ISOO - NISPPAC May 10 2017

[background conversation; not transcribed]

M1:

Okay. We're aware that when you say proceeds -- sorry to yell, but we need to get started. Thank you.

[background conversation; not transcribed]

Bradley:

Okay. Everybody hear me okay?

M?:

Yes sir.

Bradley:

Right, okay. Wondered if this thing was on. I am Mark A. Bradley, the I want to say new director of ISOO, though I've been here for five months. It feels a lot longer than that. So anyway, many of you I've met and actually had a chance to speak with. Others I have not, but will, as we go on. Anyway, I want to welcome you to the 56th meeting of the NISPPAC. We have, as you know from what's in your packet in front of you, a full agenda. So instead of my prattling on, I think we’re going to jump right into it.

This is a public meeting. It is audio recorded. One thing that you will hear from me probably throughout this is that it is imperative, as you speak, that you identify yourselves. What we’re trying to do is, as you know, we’re recording the meeting. What we do is, when we sit down to do the minutes, and the transcript, it is vital that we are able to identify who said what. What we’re trying to do is shorten our minutes and rely more on the transcript now, to save some resources and some time. So again, if I interrupt you, it’s not because I’m rude, it’s because I’m trying to figure out or trying to get you to remember that you’re going to be immortalized in the transcript.

For those of you here in the room, please be mindful that we have people on the phone, for teleconferencing. What we’ll do is, once we go around the table, we will ask the folks on the phone to identify themselves. Microphones around the table can be repositioned in front of anyone who wants to speak, so that everyone can hear. So, again, make sure that you’re within arm’s reach of a microphone. If you don’t use a microphone, those in the room and on the phone are not able to hear you, so that’s why we have to use the microphones. A floor microphone is also here and in the room for anyone not sitting at the table. I see one. Yeah, okay. Presenters can use the podium at the front of the room, which is over here, right? Before speaking, please identify yourself each time so that the information is captured in the audio recording of the meeting, as I said.

To start with I'd like to introduce our newest ISOO employee and NISPPAC lead, Laura Aghdam. Laura, where are you?

Aghdam:

Here I am.

Bradley:

All right, yeah. We got her from you, right?

M2:

Yes. (laughter) You're welcome.

Bradley:

Thank you, [Greg?]. This is my wingman. She's our primary NISPPAC POC, and then we'll also be coordinating the associated working group, so you'll be seeing a lot of her. So far she's been first rate.

Next I’d like to welcome our newest NISPPAC government members. They are Amy Davis, NSA. Amy?

M?:

She’s not here now. [Sorry?].

Bradley:

All right. Steve Lynch, DHS. Hi, Steve. Dr. Mark Livingston, the Navy. Doctor. Zudayaa Taylor, NASA.

Taylor:

Here I am.

Bradley:

Yeah. Hello. We welcome you and thank you for your willingness to participate on this committee. Now, beginning with the table, I’d like each person to introduce himself or herself, and then we will have those on the phone provide introductions. We’ll go from my right to you.

Sutphin:

Michelle Sutphin, industry spokesperson.

Pannoni:

Greg Pannoni, ISOO, also the designated federal officer for the meeting.

Piechowski:

I’m Carl Piechowski from Department of Energy.

Eanes:

Matt Eanes, Performance Accountability Council.

Onusko:

Jim Onusko, NBIB.

Poulsen:

Kirk Poulsen, industry.

Minard:

Keith Minard, Defense Security Service.

Ladner:

George Ladner, CIA.

Strones:

Marty Strones, industry.

Lowry:

David Lowry, Air Force.

Lynch:

Steve Lynch, DHS.

Harney:

Bob Harney, industry.

Taylor Dunn:

Zudayaa-Taylor Dunn, NASA.

Aghdam:

Laura Aghdam, again, ISOO.

Tringali:

Robert Tringali, NASA.

Loss:

Lisa Loss, Office of Personnel Management, here as the suitability and credentialing executive agent.

Wilkes:

Quinton Wilkes, industry.

Berry:

Kathleen Berry, Department of Justice.

Hanratty:

Dennis Hanratty, NSA.

Keith:

Dennis Keith, industry.

Livingston:

Mark Livingston, Navy.

Baugher:

Kim Baugher, State Department.

Davidson:

Phil Davidson, industry.

Ewald:

William Ewald, NRC.

Kerben:

Valerie Kerben, ODNI.

Richardson:

Ben Richardson, DoD.

Bradley:

All right. Where's the phone? Are we going to go around the room?

M?:

You can do the phone, if you have a loud voice.

Bradley:

(inaudible) [00:12:15] Go ahead to it, yes.

Wilson:

[Ian?] Wilson. [I'm a student?].

Kipp:

Steve Kipp, AIA Industrial Security Committee.

Ingenito:

Tony Ingenito, industry.

Klein:

Cory Klein, industry.

McLeod

Donna McLeod, National Background Investigations Bureau.

Matos:

Priscilla Matos, DoD.

Gearhart:

Lisa Gearhart, Defense Security Service.

Heil:

Valerie Heil, DoD.

Lewis:

Steve Lewis, industry.

Edington:

Mary Edington, industry.

[Logan?]:

[David Logan?], industry.

M3:

(inaudible).

[Schwartz?]:

[Lee Schwartz?], industry.

Matchett:

Noel Matchett, industry.

J. Brown:

Jennifer Brown, industry.

Kirby:

Jennifer Kirby, industry.

Haberkern:

John Haberkern, Defense Security Service.

[Viscuso?]

Pat Viscuso, ISOO.

Green:

Heather Green, DSS.

Mackey:

Brian Mackey, CSSWG.

Webb:

Rod Webb, State Department.

Hawk:

Michael Hawk, State Department.

Fish:

Ed Fish, DoD CAF.

Flaherty:

Kevin Flaherty, DARPA.

Rastler:

John Rastler, Government Accountability Office.

Yin:

Jocelyn Yin, Government Accountability Office.

Irvine:

Mike Irvine, OPIS.

Dondlinger:

Sharon Dondlinger, Air Force.

[Yen?]:

[Louis Yen?], industry.

Abeles:

John Abeles, supporting DoE.

Davis:

Christine Davis, industry.

Harris:

Jim Harris, [alternate nine?].

M?:

Won’t you be showing industry history?

Hollandsworth:

Matt Hollandsworth, Professional Services Council.

Ervin:

Jim Ervin, DHS.

Hellman:

Karl Hellman, Defense Security Service.

S. Brown:

Shirley Brown, NSA.

Hanauer:

Larry Hanauer, Intelligence and National Security Alliance.

Clay:

Glenn Clay, Navy.

Arriaga:

Dennis Arriaga, industry and NCMS.

Moss:

Leonard Moss, industry.

Novotny:

Gary Novotny, ODNI.

Bradley:

All right, now we’ll turn to the phone. Who would like to start on the phone?

O’Donnell:

Michelle O’Donnell, industry.

Brady:

Denis Brady, Nuclear Regulatory Commission.

[Tigma?]:

John Tigma, Department of Commerce.

Robinson:

Phil Robinson, industry.

Kaohi:

Catherine --

[Bryant?]:

Mike Bryant, Department of Commerce.

Robinson:

Phil Robinson, industry.

Peters-Carr:

Carla Peters-Carr, industry.

Price:

Emmett Price, industry.

Levasseur:

Nick Levasseur, DMDC.

Kaohi:

Catherine Kaohi, industry.

Martinez:

Hazel Martinez, industry.

Mustonen:

Larry Mustonen, industry.

Hines:

Helencia Hines, DSS.

F1:

We can really start in a couple minutes.

[Gale?]:

[Harris Gale?].

Bradley:

Anyone else? I guess not. Okay. All right. Let’s get into it. Greg Pannoni will address some administrative items and also cover NISPPAC action items of the November 10th, 2016, meeting. Greg.

Pannoni:

Thank you, Mark. Good morning, everyone. If I may, I want to ask the folks on the phone, would you mind sending an email, because I think a couple of names we’re overlapping. You could send it to me, greg.pannoni -- P-A-N-N-O-N-I -- at nara.gov, because we need to identify everyone who attends these meetings. I appreciate that.

So we have in your packets the minutes from the last meeting and the handouts and presentations. We made 50 copies. Most of you did get those. Of course, all the members did. So I know there was a few that didn’t. What we’re going to do, we’ll continue, of course, posting on the NISPPAC, ISOO-NISPPAC website, the minutes of the meetings along with past NISPPAC meetings. That would include any handouts and slides. But moving forward, what we’re going to do, we’re not going to be providing electronic copies for the meetings. We’ll be providing them ahead of -- in advance, and then if the attendees want to make their own copies, bring their own laptop, that’s fine. But the amount of paper we’re consuming in print is just so much that we thought this would be a better way to approach it.

Also, as the chair eluded to, about the minutes and the transcripts, in order to try to leverage those transcripts, we’re going to try something different. We are going to shorten the minutes, but post the transcripts along with the minutes, and by doing so we’ll be able to get these out much quicker than we have in the past. So we’re to start that with this meeting, and we welcome your input moving forward as to the efficiency of these changes.

So that’s the administrative information I wanted to cover. I want to move into old business and the action items, which you should see. There’s five from the last meeting. The first one was for DSS will provide an update on the cost collection methodology for NISP industry. This is actually a continuing item from our last meeting, and Keith Minard from DSS will give us a brief status update later in the meeting on that, on the cost collection.

Next, ISOO was to confirm the votes for the industry spokesperson amendment to the NISPPAC bylaws. This action is closed. The votes were submitted. We had some nonmember attendees submitting from the government agencies, so we had to go back out with a confirmation email from the recognized voting members. That was done. So the results are included as part of the minutes of the November 10th meeting. The amendment to the bylaws was approved. The NISPPAC industry spokesperson is now recognized, and her responsibilities are described in the bylaws. Okay.

The third item was ISOO was to request an email vote from the NISPPAC members on another proposed amendment to the bylaws, and this was to provide more transparency to the industry member nomination process. So the members voted by email. The results are in your packets. The amendment was approved by more than two-thirds of the government members and more than two-thirds of the industry members, as required, whenever we do amendments like that. As I say, the amendment provides more transparency to the industry member nomination process, so we think that’s a good thing. A copy is in your packet, along with the updated bylaws reflecting the two amendments.

Next, NISPPAC industry members and the CSAs were to make a recommendation to the NISPPAC chair regarding the establishment of a NISPPAC NID -- National Interest Determination -- working group after meeting to discuss the issue. So ISOO hosted a couple of meetings. We had one meeting on January 11th with the CSAs, a second meeting April 24th with the CSAs, a couple of Cognizant Security Offices -- the CIA and DSS namely -- the NID concurring agencies -- NSA, ODNI, and DoE -- and industry. Our focus was to discuss both the number of government NIDs pending, the average number of processing days, the current status of these NIDs, and also the group completed its review of the NID portion of the 32 CFR Part 2004, which we commonly refer to as the NISP implementing directive. We all agreed that the group should continue to meet until the NIPS implementing directive is in place, the update to the NISP implementing directive. There is some movement in that direction on streamlining and reducing the current time frames. The group decided it would be best if we meet again in October prior to the November NISPPAC meeting. This time frame happens to coincide with the probable promulgation of the updated NISP implementing directive, which I will speak to later in the meeting.

The last item was industry members requested an update from DSS on the status of the NISP Information System for Security, NISS, N-I-S-S. DSS will provide that update at the next NISPPAC meeting in July. Are there any questions? Okay. Thank you. Back to you, Mr. Chair.

Bradley:

Yes, indeed. All right, now we're going to turn to some new business, and that's going to deal with the process for government membership to the NISPPAC. Greg just gave you the information on the amendments to the bylaws to make the industry NISPPAC member nomination process more transparent, which I think is an excellent thing. ISOO now needs you to do some housekeeping with regard to the government NISPPAC members, to make sure that we're getting all that right.

One, identification of the Senior Agency Official for the NISP. While ISOO has current records of the agency senior officials designated under Executive Order 13526, we don't have a similarly updated information regarding the NISPPAC, the NISP senior official from each agency. So that's a bit of a problem. We don't know who to reach out to. ISOO staff will be contacting the government NISPPAC members first, and then reaching out to all the agencies to verify the NISIP senior agency official, at least who we think it is. We appreciate your anticipated responsiveness to this request. I mean, this isn’t going to work unless you get back to us.

As the director of ISOO and the NISPPAC chair, I’m responsible for appointing the members of the committee. The bylaws say that the chair will solicit and accept nominations for committee membership for representatives of the respective agencies from the agency head. That’s why it’s important that we know who the agency head, the designated official, is. ISOO staff will also be taking action to follow up with the government member agencies to confirm, through the agency’s NISP senior agency official, that the agency endorses the current members. Action item. We have endorsements or nominations from some member agencies, but not all, so, again, please send us your nominations so we can keep this thing running as it ought.

