA and the decision was a duty CAF will align under DSS

not later than the end of 2019. It probably will happen sooner

than that. We'll still trying to make sure we do it the right

way so that there's no lapse of mission, etc. But yes. Did I

answer your question?

F:

Yeah, end of 2019, that's good, thank you.

FISH:

So we're already planning on that, no firm time yet.

F:

OK, thank you.

BRADLEY:

OK, anyone else? OK, that will end that section of our program.

Closing remarks, they're going to be very brief. The next

NISPPAC meetings are July 19th and November 15th, same time, same

place. All right? So, without further ado, unless I hear

anything else I'm going to adjourn. All right? Adjourned.

END OF AUDIO FILE