Pannoni:

If I could have one item on that, Mr. Chair?

Bradley:

You can.

Pannoni:

So, for the government members, you know, just like with the industry membership, it’s a four-year term, so we just need this endorsement once, of course. However, at the end of the four years, if the person wants to continue, we should get another follow-up endorsement. Some members from the government side may stay on way beyond the four years.

Bradley:

Yeah. And to amplify that, we will also be following up with the government members to ensure they all have met the requirements established in the bylaws. Members serve, as Greg just said, a four-year term. Their term can be extended with senior agency official endorsement, but not otherwise. Government members must also file annual confidential financial disclosures with the NARA general counsel. Three, members are expected to attend the meetings. Members may designate an alternate to attend, but with advance notification to the chair. Four, only members or the designated alternates are authorized to vote in any issue before the committee. You will see in your packets a current list of NISPPAC government members with their term dates. This was as of what we know today. Again, if you see any inaccuracies in there, please point them out to us. We will come back to this topic at a future meeting. Again, it’s important that NISPPAC be properly constituted and also legally constituted.

All right, now I'm going to turn to DSS implementation of NISP Contract Classification System, the NCCS. Lisa Gearhart, from DSS. Thank you.

Gearhart:

Hi. Thank you, everybody. My name is Lisa Gearhart. I'm the program manager and functional lead for the NISP Contract Classification System, or NCCS. I'm going to give you all an update. Next slide, please.

(SLIDE)

So for those of you who are not aware, what is it? NCCS primarily is an automated 254 system. It is 1 of 14 e-business suites within AT&L's wide-area workflow. It automates the complete process by roles and also through workflow processes. It is [PAC?] PKI required. Probably one of the biggest goals of NCCS is to eliminate the very manual and paper process of the 254 that we have now. Also NCCS will identify both primes and subcontractors for a complete supply chain view, and currently we are linked with SAM, or the System for Award Management, for all CAGE codes. We realize that some CAGE codes in industry are branches or divisions and not in SAM, so we are also adding DoE’s CSI system as well as a secondary authoritative source for registration purposes of CAGE codes, for actual performance locations, and also for subcontracting those CAGE codes. We currently have a push with ISFD, or the Industrial Security Facility Database, which is going to go away, and NISS will replace it in October, which I heard that you will get an update on that as well. I think you all will be really pleased with that. But we do have a push with some of the facility clearance information between NISS and -- well, ISFD and NCCS.

Some of the future things we’re looking at is a potential link with DISS from a contract personnel security investigation metrics perspective, across [the mean?] solution, and there are some other requirements that we’re looking at as well. I’m currently developing a FAR clause within, well, AT&L is helping me. There is a moratorium on all new rules right now, so it’s on hold and abeyance until the FAR clause can go forward. But that will mandate the use of NCCS unless an agency or industry has an existing electronic system. Then we’ll work to interface those systems with NCCS. Next slide.

(SLIDE)

As far as implementation goes, we met initial operating capability last June. We had two agencies and two industry partners that actually started using NCCS. It was great, because then they could get into the system and show us some of the issues that they were having and then get new requirements developed. By December of last year we met full operating capability. That means that every requirement that we initially had for NCCS was in the system. At that point in time we had five agencies and eight industry partners that were using NCCS. Between January and April we were in Phase 3. I'm pleased to say that DCMA registered, OPM registered, DHS has registered, DoJ has registered. OPEC has registered. I'm on Phase 4 right now, so I'll be working with Commerce and HUD -- I'm trying to think -- WHS and [PFPA?], DARPA, MDA, and several other agencies as well, which are listed on the slides. Then I've got two other phases that we'll be working with the various agencies as well. As far as the services go, I'm working with them separately, because they're much larger, so I'm trying to work with the commands and try and help them to implement within these phases as well, several Army and Navy we've been talking to, so hopefully they'll be in the system shortly.

Then with industry, I’m pleased to say that we currently have about 30 industry in NCCS right now and about 30 that are pending in various processes. Again, I’m willing to take you all on anytime, so come on and just email me, and I’ll help you to get implemented. Next slide.

(SLIDE)

So these are the roles. Much like JPAS, it’s a hierarchy, hierarchy roles, so the most important role is the GAM or the group administrator role. This is the role that’s going to actually administer the user roles and make sure that they’re active or deactivated if somebody leaves a company or an agency. Then for both industry, they call them vendors within wide area workflow, and government, you have an originator, that’s the person that originates the 254. A reviewer, which is an optional role. So, for example, let’s take government. Let’s say the contracting office is the originator, security is a reviewer role, and then maybe acquisition contracting or core, the core is your certifying official. This allows you to have whomever within the agency or industry is responsible for the 254 and at what point to be those roles. You can have multiple roles. So if you’re a small company, you could be a GAM, you could be the originator, and you could be a certifying official as well.

We’ve also added a contracting officer role, because there are certain accesses that require approval to subcontract. So we’ve automated that process in the system. We’ve also automated the facility clearance process as well. So if you create a 254 and they don’t have a current facility clearance, an ISFD, you’ll automatically get a pop up that facility clearance sponsorship is required. A lot of automation, a lot of workflow processes. Next slide.

(SLIDE)

We do have two test sites. We actually had a wonderful workshop last week. NCMS and NISPPAC actually had several industry partners that participated. It was a two-day session, so we tested [5.10.1?], and then I had about 10 government per session. We’re actually putting the National Interest Determination Workflow process into NCCS. The process worked really, really well, except we did have one minor flaw. The system is pinging every CAGE code to do a NID, which we don’t want. But we’ll get that fixed. But the process in itself, the workflow process, really did work, and I think hopefully when we get this right it will really streamline the NID process.

We also enhanced the 254 system for industry as well. They get their prime, and then they can automatically create subcontracts directly from that prime contract. They can take away security requirements. They can’t add to them. So we’re hoping that will help with any errors in the future for 254s. We created a library. We did enhance the dashboard, and then also we encrypted the data at rest, which we thought was important, since this will be the first of its kind for an automated 254 system. Let’s see, I did talk about the two-day workshop. Next slide, please. It was hosted at Northrop Grumman facility as well, so I have to thank Tony Ingenito for allowing us to come to his facility.

So basically to get a GAM, all you need to do is complete a GAM appointment letter. Right now I’m having everybody send them to me, so I can try and help them to set up their groups. Once we set up your groups it’s an easier registration process, and I think I have, yeah, my email is dss.nccs@mail.mil. Then I can help you set up either your agency or the company group. Then I will forward you registration process. I’m actually working with CDSE as well to create a job aid that will go on the FSO toolkit so that it will help you to understand how to register more easily as opposed to coming to me all the time to ask how you register. Next slide.

(SLIDE)

There is training, and there is also certain machine set-up requirements. Because we’re digitally signing the 254s within the system, java is required. Then we do have some DoD certificates that are required as well. That link will provide you all the information. If you go to the DSS website as well, the www.dss.mil, under information systems we have a link not only to NCCS but to NISS as well, and that will provide you a lot of this information. Because of the workshop we had last week, they’re helping me to create a user guide, which will also get posted, and then this will also help to streamline the understanding of how to register and work through the system. I mentioned CDSE’s job aid, the library, which we’ll post as much information as we can. Next slide.

(SLIDE)

And that’s it. Any questions? And, again, I have to thank -- NASA has also registered for the system. NGA has been phenomenal with registering and helping me to find out some of the bugs in the system.

Bradley:

Lisa, I think we have one question.

Gearhart:

Yes.

Keith:

This is Dennis Keith, administrator. Given the sort of moratorium on new rules and regulations that you mentioned, what would be your optimum timeline for the FAR clause?

Gearhart:

I really can't answer that. I'm kind of -- it's ready to go. It's just waiting for the powers that be to lift the moratorium and put the FAR clause into the *Federal Register.* As soon as that's done --

Keith:

So it's written, in other words?

Gearhart:

It’s written, it’s ready to go. I understand it’s been signed. It’s just waiting to get the word to be put into the *Register* for approval and review.

Bradley:

Any other questions? Thank you.

Gearhart:

Great. Thank you so much.

Bradley:

All right. Next we’re going to turn to reports and updates. The first one is one of, I think, keen interest. An update on the National Background Investigative Bureau. Jim Onusko, deputy assistant director, from the Federal Investigative Records Enterprise, National Background Investigative Bureau. In November, 2016, Charlie Phalen, the first director of the NBIB, reported on the stand up of the NBIB and his experience in taking on these new responsibilities. Now Mr. Onusko, deputy -- assistant director, will brief us on what’s been happening since the November meeting. Jim, please.

Onusko:

Thank you very much. Good morning, and thank you for the opportunity to be here today. The NBIB has now been in existence for more than seven months, and we’re making tremendous progress on a variety of fronts. The organization has stood up, it is now firmly established in the Washington, DC, area. This has substantially influenced our ability to communicate with customers, and that is very important to us, as we strive to meet customer needs and expectations. By introducing a higher degree of customer service, we have established the customer service advisory board, the CAB, comprised of senior executives from our largest customer agencies. The CAB serves an advisory committee of the director of NBIB to assist in the many critical decisions the director needs to make on topics such as prioritization, working down the backlog, pricing, and other important issues. NBIB will continue to leverage the background investigation stakeholders group, as well as the many other interagency groups, including the NISPPAC, to which your NBIB remains transparent and accountable to the administration, Congress, industry, and government stakeholders.

As another accomplishment, key positions have been created that provide dedicated support in many areas that were lacking in the Federal Investigation [sic] Service, namely key infrastructural areas such as a chief of staff, a full-time legal advisor, a head of contracting activity, given the heavy focus on contractor support to execute the mission, legislative liaison, a chief privacy officer now on board with OPM, an acting senior IT official, all concentrated in the Washington, DC, area, working in close proximity to the director, establishing synergy in all directions. An aggressive pace of hiring has taken place to fill these positions, while often using an interagency hiring panel. This month we expect to onboard an SES leader to our customer engagements mission, as well as an SES chief in our policy, strategy, and transformation office to provide continuing emphasis on the business process reengineering effort.

Another aspect of the NBIB is to incorporate a greater level of national security into the organization. Recently the director of national intelligence has approved joint credit for detailees throughout the IC who serve with NBIB. So we’re especially excited to advertise a number of key positions to the IC and incorporate their breadth of experience and expertise into the NBIB. Today we have our own detailee working inside the National Joint Terrorism Task Force, one assigned to the FBI’s records management division in Winchester, Virginia, and we are in discussions to put our own detailee inside the FBI’s

Terrorist Screening Center. We are also looking into leveraging state and local police as detailees in our law enforcement liaison office, to tap into their vast level of expertise.

In addition to strengthening the overall organizational structure, a new director was established to the Federal Investigative Record Enterprise, known as FIRE, which I actually lead. This entity oversees the performance of 16 million annual national agency records checks across the enterprise. The FIRE's incorporating improvements in this area, while also instituting an outreach element that looks into new and evolving data sources and opportunities to institute automation wherever possible, focused on federal records repositories, state and local law enforcement records across the country, and commercial data sources wherever possible to meet the federal investigative standards. This takes the labor burden off of the field investigator. Most recently I've worked with the -- we have worked with the Pennsylvania State Police to create a single law enforcement check process across the state of Pennsylvania, while also adding more than a dozen LE agencies across the nation to provide criminal history records information to NBIB.

This directorate is also developing the continuous evaluation business line of the future. In February of this year we introduced a continuous evaluation service that exceeds the ODNI’s minimum 2017 requirements, and we are aggressively building a more robust service and will continue to meet the DNI’s evolving CE standards from year to year. We also have a goal to introduce FBI’s [wrap back?] in the coming year, which will push real time arrest information to NBIB and provide the federal community with a centralized repository for identifying and reconciling arrest information and the associated adjudicative actions, which will aid in reciprocity across government and industry. The NBIB is also actively engaged in a social media pilot with a large federal agency, intended to inform us on how best to roll this capability out as a responsive business line to customer agencies to meet the needs of personnel security and Insider Threat programs across the federal community.

Another important pillar is the initiative to establish greater investigative capacity. Last year the NBIB successfully hired 400 FT investigators and is on track this year to hire nearly 180 more FT investigators this year. Our training center has scheduled training classes back to back through the entire year. Additionally we have expanded our contractor workforce to four vendors across the nation, and they continue to ramp up and accept more work with more than 1,091 additional contract investigators projected being on the streets by the end of this fiscal year.

In addition there have been a number of workload management initiatives introduced through collaboration with ODNI and customer agencies to increase efficiency, which include focused report writing, telephonic interviews where appropriate, centralized interview venues to minimize travel time, and the use of video teleconferencing centers, all of which are speeding up the performance of investigations. As another improvement, these new field contracts are performance based. If the contractor does not meet mandatory quality or timeliness standards, financial disincentives apply, resulting in payment by the contractor. Our contracting officers representatives have daily calls and weekly structured meetings with the contractor leadership teams, as well as quarterly performance management reviews with their senior executives. If a contractor is not meeting performance expectations, the NBIB has the authority to on ramp new contractors as well as off ramp legacy contractors.

We’re diligently working on the backlog. The steep climb has leveled off, and we’re beginning to see signs that it is receding. We have successfully cleared a temporary six-week backlog in the prescreening process, and cases are now moving rapidly forward on a real-time basis. While there’s no question that we own the entire backlog, there are federal community stakeholders who have an influence on its size. There are federal agencies who have backlogs in providing records to NBIB, and we are working closely with them to remediate those situations. This week we have sent our personnel TDY into a federal agency to perform records checks to eliminate that agency’s pending inventory. Within that particular backlog, there are thousands of outstanding records checks as well as 1,500 last leads that will be closed by the end of this week due to this initiative and effort. When it comes to the submission of fingerprints, 94% of fingerprint submissions are electronic, which is good overall, but we are certainly focused on continuous improvement, which means that 6% are submitted on paper. You do the math, that’s 125,000 per year, or 400 per day, that we receive. We’re encouraging those agencies to adopt electronic processes, as we’d certainly like to scale down our mailroom operations and pass on those dollar savings to customers.

We have made significant progress in acquiring records from other federal agencies in response to the national agency check. Last year 95% of NAC responses transmitted back to NBIB were received in under 30 days. This year we are experiencing more than a full percentage point improvement in that response rate, given that we receive approximately 4,000 new cases every day, six days per week, this is real progress in the right direction. This past month three agencies have eliminated their backlogs, and three agencies have actually cut them in half.

After the OPM data breach, IT security has been a top priority at OPM. OPM's chief information officer continues to vigorously protect, strengthen, and modernize its network. In partnership with experts from the Department of Defense, DHS, and other federal agency partners, OPM continues to take action to strengthen its broader cyber defenses and information technology systems. OPM has deployed two-factor authentication, enhanced encryption and data loss prevention, established an agency-wide centralized IT security workforce under a chief information security office, or [CISO?], among a number of other initiatives, as part of a comprehensive cyber security program.

Automation is also a key area, and we are keenly focused on a vision that involves the receipt of machine-readable data, rather than the dumb images often found today in PDF and TIFF files from all data sources throughout the establishment of APIs that flow into a reportive investigation. We are making favorable progress towards this goal with the future generation IT system, NBIS, the National Background Investigation System, in service, being built by DoD, with NBIB's requirements, providing a horizon to realize that success. Presently, we have over one dozen automation initiatives actively ongoing in a partnership with the federal and state and local communities to establish data interfaces with records repositories. These repositories span across the country and include DoD's DMDC, the State Department, US Citizen and Immigration Services, the National Law Enforcement terminal system, expansion of state law enforcement criminal history reporting information, Social Security Administration, OPM's electronic personnel files, and several others. Our automation goal is continuous improvement each quarter until we arrive at the final destination. Ultimately this will become the automated records check capable to be the filter of the future, pushing real-time information rather than pulling historical information, which will lessen our reliance on and potentially even one day replace the labor-intensive, five-year periodic reinvestigation process that we use today, which is only one snapshot in time.

DoD's building NBIS to be a smart system in an effort to make the investigation process more efficient. NBIS will be a whole-of-government solution that will be available as a shared service to the community, through the OMB security suitability and credentialing line of business. That will track an individual throughout their entire career, particularly as the employment pattern of today's public servant is likely to intersect between military service, civil service, and private industry.

Additionally, our close partnership with DoD involves the establishment of e-Application, which is currently a prototype that has been established to replace eQIP. This prototype, developed with the expertise of Silicon Valley assets of GSA's 18F, is currently undergoing prototype testing and will provide the user with more of an interactive experience, which also addresses and resolves key aspects of the investigation earlier in the investigation's process. A good example is a credit report. If the applicant can't immediately call up their latest credit report, they can address any questions in real time while filling out their application, versus expending the time and cost of explaining the circumstances to a field investigator later in the process. Our goal over time is to create a number of web services into e-Application which can collect more information validated by the subject sooner in the process.

There is a bright future ahead in a number of meaningful research development projects on the horizon, overseen by OMB, that will continual to lead to improvements that will be focused on in the coming year. As an example, to supplement the comprehensive interview techniques that are in practice today, we are engaged with a behavioral scientist from the IC through OMB's PAC PMO to institute any improvements possible in the way our investigators are trained and perform interviews to meet the needs of the future. Thank you for the opportunity to speak with you today, and thank you for each and every one in the room who protects national security each and every day. Thank you.

Bradley:

Any questions for Jim?

M3:

Just one question. Or, go ahead, you go ahead.

Livingston:

Mark Livingston from the Navy. You had mentioned that DNI had approved joint duty credit for people that go up there on assignment. I think from the military departments, we would like to consider military service members possibly doing a joint duty assignment there. I know that in L&O, certainly from the

Navy, and I won’t speak for the Air Force or the Army, but I think we would consider that a good thing from the intel community. So I don’t know if you’ve got military service members there, but we’d like to consider that.

Onusko:

These are the Title 50 agencies, and I may defer to Valerie, if she has any comments on that. Okay. So, yeah, we’ll certainly look into the definition of how that was done and whether DoD falls into the Title 50 definition, for sure. Very good.

Livingston:

It would go a long way.

Onusko:

Thank you very much.

Bradley:

Jim, one more.

Onusko:

Oh, sorry.

M?:

One more question.

Hanauer:

Larry Hanauer, from the Intelligence and National Security Alliance. It’s just your reference at the end about the ability to track people’s [newest?] evaluation and amend it. A person’s entire career, regardless of whether they’re a civilian government, military, or private sector, (inaudible). Could that conceivably enable the rapid re-granting of classified access to someone who leaves government, goes to the private sector, and then comes back, regardless of whether they’re in scope or any current definitions?

Onusko:

It will certainly foster reciprocity, or those quicker determinations can be made for access, and the derivative factors of the personnel process for sure, personnel security process.

Hanauer:

And what did you call that database that you --

Onusko:

NBIS, it’s built by DoD, based on the NBIB’s requirements. Thank you very much.

Bradley:

Yeah, excuse me, Jim.

Pannoni:

Greg Pannoni. Just one question for you. Thank you for the presentation and recognizing all the interdependencies that go on with the investigative product. What is NBIB’s projected timeline to get back to meeting the [ERP?] of 90% of the cases being completed, 40 days for the secret investigative piece, 80 for the top secret, and 150 for the PR piece?

Onusko:

There’s not a clear-cut answer to that, because in the end it’s a very difficult and complicated mathematical equation. What I can speak to is really the four points of factors that are being implemented to attack that backlog. The top four are actually the capacity equation, to rapidly raise the capacity aligned to the demand, institute these workforce management initiatives that the communities come together and say these are good risk management initiatives to lessen the labor footprint on the field investigator and perform that investigative mission, more importantly. The automation that I spoke about certainly is the fact to transfer data quicker, from one place to another, and alleviate that burden of the field investigator going to have to manually retrieve that data. And then tomorrow’s solution is that NBIS, building a smart system to actually do this, end to end, leveraging data, and e-Application providing more responsive information right up front, earlier in the process. All those, the confluence of all those factors together, will certainly impact this mathematical equation that you’re speaking to. So until those things are really getting traction and working together, really we can’t answer how long it will actually take. Policy, upcoming policy issues from DNI and the suitability executive agent can certainly affect that as time goes on as well.

Bradley:

Okay. Thank you.

Onusko:

Thank you.

Bradley:

Oh, there’s another question.

Keith:

This is Dennis Keith from industry again. This is not necessarily a question for Jim, since he is trying to get to his seat pretty quick. Okay. But I think one of the industry perspectives that need to be taken account here goes to Greg's question about when do we -- when are we well? When do we get better? Because one of the questions that we get very, very frequently is when is this affect on our hiring going to be mitigated? When is the competition for cleared [resources?] amongst companies going to diminish? When is this no longer going to be an issue that a CEO is going to have to be worried about on a day-to-day basis? So I would just offer that, you know, in addition to your four points that you made very eloquently there, and all the process improvements that you and Charlie have put in place.

Bradley:

Jim, Mark Bradley again, the chair. These, coming last year, both at times, and hiring freezes, I mean, do they impact you at all? And if so, how?

Onusko:

So, we don't feel the impact from that. We're on 100% [revolving?] on operations, so fortunately we can continue to work very aggressively through those times. Okay, good. Right. So don’t be afraid about what you read in the newspapers.

M?:

It’s important to get him in ISOO.

Sutphin:

I had one more question, sorry. Michelle Sutphin. You were talking about the backlog beginning to plateau. Are you taking into account that DSS is currently metering cases, and they’re not going to you as quickly as they should be? When those faucets turn back on and the money starts flowing, are you prepared for more cases to hit, and will you still see the backlog plateauing at that point?

Onusko:

You figure with these 179 new FTE by the end of the fiscal year, as well as 1,091 contractors, we’ll up that capacity, so that I’ll continue to accommodate the aspect of [where it is?].

Sutphin:

Okay, thank you.

Onusko:

This is a continuing capacity, optimizing [over?] performance.

Bradley:

Anyone else have anything else for Jim? All right, we're now going to turn to an update on the Controlled and Classified Information Program. Dr. Pat Viscuso, one of my associate directors, is here to give you an update on where we stand with CUI.

Viscuso:

Good morning, everyone. I'd like to first of all say that the CUI oversight liaison team has been crisscrossing the country, providing briefings at industry events, receiving your feedback, your questions. We have a special session that's been arranged for May 17th, a WebEx. It will be two hours, from 10:00 to 12:00. We'll have another one on September 13th. In between that we'll have a number of briefings presented at conferences and other types of meetings, like NCMS chapter meetings, and that sort of thing. But if you would like to participate in that WebEx, I can provide an email address. It's very simple. Mark.Riddle@NARA.gov. That's my lead for oversight, and if you would like details on how to call in, please feel free to email him. If anyone didn't catch that, I'll be more than happy to provide that information to you after this meeting.

As many of you already know, we were reaching a six-month point since the implementation date of the CUI federal regulation, which took place on November 14th of last year. By that time agencies are expected to be well into the process of revising their information security or management policies to begin implementing the program. That's sort of the foundation of what is going to go on in agencies. From the revision of the policy we'll see the revision of training, and we'll see the creation of training, CUI training, throughout departments and agencies. Agencies will be expected to assert the physical safeguarding requirements of the rule within the first year. They will also be expected to do an assessment of information systems, since there is a requirement of safeguarding in the electronic world of no less than moderate confidentiality according to NISP standards and guidelines. Agencies will be expected to do an inventory of those information systems where CUI is processed, transmitted, and stored. We'll be developing a transition plan if those systems are not at the moderate level.

Likewise, in industry, there are going to be expression of these requirements. The requirements are captured in a standards document, which I think many of you are familiar with, which is the NIST special publication 800-171. We are planning on moving forward this year with the Federal Acquisition Regulation that will address the CUI requirements for industry, for contractors. It will concentrate on several points, which we have obtained really from your feedback. We will invest in lessons learned from other efforts. We will be emphasizing the identification of material necessary to be protected on the government side, the marking of that information. We will be emphasizing the need to express specified requirements, because there are some -- there is CUI specified, which has particular requirements expressed by law, regulation, and government-wide policy that need to be expressed. So we will emphasize the need for the government to provide clear guidance on requirements.

We will encapsulate in that CUI FAR our oversight approach. We are emphasizing self-certification, and in some instances self-certification with documentation, and in a very limited number of instances self-certification with documentation and validation. Let us keep in mind the population that will fall under the CUI program in the contractor and grantee and licensee world. According to the last figures in the system for award management, there are 300,000 registrants. We estimate that at least two-thirds of those registrants handle CUI in some way, shape, and form. If we just do the mathematics, you can see that the oversight approach has to be much different from that which is in the National Industrial Security Program. The opportunity to do validation in each and every case is not desirable or possible on the government side, and thus there must be criteria by which such actions take place. It would have to be limited. It can be based on large quantity and sensitivity of program. This would make sense.

What we seek to do in the CUI program, through the Federal Acquisition Regulation that we will be working on this year, is to bring consistency in the government approach to the levying of requirements on industry. We have worked very closely with industry associations and have heard you clearly on the need for consistency and clarity of requirements.

We are working with government agencies to help them to get to the implementation phases, that they are expressed in our CUI Notice 2016-01, which is on the web. I might add, all of the guidance connected with this program is open. It is on the web. So you can see for yourselves what the implementation guidance is for the program and the various phases. We are assisting these agencies particularly with regard to training. Training goals will be developed, consistent goals. We are working with the CUI advisory council to produce this. We are also working in an implementation group that will refine self-inspection checklist criteria, which will also be available for industry to take a look at. Because as you can imagine, what will be looked at in terms of self-certification may also have some application to the private sector as well. So we will make sure that industry also has access to these inspection criteria.

In that connection I would like to mention an effort that we are working with the National Institute of Standards and Technology. We will be working later this year with them on the NIST [SP?] 800-171A. This document is an assessment guide for evaluation of compliance with the requirements of the 171. It will be developed according to the standard NIST processes of public comment, and you will have, industry will have an opportunity to publicly comment on the development of this document, which will be used by agencies in order to assess compliance with the 171.

The CUI registry continues to be updated as agencies move out on implementation. They also make assessments of what information they have been protecting, and they also discover laws, regulations, and government-wide policies which call for the protection of certain categories of information. We capture these in our work with the government agencies and note on the CUI registry any changes, any expansions of the registry and the additions of categories and subcategories.

Please be tuned to the registry. It’s www.archives.gov/cui. We are providing new resources. We are providing trifolds that can be used by industry and various other training materials that can be used by industry and government as the program is implemented. Our latest one addresses the marking of audio, photography, and videos. You can -- it has been recently posted, in addition to our general marking handbook, which addresses marking in general CUI. But please stay tuned, because we anticipate producing other useful materials. In addition, we anticipate in mid-June hosting training tools that will provide an overall training in the program.

That is the sort of synopsis of an update on the CUI program. Do I have any questions?

Kipp:

Steve Kipp, from AIA. So, Pat, you mentioned the federal rules that you proposed, they’re incredibly different. So self-certification, self-certification will have to work itself sort of thing, certification knowledge.

Viscuso:

Yeah.

Kipp:

What are going to be the limiting criteria for that? Because unless the criteria are very strict, you can usually see where everybody's going to go to the third option versus going with [a phased?] option.

Viscuso:

Well, I will say two things here. I think agencies are constrained by resources from going to any of the third option. But in those cases, we intend to establish consistent criteria for agencies in order to preserve -- as our steward, we are the CUI executive agent responsible for oversight, and so as part of our oversight responsibilities we feel that establishing consistent criteria is something that we should be doing. Yes.

Moss:

Leonard Moss, industry. Just real quick, first, I really appreciate how engaged you guys out there in industry with this process for so long, you really have. That (inaudible). My question is, do you have a tentative expectation of when you're actually going to roll out the CUI program?

Viscuso:

Well, the CUI program is rolling out now, as we speak. I would probably like to mention that on April 7th we sent a request to the heads of all executive departments and agencies asking them to report on their implementation of the program, if you'd like to see a copy of that memorandum. And also attached to that is a status form. We forward it to them. If you'd like to see that, that is on the registry. It covers policy, training, physical safeguarding, information systems, self-certification, and any additional information they'd like to provide us. But it captures where they are right now. Because, as I said before, the 2016-01 CUI Office Memorandum, which was developed with training ISOO and OMB, sets phased implementation guidelines, the first of which is coming up in May, which is the revision of agency policy.

Now, we've been in discussion with agencies. Initially we thought that there should be some additional time given for revision of agency policies, given the fact that we are dealing with very large organizations where the coordination process can take some time, especially if you take in consideration many lines of business. But in general we are looking towards this six-month deadline for revision of agency policy and have already received some draft agency policies for us to review. Yeah.

Bradley:

Anyone else have a question for Pat? Thank you, Pat.

Viscuso:

Thank you. I'd like to again thank our industry partners for the very valuable input that they have been giving to us. Know that when our team goes out to all of these conferences and meetings, your questions and your input is extremely important. I would like to, again, highlight that meeting that we're having on May 17th, two hours. Please bring any of your concerns and input to that meeting, and please see me if you would like to have the email address so you can register.

Bradley:

Thank you. All right. Now we're going to turn to the industry presentation, and Michelle Sutphin, the NISPPAC industry spokesperson, will provide the industry updates. Michelle.

Sutphin:

Thank you. Good morning, everybody. Next slide.

(SLIDE)

Thank you. I’m just going to provide a brief update of some changes in our membership, impacts the industry is seeing on policy changes, and some updates to the working groups. Our NISPPAC industry members have not changed since the last meeting. Next slide, please.

(SLIDE)

But I do want to welcome several new industry MOU members. So I would like to welcome Steve Kipp as the new chairperson for AIA. Bob [Wilgi?] for ASIS, and [Howand’s?] work for PSC. I also want to note that two new MOU groups were recently added, and a new MOU is being passed around today and being signed. So Shawn Daley, who could not be with us today, is the chairperson for the FFRDC group, and then Larry Hanauer, who is sitting over there -- thank you, Larry -- is the representation for INSA. So we’re very excited to be working with these two new groups. Next slide, please.

(SLIDE)

Heil:

Could I ask a question?

Sutphin:

Yes, ma’am.

Bradley:

Could you identify yourself, ma’am?

Heil:

Valerie Heil, DoD.

Bradley:

Excuse me, ma’am. Okay. She’s right. Thank you.

Heil:

I’m sorry. We’ve had conversations over the last year or two about the MOU itself, and it’s great that you all are updating it. When it’s final and signed, is it possible for the NISPPAC to have that information, a copy of that?

Sutphin:

Yes, absolutely. Steve has that right now, and as soon as it’s signed he can pass that to me, and we can get that to everybody.

Okay, so keeping along with the same theme that we stated in the last NISPPAC meeting, industry is really just bracing for a year of change. As you all know, we are implementing Insider Threat, the upcoming CUI, RMF, JVS, NISS, NCCS, and then DISS, that goes along with JVS. So right now we’re just kind of bracing and working together to figure out how we’re going to be implementing all of these new changes. In terms of RMF, I took the liberty of doing a quick search on clearancejobs.com this morning. I found there are 300 postings in the DC area for [ISMs?] and ISOOs. I think that may primarily be attributed to RMFs. Probably about three years ago there was only about 10 at any given time, so we’re definitely seeing a huge need right now.

Obviously we are very concerned about the growing backlog of clearances and security investigations, and we appreciate the update we just received from NBIB. Then we’re ready. We’re ready to work with you, and we’re ready to get moving on all of these changes. Next slide, please.

(SLIDE)

One of the things that has come up as new business for industry since the last NISPPAC meeting is the HSAR 2015-001 proposed rule out of DHS. Pat said very eloquently earlier today that ISOO is seeking to bring consistency in the government approach to CUI. One of the things that concerned industry about this particular proposed rule is that that may not be doing that. This DHS proposed rule is implementing four new categories of CUI that are not in the NARA CUI registry, and it is also stating that we aren't necessarily going to have to safeguard their CUI information in accordance with NIST 800-171 standards. So that brings a lot of concerns to us that we may have to duplicate some of our efforts, and there may be some added costs as we're having to safeguard CUI differently. The NISPPAC and the MOUs got together. We did submit a formal response to this. We understand the original due date was March 20th, and that was extended to April 14th. We also are aware that a [CODSIA?] letter in response was submitted as well, so we are eagerly awaiting to find out the result of our responses to this initiative. Next slide, please.

(SLIDE)

We understand that SEAD 3 was signed in December of 2016 to be implemented June of 2017. One of the concerns that industry has is how are we going to be implementing the requirements in SEAD 3? We are still waiting on implementation guidance. In this SEAD it's going to require pre-approval for foreign travel for collateral clearance holders, which is something that has never been done before. We’re interested in understanding how that pre-approval process is going to take place. Is this going to be handled by industry, DSS, or potentially other CSAs? How are we going to handle the influx of these reports that this is going to be generating? Also, we are going to have to do a major effort to reeducate the work force of the standard clearance holder into these new reporting requirements that are going to be imposed upon them. Next slide, please.

(SLIDE)

Another item that came to our attention recently was NDAA 2017, section 1647, proposed the formation of an advisory committee on industrial security and industrial base policy. It’s our understanding that this committee is going to report directly to OSD, and that DSS is going to have the lead on implementing this committee. We understand there’s going to be five government and five nongovernment entities. One of the items that the NISPPAC is asking is what role will this committee play? How will it interface with the NISPPAC? Is there going to be any duplicate of efforts, or potential to fracture the NISP with this new committee? We’re looking to seek more information at this time. Next slide.

(SLIDE)

As far as old business, obviously we are still concerned about the clearance timelines. We're definitely concerned regarding the 29,000 cases that are currently in queue with DSS. We do understand that everybody is avidly trying to work this issue. The OUSDI memo that was published December 7th of 2016 stating clearances don't expire did help, but we are also requesting a similar memo from DNI. We understand that memo does exist, but it's currently marked to FOUO, and we'd like to find some way to be able to promulgate that. Our other concerns are with the knowledge center, the wait times are in excess of 45 minutes right now, and also not very conducive to the western region business hours, so we are definitely looking to see some stabilization in that as well. Next slide, please.

(SLIDE)

NISPPAC's been very busy with multiple working groups. The NISPOM rewrite effort is still continuing and underway. We last held our meeting May 3rd of 2017 regarding the international chapter. We are definitely looking forward to seeing this be finished. We know that we still have a long ways to go, but we've been very successful thus far in our efforts here. Also, DSS In Transition, Dan Payne has reached out to industry, and we have supplied DSS with 66 industry names to participate in a working group regarding the establishment of the DSS In Transition. Sixteen of those 66 members are part of the industry IPT group, which is really the core working group. They’ve already had three meetings so far. There’s going to be another meeting in person next week, and, again, there’s not a whole lot for industry to say on this yet, as we are still waiting to see how this program is going to come to fruition and be developed. As Greg said, we’ve had several NID ad hoc meetings, and we just determined that we would be holding working group meetings until we see the resolution of 32 CFR 2004. Next slide, please.

(SLIDE)

As far as the personnel security applications go, industry is just really trying to wrap our arms around all of it and get everybody trained and up to speed. Great update on NCCS earlier today. We are a little bit concerned that currently there is only one POC at DSS to set up the accounts. Our concern is when this starts hitting and everybody wants to get on board, we hope that we can get the accounts set up quickly. We also would like to see this incorporated into the knowledge center so that people can call in and get the help they need. DISS is projected to go live for quarter four of 2017. We are curious as to how the mirroring is going to go between JPAS and DISS while we are transitioning to industry. We are still asking for who will be our industry advocate on the governance review board when we're looking at the change requests for the system. Right now we have been working with DNDC. They have supplied us with multiple report templates so that the developers for Sims, Access Commander, and ISMSi can be prepared to import the data from DISS and be able to run their reports quickly and accurately once that goes live. We also are still working to understand how training will be conducted for DISS. I know NCMS is on the forefront of that and ready to assist with that, but we are going to have to have a lot of people trained in a very short order.

eQIP, we understand that eQIP will be replaced with eApp. We are just asking that industry be a part of the test pilot so we have a better understanding of what that system's going to look like. We're going to have to train our facility security officers and personal security personnel so that they'll be able to train candidates on how to use the system, so we are eager to get involved in that.

Finally, the development of the NISS system, I personally got to sit in on a demo with that on March 1st. Clinton was there as well and some others in the room. We were very, very happy with how the system looked so far, and we're actually very excited to see that go live soon. Next slide.

(SLIDE)

Insider Threat Working Group. We've been working. We fully understand that this year DSS is just concentrating on minimum compliance and the fact that companies are getting their programs established and set up, and that they've designated their IT PSOs. There are some differences between this slide and what you may have printed, because we had some last minute changes, so I apologize for that. But it is our understanding that we are now at 99% compliance with the IT PSO appointments and 96% of industry now has plans certified, so that is great. One of the things that the working group is really going to be concentrating on going forward is how DSS is going to be rating the effectiveness of the programs. We understand that that's not going to be until primarily 2018, but we are starting to prepare our folks on what they need to know for that.

Then, finally, the Information Systems Authorization Working Group. I understand that as of today we've had a total of 34 RMF authorizations to date, an average of 45 days to approve. As I said, I think what my earlier comment this morning, we have 300 openings in the DC area for ISMs and ISOOs. It's a good indication of what industry thinks of RMF right now. It's a lot more work for us, and we're trying to get ramped up to prepare for that. I believe that's all. Thank you.

Bradley:

Anyone have any questions for Michelle?

Baugher:

Baugher, State Department. I want to -- can someone speak to this committee on industrial security industrial base policy?

M?:

I thought they were during the DoD time.

Baugher:

Okay.

M?:

[That's when we do it?].

Bradley:

All right. Anybody else? Now we're going to turn to Office of the Director of National Intelligence update. Valerie Kerben will provide an update on SEAD 3, which we just saw, and SEAD 4, National Security Adjudication Guidelines. Val?

Kerben:

Yes. Good morning. Thank you, Mr. Chairman. Good morning, everybody. I'm going to give you an overview of two of the security executive agent directives that did come out. Michelle did allude to SEAD 3. Just to also let you know, yes, it is unclassified, but this document as well as SEAD 4 is not to be posted on public websites. It's for all of us as government employees and working with you industry to use as your policy guidance, but not for public posting. So, SEAD 3 did come out June 14th. Former director Clapper signed it December 14th, and it is effective 180 days, which is coming to June 12th. We do expect agencies to work through and put together their programs and their policies, but we understand that it is a bit of a challenge and sometimes needing the resources and budget to ensure full capability. But we are going to work with your agencies and ensure that we can help you, and we'll be looking forward to working with you to get to the end result.

So the purpose of the policy is to establish reporting requirements for all covered individuals who have access to classified information and who are in sensitive positions. Agencies may impose additional reporting requirements in accordance with their respective authorities and their missions. It applies to all executive branch agencies with those covered individuals. So some of the policy highlights: all covered individuals incur special obligation for reporting information that they recognize and avoiding especially personal behaviors and activities that could adversely impact their continued national security eligibility. Covered individuals should report information to their agency, and also for pre-approval and planned activities. Failure to comply with these reporting requirements could result in administrative actions, and those, of course, are things that need to be worked out within your respective agencies.

We’re asking that reporting be done to the extent practical in an electronic format. We know sometimes it’s hard to get there immediately, but doing [it?] any way you can with Excel spreadsheets or internal case management systems, in some way, will help all of us. Then we’re hoping -- we are going to be working with the PAC and NBIS the future reporting system -- the future computer system to ensure that there is a reporting mechanism in that, whether it be in the e-Application. So there’ll be some future needs met for reporting, so the rest of the community can share. Heads of agencies should also make available resources to help determine travel risk. We want to make sure that the employees who hold clearances are not going to place an unacceptable risk to your agency if they travel to certain countries.

So the responsibilities. The security executive agent has the responsibility to monitor the effectiveness of your reporting programs and oversee compliance. We’ll be putting together some of that information in our security assessment programs when we come out to your agencies to assess, also working with the (inaudible) on some of those assessment programs. The heads of agencies are responsible for the information that they are collecting, and it has to be retained and handled according to your specific agency system of records and [storage?]. Of course, the appropriate laws, and privacy, and civil liberties have to be included when the programs are being implemented. Heads of agencies should be sharing relevant information. A lot of our personnel do have clearances with various agencies or work and support other agencies, so it will be important if one agency finds out information, it is shared with the other agencies.

Of course, necessary training. We do know that there's going to be some education on the agencies to ensure that their employees know what to report, when to report, and how to report. But I think that most of you all, or at the agencies with individuals who have clearances, reporting requirements have been part of the policies at this point. It's an expansion of certain things, but I think most of us have already been reporting. If you have a security clearance, that's a responsibility. Okay.

Also coming up, the DNI in partners with Insider Threat and our partner engagement group, we're hosting a forum next week, and it's for our government partners, CSAs, so they understand what requirements will be placed upon [them?] for the SEAD. So that is coming up for our government partners.

Okay, for SEAD 4, the National Security Adjudicative Guidelines. Again, the DNI signed this directive December 10th, and it also will be effective 180 days from the date of signature, which is June 8th. The purpose of this is to have a single common adjudicative criteria for those covered individuals, those who have access to classified, and those in sensitive positions for the initial eligibility, and, of course, continued eligibility. The requirements supersede -- I mean, the national security adjudicative criteria supersedes the last ones that I think we’ve all been using since 2005. It applies to all executive branch agencies authorized and designated to conduct adjudications.

So what’s also good about this directive is it includes all the adjudicative guidelines, the 13 guidelines, the exceptions for granting clearances, and also the prohibitions and disqualifiers according to the [Bonds?] Amendment. So it’s all in one specific directive. I think that’s about it. So that’s an overview of the two SEADs that have come out from the security executive agent.

Bradley:

All right. Anybody have any questions for Valerie? Thank you.

Kerben:

Thank you, Mr. Chair.

Bradley:

Okay. Now we’re going to turn to the man on my left here. Ben Richardson from the Security Policy and Oversight Division in the Office of the Under Secretary of Defense for Intelligence. We have the update from DoD as the NISP executive agent.

Richardson:

Thanks, Mark. Just hit a few topics here and try to cover down some of the stuff that Michelle hit on the ISOO side, on comments. So first, we do recognize that 2017 is a big year of transition, for everything from Insider Threat, to NCCS, DSS In Transition, and when we highly appreciate all of DSS -- or all of industry's support to implementing those things, and I think there's a lot of great opportunities for us down the road there. So I want to highlight that collaboration and see more of it in the future as we move forward in these efforts. Valerie just spoke to SEAD 3, and we continue to work with ODNI on that implementation, and deciding how we want to move forward on that with DoD, and how to best meet those requirements, and with DSS, with industry. So we will keep ISOO informed as we move forward and engage on that piece of it.

Michelle, you brought up the fact of the Federal Advisory Committee Acts requirements and the NDA from this past year. You know, we were somewhat surprised to see it in there as much as industry, so we are responding to that. We have met the requirements and have a charter done by 30 April that's submitted, that’s online, so you can see that piece of it. We are still reviewing it inside of DoD, to assign it to USDI. The NDA requirements asks for the secretary of defense to set up a committee to look at cyber security, industrial security, information security, physical security, and industrial base issues. That’s relatively broad, especially for DoD. USDI will most likely be the one that’s assigned the requirements for that committee, from what we’re seeing here right now, considering most of those items I just spelled out fall into USDI’s role there. Not all of them do though, so we’ll have to work very closely with CIO and with AT&L inside DoD to kind of establish those. Most likely, as you also mentioned, Michelle, we’re probably turning to DSS for kind of the implementation of that piece of it, but we’re not there yet, and we haven’t assigned it to them to date, as we establish this out.

It’s hard to predict right now what topics and issues will be discussed and focused on in that committee. Michelle, as you mentioned, it’s five government, five industry, as we decide on who is part of that committee, those individuals would come together and decide on topics to kind of go forward. Again, it’s a broad range of topics, the topics there. I know some of the intent behind this was to address issues like physical access to base with -- industry has some concerns on those. So those are slightly outside traditional things that come up in the NISPPAC and other areas. But there’s no desire or focus from the DoD perspective to fracture anything going on in NISPPAC. We have a good relationship with the NISPPAC, and we’ll leverage that as we have in the past. We’ll do everything. Again, I expect myself [and?] four people in my office to be greatly involved in the establishment of this committee, and we’ll do our best to make sure that there’s no overlap. We don’t have the time or resources for any redundancy, to say the least. So we’ll kind of keep working on that as we move forward. But, I mean, there are some industrial security issues that are DoD. We kind of sold you the issue, so those may come up, but, as I mentioned, there’s a broad range of issues outside of industrial security that this committee may look into. Time will tell when and how that will be established. It’s a five-year committee, only requires one meeting a year. Don’t know if we’ll have a dozen meetings a year or one. So we’ll have to see as the members get established and the topics get kind of worked out.

It’s also worth mentioning that there’s a Government Accountability Office engagement with DoD right now in the oversight of the NISP. We’ve begun that. They have been working very closely with DSS on that piece of it, have sent them questions and engaged with my office, Office of the Secretary of Defense, on this as it goes out. The range of issues, everything from foci to how we support [CVS?] to, you know, facility clearances, everything else that you could possibly imagine, they're asked questions about. Don't know where they'll land with different topics, as they move forward. This is the beginning engagement, from a GAO perspective on that, that perspective.

The last thing worth mentioning is DISS. You mentioned the timeline on there. Right now we are deploying DISS and working it mostly on the CAF side for the adjudication piece of it. So that the timeline for the fall, we hope to have it through for the adjudication side, for that piece of the system, done in the fall. We're slipping to the right when it comes to JPAS implementation for DISS. So the fall requirement you mentioned on your slides is probably moving to the right. I tried to get an update on that this morning. The best I could get is that the timelines will not be driven by any specific dates, but rather by events. So once DoD is comfortable with where we're at with DISS with regard to the adjudication piece of that, then we'll start build -- putting out those timelines for JPAS and other requirements. The original [debt?] with that was to move out in different components and elements of DoD and then shift it to industry on kind of the back end of that. So we are motivated to move this, because, as you can imagine, we're paying for both DISS and JPAS at the same time. So we're motivated to get this implemented, but at the same time we want to do this smartly in coordination with industry and other partners, as we move forward. Any questions?

Baugher:

I'm Baugher, State Department. Speaking of JPAS, it's been a year since I did my plea, sitting over there, to NISPPAC and everybody else, for the State Department and other non-DoD agencies to get access to JPAS. We met with your office, and we showed them CVS versus JPAS and thought at that time, which is months ago now, that there was -- because we're constrained using CVS, which is a system that's still onerous and still has issues that we find all the time. So I guess my question is, are we -- are any DoD, non-DoD agencies ever going to get JPAS access, and whatever replaces JPAS, JVS, whatever? Is anyone going to consider that non-DoD agencies have the right to have access to it as well?

Richardson:

We definitely are moving forward with the DISS piece of that. That's been a known requirement for a long time with DISS, to allow that access beyond just DoD. JPAS, we can talk, but we’re still dealing with a number of issues.

Baugher:

You’ve talked a long time.

Richardson:

I know we have. We’re still having challenges on the technical side of that and other requirements to have it beyond just DoD. There’s also funny requirements and restrictions we have internally to DoD and how we establish systems to make any changes to systems that are [sunsetting?], currently a sunset process.

Baugher:

So more to follow at the next NISPPAC meeting.

Richardson:

Sure. (laughter)

Bradley:

Yes, ma’am.

Loss:

That doesn’t make the case that --

Bradley:

Identify yourself, please, ma’am.

Loss:

I’m sorry. Lisa Loss, with OPM. I believe it’s the case though that in the future there’s not going to be a CVS and a DISS. There’s only going to be one system.

Richardson:

Correct.

Loss:

So agencies who are not DoD agencies that need access to that information will be going into the same system that DoD is using.

Richardson:

Correct. So eventually we will be -- and NBIS, I don’t have a timeline for that. There’s a lot of requirements, but we have, as discussed before, NBIS is going to be an end-to-end system. And as an end-to-end system, it would meet some of these requirements and incorporate DISS and other things that have been [reported?] on that.

Loss:

And I know that one of the user stories that was submitted was trying to get all of the information that's needed in one screen or one easily usable screen, as opposed to having to tap through screens as agencies must in CVS. I do know that was submitted as a user story. I don't know the status on that, but I'm assuming that that's going to be incorporated?

Richardson:

Yes. There are a number of great things that we have captured as requirements in building out from NBIS. The challenge in NBIS is the timeline, not the opportunities or the funding piece of it.

Loss:

Thank you.

Bradley:

Anyone else have a -- I'm sorry.

Hawk:

Michael Hawk, State Department. One of our breaks in services is [debt pay?] that we see in the CVS, and what our FSOs are telling us is in JPAS. In some cases, the senior eligibility in JPAS, but they see eligibility in CVS, or vice versa. So we have a lot of concerns with that data feed and what the accuracy of that data is after seeing it. We're concerned that that could cause some future issues with us. They're (inaudible) in other states.

Richardson:

That [grading?], and we have the same concerns, so we're motivated to try to find that. That future is at stake.

Bradley:

Anyone else for Ben? Okay. Thank you, Ben. All right, we're now going to hear from the DSS, Defense Security Service update. Keith Minard, from DSS, will give us an update on the latest DSS initiatives.

Minard:

Thank you. So some of these will address actually what Michelle was talking about earlier, and plus some of NISPPAC actions items. The first is the cost collection survey. It's been completed for FY16. It came out to $1.271 billion, which was within 1% increase of FY15. The second part of that is we are trying to update the instructions this past year, but we can't -- rolled into the OMB re-approval process, so that's something we have to reengage now that the survey's done, to revise the instructions to better align with the SF716 form, which is how governments advise on -- correlate in addressing the buckets of information in the cost reporting. So that's something we're reengaging on now that this cost collection is done.

The second one is Insider Threat. As Michelle said, we're at 99% Insider Threat officials appointed, 96% plan certified. For about 13,000 facilities, 10,000 companies, that's quite a success story in the last few months, is the implementation of NISPPAC -- NISPOM change, too. We'd like to remind everybody that May 30th is the suspense date for employee awareness training and for your cleared employees that were in access. After the issuance date, this is, remember, the requirements initial training and then annual refresher training thereafter. DSS is looking at those companies who have not yet completed the core requirements, and we are reviewing to make sure things that have not been submitted, we're reviewing for invalidation, because those requirements are necessary to support the requirements of the NISP.

We will be having a couple events coming up. There is an Insider Threat panel at NDIA-AIA, and also at NCMS. I'd like to thank NCMS. We're trying something new this year. DSS will moderate a group of industry panel members. We want to get their interaction between the peers in the audience and then their peers on the panel about their challenges and successes in setting up their Insider Threat project. We find this might be valuable to actually ask one another on how things are going, and how they did, what they did, to get their programs in place.

Greg mentioned that there will be a presentation on NISP in the November NISPPAC. But we have some milestone dates prior to that for National Industrial Security System, which replaced ISFD and EFCL. It will be role-based access to cleared industry facility information, and it will be behind NK single sign on. August 17th is the soft launch date. Users can register and test the system, and there will be training available prior to that from CDSE. During that time ISFD and EFCL will still be available, and on October 17th is the planned full deployment date and transfer of information. There will be demonstrations on NISS at NCMS.

One of the last things I have here is reference to Michelle's points on DSS In Transition. For those that have not heard and not been part of Mr. Payne’s briefings, DSS is moving from a focus on scheduled, driven compliance to an intelligence-led, access-focused, and threat-driven approach. We’ve got some information on our website. I think we didn’t get this out in a VOI, Voice of Industry, last month. But on our website dated April 10th, there’s a list of frequently asked, or there’s a facts sheet, there’s some slide information. But I’ll go over some key points on that, and we’ll make sure we get some information out to industry so they can get that information.

Throughout 2017, current industrial security oversight processes will continue. DSS will conduct security vulnerability assessments and maintain the importance placed on them. DSS will internally implement some foundational efforts in advance of the move to the new methodology, include -- this is internal to DSS -- establishing business plans at the field offices, conducting risk training, and implementing threat reviews prior to security vulnerability assessments. We are in partnership with cleared industry. We’ll conduct a series of pilots on each component of the new methodology and gather lessons learned to integrate findings and overall process. As Michelle mentioned, we actually have two industry groups with participation. One is a red team on the concepts, and the other is a focus group to validate and on a quarterly basis provide feedback on gaps and validate approaches. So we are working with two different sets of groups from industry, to work through these processes.

As of April, 2017, we launched integrative process teams to develop concepts of operations on the methodology. These IPTs, as we've discussed, are in partnership with cleared industry and continue to develop in pilot and refine new methodologies. In developing the new methodology, we'll learn as we go, make continuous improvements along the way, and apply what we learned to help develop the other components of the process. I know the big question is about when and how. Once we've tested, refined, and validate the new DSS methodology by the end of summer 2017, we'll have enough information to begin to consider on how to gradually implement a new methodology, okay. And this information is actually available for all of industry and government on our website. I believe it's dated April 10th. That's all I have.

Bradley:

All right. Any questions for Keith? Sir?

Keith:

Keith, Dennis Keith, from industry. I may have missed it. The next steps on the cost collection, [PCM?]. What was next?

Minard:

So what we had was, is because the OMB required re-approval of collection, we got behind the curve on that for updating the methodology and instructions that we’ve been working on. So now that the cost collection is done, we’ll reengage that process for this year, to renew that process and get the OMB approval to include those instructions.

Keith:

All right. The reason I asked is the point that Michelle made earlier about the confluence of the regulatory requirements that are being placed on the industry, and then somehow calibrating that cost collections survey to account for those. Because a 1% increase through cost for an implementation from this year, from last year to this year, it seems a little low given what we have experienced. So, you know, a better way to collect metrics of the cost of the new regulation would be helpful.

Minard:

I think what we’ll -- we’ll benefit from the instructions if we mirror the sub-SF716 because it breaks it out into I believe nine categories. Seven will apply to industry. Right now we ask what the total cost is and break out the percentage of manpower. The 716 instruction, if we correlate that to industry, it breaks out physical security, classified information management, personal security. So it breaks it on categories and provides a better scope and understanding in detail of what those categories would include. So that’s the intent. And it might help drive a better understanding of the cost collection and actually bring to the table a better analysis of those costs.

Keith:

Okay. Thank you.

Bradley:

Anyone else for Keith? All right. Thank you, Keith.

Minard:

Thank you.

Bradley:

Now we’re going to turn to the NISP implementing directive update. Greg Pannoni, of my staff, will give a brief status update on the revision of the NISP implementing directive formally known as 32 CFR, Part 2004. Greg.

Pannoni:

Thank you. I just want to clarify a point, Keith, that you made. The NISP update we're looking for at the next meeting in July, so not November. And also, since we're talking about cost collection, and this relates to the NISP implementing directive, there is a piece in there that includes -- right now the requirement actually derives from the 32 CFR, Part 2001, which is the directive to the classified national security information, Executive Order 13526.   And it squarely puts it on the shoulders of the executive agent, DoD, to do that, which they've been doing. But in this 32 CFR, Part 2004, the NISP implementing directive, we added some language to include the other CSAs to provide similar cost data. Well, it's going to be much smaller, of course. DSS has the preponderance of the work. It may get us to a better place in terms of more accuracy in the estimate of the cost. So I just wanted to make that point.

The update of the NISP implementing directive is making good progress towards finalization. Where it is now, it's in the process of submission to OMB for review of the mitigated public comments, which were almost entirely centered on the NID process, the comments that we did get. Once OMB completes their review, it will go back out for final interagency government review as a proposed final rule. While I cannot give an exact estimated timeframe, it’s probable that all of this will be completed by the end of the fiscal year.

But I do have to mention, as you probably know, it’s been brought up, the Trump administration has implemented what some refer to as the two-for-one requirement for publishing any significant regulation, meaning an agency must implement two existing -- must eliminate two existing regulations for every new one, or in this case a significantly updated one it wants to promulgate. This one was considered significant. That process actually took place last year during the Obama administration, the designation of this as a significant regulation. So while there are some provisions for exemptions based on national security, we are uncertain as to the exact time this will happen. It’s just an ongoing process.

But we do encourage NISP industry to express their support for the updated regulation, as we believe it does not create any new economic burden on the public, which is a key point in terms of the two for one on eliminating regulations and adding one. And also, it properly places all of the government responsibilities, vis-à-vis the NISP, in the National Policy Directive as opposed to the NISP Operating Manual. So, just again, those expressions of support could be as simple as an email or a letter to the

NISPPAC chair from any or all the NISPPAC industry members collectively or singularly, and the MOU groups. Any questions?

Baugher:

Kim Baugher, (inaudible). I just have a question. If that directive ever comes out, will DSS -- well, just because it’s out, you know. It’s not that long. Will DSS then take on another role with regard to non-DoD agencies and NIDs that they don’t do, they’re not able to do now, or not?

Pannoni:

So, there is language in there, as I recall, that, yes, DoD, DSS -- we’ll say DoD, because they’re the CSA, but ultimately you’re right, DSS -- has its responsibility as the executive agent, and the signing of the MOU with all of the non-DoD user agencies, except for, of course, the other CSAs, would in fact take on that role. That’s my understanding of the way the language is written at this time, yes.

Minard:

That’s absolutely -- that view of ENS --

Bradley:

Identify yourself.

Minard:

Keith Minard, DSS. DoD actually has the role for the signatories, and that requirement then falls into the DoD policies, like the Volume 3. Right now the directed-type memorandum addresses DoD. Volume 3, which the signatories must conform with, under a signatory NISP then implies that whole role across the board for DSS then.

Heil:

Can I also -- this is Valerie Heil from DoD. Maybe put it in the context of all the DSS CSAs once this 32 CFR 2004 is final, as an update. Are you going to have to look at their individual internal industrial security NISP policies to see what they have to update? So DoD is going to have to do that with its policies related to both ISTs mentioned, including NIDS, and then (inaudible) included consideration of the process for NIDs for non-DoD agencies. But until it’s final, we’re constrained from changing our processes or policies, until we have the final language. It is kind of a weird conundrum. So that will just stay until this is approved.

[Pannoni?]:

I skipped.

Bradley:

Anyone else for Greg? Okay. Now we're going to move into our working group reports. We're starting with the report from the Personnel Security Clearance Working Group. The working group is no longer focusing just on statistics for processing investigations from adjudications, but it's also discussing emerging policy issues that impact cleared industry. The working group will report first on its policy initiatives and then on the statistics. So Donna McLeod, from the National Background Investigations Bureau.

McLeod

Hello. I am here today to give you an overview of the SF86, the questionnaire for national security position. OMB approved the revision of the form back in November of 2016. So we, NBIB, we're working our partners to actually implement the revised form. But what I want to do today is give you an overview of what changes you will see on the form. You can actually find a version of the draft form on reginfo.gov. If you go there, you can see the content guide of the entire form. So the changes that you'll see on the SF86, we made some modifications for the routine use section of the form to conform with OPM routine uses that we just changed, so you'll see that. We made modifications to information contained in section 7, where you provide information about contact information. I think we modified something specific to the telephone number and how many numbers you’re supposed to provide, a subject is supposed to provide. The citizenship section, section 9, we made modifications in that area to collect information regarding derivative citizenship. We found a problem before that we didn’t have that information collected up front, and it took us additional time during the investigation to get it. So we modified that area.

We modified the area, section 11, where you lived, to get information regarding the land board, for rental, rental residence. We modified the education section, section 12, to provide a link to help people with determining school address. Question 13, employment activities, was modified to get information to support the need for information regarding employment. Some of the instructions were confusing before, so we took that into consideration and made a change in that area.

On section 17, 19, and 20, they’re only -- the wording changes where we changed information about marital status to include civil marriage, legally recognized civil unions. So we had made some changes to previous forms back probably like three years ago, and we’re just getting round to making the changes on the

SF86. We also made modifications to foreign countries you have visited, section 20. We clarified the clarification of official government orders. There was some confusion on that on the form about when to list government travel, so we tried to clear that up.

Section 22, police record information. Oh, we added wording about legally recognized civil marriage, civil union. And the question for drug use, we put an explanation in there to explain that drug use is illegal, based on federal law, not on state and local jurisdiction, so that change was made. Then we made some changes to the financial record to include chapter 12 bankruptcy. There was some modifications to the releases, which prior to -- we found out that the fair credit release, the journal release, the medical release, we made changes to try to have consistency on the language on all the releases, so you'll see that change.

Oh, the one change I forgot to mention is question 21. (laughter) How could I forget? That was one of the reasons why the form went out for renewal I think back in 2013. We didn't get it approved until 2016, and one of the reasons had to do with question 21. So you will see the new realized question 21 on the form, and the goal with that revision was to focus on making sure that we were getting information regarding the behavior, that we’re not focusing on the treatment. There was a lot of work done into getting that question together, getting it correct, so you’ll see that new wording on the form.

As I said, implementation, we’re working on implementing the form later this year. Our goal is probably around August timeframe. But again, if you want to see the actual form, reginfo.gov, and you’ll see the actual content guide. Any questions?

Hanauer:

Larry Hanauer from [industry?]. Do you expect that the changes will, being transferred, are you seeing now that information that applicants have to provide and the amount of time taken to requirements that (inaudible)?

McLeod

The goal in making the revisions was to only collect the information that was needed to support the investigation. So I do not think it would take additional time for the applicant to complete, but the focus was don’t have, don’t get information that you don’t need. So that’s why we try to tailor it exactly to what’s required for the investigations being supported by the form. Any other questions?

Bradley:

No one else?

McLeod

Thank you.

Bradley:

Thank you. All right, now we’re going to move into processing statistics. First we’ll hear from Heather Green, from DSS.

Green:

Good morning. I will be providing you with the DSS personnel security investigations for industry update. Due to a funding shortfall in fiscal year ’17, the PSI program budget, inventory carried over from fiscal year ’16 and constraints with two consecutive continuing resolutions, the industry investigation submissions to NBIB are continuing to be metered. Our current inventory is approximately 28,000, with the oldest initial in our inventory being at 40 days, and the oldest PR in our inventory being at about 115 days.

DSS is working to minimize the impact of contract performance by doing a few things. One is prioritizing initials and interim determinations. Additionally, on February 10th of 2017, DSS posted updated guidance on top secret PR submissions, limiting the number of T5R submissions to PSMO-I. That guidance is posted and the applicable policy memorandums are located in the new section of our DSS website.

Lastly, we have requested reprogramming and funds to bridge that shortfall gap. Now that we are under a permanent budget, we're no longer under the constraints of the continuing resolution, we are working an aggressive inventory reduction strategy and anticipate significant reductions in our timelines. Additionally, if the requested reprogramming is received, we're thinking that will be in the June-July timeframe, and the submission rate remains consistent with our projections, we will be in much better position by the end of the fiscal year, looking forward to a steady state submission rate for the initial investigations. DSS will continue to communicate our progress with our industry and government stakeholders, and we welcome any feedback or additional communication as necessary. Any questions?

Bradley:

Anything for Heather? Thank you, Heather. All right, now we’re hear from Gary Novotny, ODNI. Gary.

Novotny:

Thank you. Good morning. My name is Gary Novotny. I’m the chief of the National Security Oversight branch at the ODNI. One of the teams that works for me is a metrics team, which helps gather the timeless metrics for your national security cases. So what we do is when we -- the slide -- PowerPoint doesn’t want to come up. (laughs) Well, what the team does is kind of slice it and dice it for this NISPPAC group.

(SLIDE)

For the slides that are finally up there, what we have here, what I’m going to show you, is the DoD industry data, which is provided by OPM and the Industrial -- I’m sorry, the IC contractor data, which is provided by CIA, DIA, FEI, NGA, NRO, NSA, and the State Department. So these are -- this is the time it takes to complete those background investigations, completed on those individuals, so not an industry that may be an investigative service provider, how long it’s taken them to complete it. If we go to Slide 3, Robert.

(SLIDE)

What I thought I'd provide here is -- you heard Greg ask Jim, who was trying to get away from the podium, "How you doing on the 40 and 80-day timeliness?" So I thought we'd -- I'd provide a slide here that kind of shows you how we got to those goals real quick. So real quick. At the top there, the intelligence Reform and Terrorism Prevention Act of 2004 set your initial secret and top secret goals, which is the 40 day investigate, 20 day adjudicate. In 2008 the Performance Accountability Council and their measures and metrics subcommittee came on board and then added the initiate phase, which is the initiate 14 days for your initial and then also added a periodic reinvestigation, [a timeless goal?], and there would be 15 initiate, 150 investigate, and adjudication for 30 days.

(SLIDE)

Then in 2012, director Clapper came along. Again, my metrics team kind of collected all this data. It was kind of obvious that a secret investigation was going to take less time to investigate than the top secret investigation. So expanded that investigate time for your top secret to 80 days. So again, having the end-to-end goal's a little bit different for your initial secret, your initial top secret, and PRs. In our sub-working groups there was some questions as to how we got to these goals. I just thought I'd provide that. You'll hear Ned talk about that adjudication phase after me, and we've talked about those investigation phases. So just thought I'd put that up there. You're welcome to use this slide if you want, if you're educating people on those goals.

(SLIDE)

But what I'm here to talk about is slide 4 here. It's the timeliness metrics for, again, your DoD contractor, IC contractor data. I only went to quarter one here, because we were supposed to be here in March. So this is only up through quarter one of fiscal year '17. But as you can see, the story kind of remains the same from the last couple NISPPAC meetings. The purple graph there shows an increase in time and in timeliness for this population for your secret and your top secret. But as you can, in the periodic reinvestigation for quarter one of fiscal year '17, the time did decrease a little. You just heard Heather talk about some of the PRs and what they're doing at DoD. But this all is back in the first quarter, and you can see the volume there at the bottom had not changed for PRs. So we don't know if this is kind of the peak that Jim talked about a little bit before, or if this is just maybe a delta for that quarter. So we’re going to continue to monitor that. So there is good news stories there, at least for this population for your PRs.

(SLIDE)

What I did then, just real quick, on the next three slides is break up secret, top secret, and PRs to kind of show those three different phases that I talked to you about. As you can see here, the secret, that investigation time there is in blue in the middle, but the goal there at 74 days, obviously that part of the chart is above that.

(SLIDE)

The next slide, what I did do though is slice it a little bit differently. You know, there are still some of those legacy [ANACEs?] or [ANACIs?], whatever you call them, or [natflix?] that are still out there, your legacy cases, but then your new Tier 3 investigations. So just to kind of show the difference between the new Tier 3 and how long those are taking versus those legacy cases. So when you talk about that overall secret bar, it is kind of high. I was talking to some of you beforehand. But it may be because some of these legacy cases are still out there. So as those kind of eventually go by the wayside and we're on the Tier 3, you can see that it's taken a lot less time to investigate and adjudicate those cases there.

(SLIDE)

And then slide 7 and slide 8, again, slide 7 shows your top secret not meeting that 114-day goal. But your PRs on slide 8 there does show that decrease, and you could see it. Maybe you accounted for it on that adjudication phase, but also the investigation time for this population did go down by 12 days. That's actually all I got for you. So with essence of time, I don't want to take Ned's time here. I know he's got an exciting presentation. If there are any questions though, or also if you just want to see -- if there's any other metrics that you would like us to provide for transparency, we are able maybe to provide additional metrics here. The plan is to provide some quality metrics, quality data, of the background investigations that adjudicators are going to receive here in future meetings. But if there's anything you want to see, my point of contact there is there, and I'll open it up to any questions.

Bradley:

I have one here.

Hanauer:

Larry Hanauer, industry. Can you do some explanations for why you think the amount of time taken for these investigations in virtually every category is going up significantly?

Novotny:

I think it's just -- I don't want to speak for Jim at NBIB. Oh, I'm going to defer to Jim.

Onusko:

Well, yeah, and then actually I raised my -- Jim Onusko, NBIB here -- I raised my hand at the same time you did to make a statement, what I think is your question is actually, as we turn this corner this year and start attacking the oldest cases, our performance numbers are going to look worse, vastly worse, but it's actually a good thing because we're closing those older cases.

Novotny:

Remember, right, the IC data is other than NBIB as well. There's IC that [we're rescuing?] as well, but it's kind of the same issues that they're dealing with, the record service providers that Jim was talking about. So some of the very similar struggles that the IC is having.

Hanauer:

And do you think they'll be meeting the goals set forth in the IRTPA for this population?

Onusko:

Well, certainly it's impossible to meet the IRTPA goals for the older case population of the backlog, so we struggle through that as we attack the backlog in this transition year, and make those efforts with increased capacity.

Novotny:

And like I say, we're hearing the same thing when we're reaching out to investigate service providers for the IC agencies as well. Like I said, just kind of similarly trying to get that backlog down. You're not going to see a strong decrease until we tackle that backlog.

Bradley:

Anyone else? Keith.

Keith:

Yeah. Dennis Keith, again, from industry. The current targets were set in 2012. Is there any sentiment to relook at those based on the present realities?

Novotny:

No, absolutely. That’s what we -- we need data, we need that data before relooking at that goal. So we have the data right now. Right. What good is a goal if nobody’s making it, right? So that’s actually part of the information that we’re trying to push up to the new Director Coats to see if it’s something that he wants to expand on. We’re in discussions with that. Again, it’s working with our partners, with NBIB and DoD and that.

Keith:

The reason I asked that question is all of us are in the business of managing expectations, and if we have a goal that sits out there that is realistically impossible to achieve, that doesn’t do the whole reform argument much good at all.

Novotny:

I couldn’t agree more.

Bradley:

Michelle.

Sutphin:

Michelle Sutphin from industry. This may actually be a question that Ned may need to answer as opposed to you, Gary, but I see this as a significant difference, 146 days to adjudicate NACLACs as opposed to 14 days to adjudicate Tier 3s. What is the driver for that? Is it that Tier 3s are easier to adjudicate, or is it because we are left with the residual hardest cases of the NACLACs?

Fish:

Anecdotally speaking, because I haven't --

Bradley:

You are?

Fish:

I'm sorry. My name is Ned Fish, director of the DoD CAF. So anecdotally speaking, off the cuff, if we are receiving a NACLAC today to adjudicate, it's not a clean NACLAC. It's been hung up for a reason, and it can't be really compared with those normal routine Tier 3s that have the broader spectrum from clean to dirty.

Sutphin:

Got it. Thank you.

Bradley:

Anyone else?

Fish:

Would you agree?

Novotny:

Yes, yeah. Absolutely.

Bradley:

Ned Fish.

Fish:

Ned Fish. That’s a perfect segue.

M?:

Back to Greg.

Pannoni:

DoD CAF.

Fish:

Yeah. Ned Fish, director of the DoD CAF. Good morning, everybody. I’m reminded, I first stood in this room about four years ago today, when we pulled together the DoD CAF, and at that point in time -- some of you may remember -- I said, “Like the country song, when you’re going through hell, keep on going.” So there’s a bit, [well ever?], a little piece of hell here. But at that point in time I was speaking, looking at the slide that you might have in front of you now, at that far left, of the backlog that we, once we got done counting heads, we had in front of us at that point in time. I think you can see as we transitioned four years to where we are today that we’ve -- we, at DoD CAF, along with our partner, (inaudible) are working hard to bring that backlog down and continue to have some good successes where, as I measure the backlog, and it’s not just the dirtiest 10% or the slowest 10%, it’s also those cases that haven’t quite worked through the process as we would like them to. We’re down now around 1,400, and as of last week it was actually down around 1,200 cases.

(SLIDE)

I’ll bring your attention to that shaded part of the slide, because that brings you back to last summer. Last summer we got another brick into the DoD consolidated CAF when we brought in the fourth estate, offices of the secretary of defense and those defense agencies. We took that TSS CI population from DIA CAF, just moved over to the DoD CAF. So since that last summer period in time, in that shaded area, there was a bit of a bump up there, you see, once we moved into the shaded area, and that’s because we then counted all TSS CI clearances for the Department of Defense non-intel agency adjudications that were in the DoD CAF. So I think we have a continuing good news story. Nothing good like this happens overnight, and not without efforts, but we’ll continue leaning into this. Next slide.

(SLIDE)

I would like to add one thing here. I would like to thank NBIB, as we talked today and Jim talked to us today, for the enduring transparency on what we have coming. I’m at that back end of the process, and so the pacing items that I look at other than interim [SCIs?] that I get from PSMO-I on what’s being submitted there, we, along with the USDI and Ben and the team here, are keeping a keen eye on that growth. As you expand your investigative capacity, what adjudicative capacity do I need to have at the DoD CAF in the next year and the out years in order that that tsunami, or however big that wave is, that comes at us, we’re in a posture to receive that, and not just prolong the process. There’s no crystal ball, as Jim mentioned, on that, but we’re keeping a keen eye each year. I know Ben is going to work hard on my behalf in all the POM cycles to make sure we have the right resources.

Richardson:

I’m there for you.

Novotny:

Yeah. On your timelines, I’m not going to try to follow Gary. He does a great job on throwing these slides and timelines up. We are relatively close to the timelines, if not -- we haven’t met the [ERPA?] standards across the Department of Defense, and I think we’ll continue to stay down inside those ERPA timelines in the days to come. Next slide.

(SLIDE)

Subject to your questions, at this point in time.

Bradley:

Any questions for Ned?

Fish:

Yes.

Edington:

I’m Mary Edington, industry. One of the challenges that industry has is when sending a request for a policy, (inaudible), and then the action builds to it. It’s when you send us the DoD CAF to then verify the clearance, that’s formally being held by an intelligence agency. I’m (inaudible) it’s not a new topic or discussion. I’m wondering if there’s been some recent discussion about how to expedite that process.

Fish:

Well, I’m going to give you my answer on that, and then I’m going to see if Gary can step in here for me. Right now at the DoD CAF we adjudicate 84% of all secret security clearances in the federal government. That’s about 96% of the DoD population. So as we bring in the fourth estate and those other bricks, and as we move into, even further move to a single system in the DISS, because right now I’m operating out of five systems, you’re going to see reciprocity improve. I think it’s improved greatly already within that population. It’s that outside intel agency population where the challenges occur. Once we move to a single system of DISS, then you’ll have 96% of DoD and 84% of the federal government security clearance cases all in a single system. So it’s instant reciprocity. But there still is not -- there’s not a plan to bring the intel agencies into that same system. So I think the good news is we’re necking down the problem set. We’re just not completely covering the whole problem. Gary, anything to add on that.

Novotny:

Yeah. Gary Novotny from ODNI. Mary, there’s still no plan to incorporate Scattered Castles into this endeavor, but I think what Ned said, combining those may help. Just that small percentage that’s still going to be in Scattered Castles may help speed up that process, but there is no plan to integrate it at this time.

Edington:

Thank you.

M:

Since the R word came up --

Bradley:

Would you identify yourself, please?

Harney:

Bob Harney with industry. Since reciprocity came up, I know for several years there were multiple ways to figure out how we could collect the stamps and the metrics on reciprocity, which most of us in industry have seen, it’s gone downhill greatly along with the initials and everything else. Is there any look at reestablishing this? We can understand where that trend is going, because that is also a huge impact on industry.

Fish:

We’re working right now on the 2017 -- no, I’m sorry, it will be the 2016 reciprocity report that we owe to Congress, that we’re working on coordinating right now, which kind of talks about the average reciprocity timeliness and some of the reasons as to why reciprocity is not accepted. So we’re working on coordinating that right now. I think it’s just important to note that our definition of reciprocity is when it hits the security office and when it leaves the security office. So there’s a lot of stuff that’s up front that I think there’s some confusion sometimes that that is in our reciprocity metric, and some things after, like a polygraph or something like that. But what we’re focused on is when it hits the security office and when it leaves the security office, and what that average timing is. We can help with agency, something, and try to figure out what these upfront things are and the things afterwards. But the actual time from security office to when it leaves is a very short time. Lisa, did you have something to add? I saw you looking at me, I thought maybe you had something to add.

Lisa:

I’m just thinking.

Fish:

Oh, okay.

M:

When will that report be provided?

Fish:

It’s being coordinated right now, so, I mean, I don’t want to give you -- I mean, probably within the next few months.

Kerben:

This is Valerie Kerben, also DNI. I just want to add that also a security executive agent directive has been drafted for reciprocity policies. It’s kind of in coordination with DNI, but it will take a while to go through informal coordination and then, of course, the [OIRA?] processes are a slow part for this. But that might help out in some of this and reporting.

F:

Will that be SEAD 6?

Kerben:

It will be number 7.

Pannoni:

This is Greg Pannoni. I just thought of something, because I often say this, that 90% of policy is implementation. In just thinking about this issue, thinking in terms of how much oversight the DNI does, since you're the executive agent. Because the point about hitting the security office and tracking it that way, the fact of the matter is sometimes it never hits the security office. There's a lot of agencies out there, or at least some, that for whatever reason, they just don't give it. They don't understand when a case is right for reciprocity. We personally have experienced that here at NARA with our own security department in terms of submitting something to the CIB, because they handle our cases, and then in essence they didn't submit it because they weren't getting the fact that they could, in this particular case. So I wonder the benefits, if the DNI is doing -- what type, if any, are they doing? Are you doing oversight with the agencies, and how pro-active is that oversight?

Fish:

We are. That's another office that falls under me. In conjunction with Lisa and the suitability type agent, we do go out and conduct oversight and [substance?] reciprocity is one of those. But, Greg, you're right. It comes to education, it comes to having a solid policy that Valerie talked about, which we're coordinating and just educating about that policy on when to apply reciprocity. Not it's all about trusting your neighbor and trusting everybody. With the federal investigative standards and the implementation of that, and the national training standards that we pushed out, I mean, that's what we're all trying to get to, is standardization and reciprocity. We're not there yet, but these are a lot of things that we're trying to push forward.

Pannoni?:

Okay. Thank you.

Loss:

I will actually go ahead and answer. Lisa Loss, from OPM. To Gary’s point, when doing the oversight assessments we do tests for reciprocity. We do a sampling. We by and large find that reciprocity is being honored based on the data that was available to the agency and that we were able to look at. I think that there may be some unintended consequences of trying to apply suitability reciprocity as well as security reciprocity in terms of the reporting of the adjudications. So one thing that we’re looking into at the suitability executive agent office is do we have the sufficient fields in the reporting systems to capture all of the opportunities for reciprocity. Because I’ve seen some examples where individuals who may have been with the government, maybe their reciprocity wasn’t being honored because there was a misunderstanding as to whether or not they actually had been deemed eligible for a sensitive position because their student voting may have been reported, and they don’t look any further in terms of the security clearance eligibility versus access. So I think that there’s some work to do there that it’s, because -- it’s not that the agencies aren’t looking to see if they can apply reciprocity, it’s whether or not the data is there for them to do it. So we’re looking at that and then making recommendations for the NBIS systems, if we find that there’s additional opportunities that would help with reciprocity.

Bradley:

Anyone else on this topic? Yes, ma'am.

S. Brown:

Jennifer Brown, industry, for (inaudible). Are you tracking the operative timeliness, for the response for that? I mean, I can turn a NISP for collateral reciprocity, just very simple, in my mind, is [a lay behind?] in collateral reciprocity. Is this -- it literally goes unanswered sometimes, I mean, oftentimes. So I'm a little concerned with that.

Fish:

So culling out within the (inaudible) use the different reciprocity ones is not the easiest thing. We've looked at it. I can tell you that -- attracting ROU process and the timeliness of all our RRUs, again, culling out the reciprocity is more a manual process, to get further fidelity. It is much like Lisa said. It's not that they're -- we're waiting for data, we're waiting for files from other agencies, is by and large the largest challenge with reciprocity when we work through it at the CAF. I want to get down to the fidelity and the granularity you talked to about the reciprocity, and that's one of the things we're also looking at as far as requirements for future systems, whether it be future iterations of DISS or NBIS, so that we can get at those problems. It's one that comes up just about every six months.

S. Brown:

What about [instant?] response to the RRU, just not receiving a response at all?

Fish:

So I'd have to look at that and maybe talk to Heather to see how that process is exactly working, because I know we worked those RRUs in tandem or in conjunction with the PSMO-I. So from where I'm sitting they're being addressed. So I think that may be something I can look into. Heather, do you have anything to add?

Green:

Yeah. We'll take that back and maybe we'll report back on the next NISPPAC or ISOO working group on that. We did have a large influx of RRUs based on some guidance that we provided regarding the T5R exemption policy. We found that that wasn't the right avenue for us to receive the exemption request for the T5R submissions. So I think we're back on track as far as I know with the RRUs, but I’ll get some numbers and some statistics, and then we can report back.

Fish:

Yeah. Thank you.

Bradley:

Anyone else? Thank you very much. We’re now going to hear from Perry Russell-Hunter (inaudible).

Russell-Hunter:

Thank you very much. Do I have any time remaining?

F:

No. (laughter)

Russell-Hunter:

(laughs) Fair enough. So very quickly then. The good news story is that in Michelle’s slide, and this is a number that goes back to March when some of us met, we were down to 145 industrial cases for legal review. That’s what happens before a statement of reasons can be issued. There’s lots of good reasons why we do that, by the way, and particularly as we go into continuous evaluation, which will have the risk of false positives. We want to make sure that when we issue a statement of reasons we actually mean it, and that it is serious. That number is down this morning to 130. That’s basically five legal reviews per lawyer at DOHA, so we are in good shape. That has also been the result of continuous work and collaboration with the DoD CAF to ensure that we’re processing these cases in an efficient way.

I also want to talk just briefly about the R word, about reciprocity, because we are very conscious as we move to implement the SEAD 4, the new adjudicated guidelines, there’s some very good things in these new guidelines, including a reform of guideline C to confirm to ICPG704.2, and what was the intelligence community standard. To get everybody on one, literally one sheet of music for adjudication and due process was critically important. It took a while, but we got there.

One of the issues that we continue to see as we try to implement, in both the current guidelines and the future guidelines, is the concept of issue resolution, because at the tail end of the process, if issues have not been resolved by the application, the investigation, or the adjudication, then they end up being done in the hearing process, which is probably not the most efficient place to be doing issue resolution. So one of the great questions that Donna got was the question about, well, is the SF86 going to be a more burdensome form. The answer is to a certain extent clearance reform envisions a burdensome form, because we’re trying to gather information up front that’s going to lead to a faster investigation, a faster adjudication, because the issues that we know are going to be issues have been already identified and potentially resolved through branching questions. Also industry now knows that there’s a best practice, which is to put mitigating information into the SF86. FSOs know, as they sit down with the subject, under NISPOM 2-202 that they have an opportunity to get that mitigating favorable information into the form so that we can get to a favorable resolution faster in the process. Then ideally the case never has to come to DOHA. So I wanted to give that further answer to your question to Donna.

With that, I also, I’m reaching out to ODNI, because one of the aspects of SEAD 4 is there’s an Appendix C which refers to the three traditional exceptions to reciprocity -- condition, deviation, and waiver. Those are, of course, bedrock principles of the intelligence community, and their application of risk management to a specific person and a specific job. I’m not so sure that was intended to apply to collateral industry, secret clearances, and top secret clearances. If it were applied, I’m not sure it’s good for reciprocity. So I’m going to be asking for some clarification on that issue, because we -- as the main applier of these standards for collateral cleared industry, we want to make sure we’re doing that right come June 8. That’s all I’ve got. Thank you.

Bradley:

Any questions for Perry?

Russell-Hunter:

Yes, Donna?

McLeod

(inaudible) Just one to follow up. Perry just said [in timing?] the form, so where additional questions may come in the future, I just want to clarify that the form that will be out this year, there’s not much more beyond what was previously on the form. As the form evolves, more questions may be addressed up front, but not on this collection right now.

Russell-Hunter:

Yeah. And also, on question 21, which is probably the biggest substantive change to the form, the reform of the question is to make it less intrusive. For the past 20 years, the SF86 in question 21 had been asking for all treatment or counseling and then narrowing that with a few public policy exemptions, which included, more recently, returning from a combat environment or being a sexual assault victim. What has happened now, as a result of this reform, is we're narrowly focusing on actually risk-related behaviors and diagnoses as opposed to asking for all treatment or counseling. So it's been a long road to get to this point, but we finally reached it. So that's a good news story for everybody. Thank you.

Bradley:

Yes, ma'am. You have a question?

S. Brown:

Debbie Brown, industry.

Russell-Hunter:

Yes.

D. Brown:

Is there -- we had wanted something about passports, foreign passports, working a lot with the State Department, (inaudible), their IRB, (inaudible) backgrounds. So we have to link their passports right now, and we have (inaudible) to put in there, or their assistant, to brief with, if they want to be granted interim clearance. Is that...

Russell-Hunter:

So that’s a great question. In fact, the current adjudication guidelines that are in force until June 8th talk about the mitigation being the surrender, destruction, or invalidation of a foreign passport. That will go away on June 8th when we go to what was the ICPG704.2 standard, but will become the standard for everybody, which is the idea that you just have to tell us that you have a foreign passport, and then that can be done as a form of risk management as opposed to expecting sort of a rote destruction, invalidation, or surrender of the passport. Again, that is the end of a long road of policy development.

D. Brown:

That one no longer resulted in interim [clearance?]. Why is that, in itself, being denied that they had retained a foreign passport?

Russell-Hunter:

Well, so one of the best practices that industry figured out on their own was that right now the best thing to do was to make sure, if somebody was reporting on the SF86 that they had dual citizenship, which, by the way, by itself is not disqualifying, but having the passport was, that reporting on the SF86 that the passport had been surrendered, destroyed, or invalidated was leading to the grant of an interim clearance. So that became a best practice. Now, going forward, that will be less onerous for industry and for passport holders, the key being that the passport holder be honest about having the foreign passport. Because now the disqualifying condition is failing to tell us that you have a foreign passport.

D. Brown:

So there's an education for this challenge?

Russell-Hunter:

Absolutely. But --

D. Brown:

Thank you.

Russell-Hunter:

But an important reform. Thank you.

Bradley:

Thank you, Perry. All right. I note that the statistics for DoE or DoD and NRC, background investigations, are in the handout packets. Okay. Now we're going to move to the Information Systems Authorization Working Group report. It's going to be done by Karl Hellman, report for DSS, and then John Abeles, from DoE, will report on DoE's process.

Hellman:

Thank you, Mr. Chairman. Karl Hellman, Defense Security Service. The first thing I'd like to do is thank the ISOO for hosting our working group and specifically Robert Tringali and Laura Aghdam for keeping us on point and moving forward, and we greatly appreciate your support.

(SLIDE)

We'll go ahead. I'll run through the slides rather quickly. There's things I'm going to update on, our process manual, our transition, things that we're improving on, and then finally some metrics and training. Next slide, please.

(SLIDE)

The DSS Assessment and Authorization Process Manual. In March 31, 2017, we released version 1.1. Our goal is to update and track updates every six months, so we have a version 2.0 that's already in schedule for a September 30th release. Through the working group, we have been planning -- we've been working with the industry members of the working group to work with NCMS, work with NDIA-AIA, to provide for the working group to be a centralized point for industry input. It allows us to avoid duplication, and it also allows for the industry members of the working group to adjudicate some of the requests ahead of time and then will work with us. So it gives us a point of central feedback, and it gives, for DSS and industry, a central point for that. Next slide, please.

(SLIDE)

Our implementation plan, for those of you who know, October 1, 2016, we implemented phase 1 of our transition to RMF. We began with standalone systems, whether they be multi-user, single user, standalone systems. DSS got -- we met internally in January of this year to assess how that implementation plan was going, and we had a meeting, our working group, in February with industry. We are proposing that phase 2 of our implementation plan begin January 1, 2018, and phase 2 will include our network systems. So at that point all systems beginning January 1, 2018, will conform to the NIST risk management framework security controls. So we've been working with the working group and other folks. Next slide, please.

(SLIDE)

Recent activity we've had at DSS, we've created an additional template in Excel format. We found that we had a variety of industry ISSMs who were more familiar with the Excel-type format for an SSP, so we created that. We are hosting the [SPA-WAR SCAP?] compliance tool and configuration checker within OBMS, so that's available for industry to use. Those are the tools that DSS is using to do validation of systems, so it allows industry to download those without having to have a CAT card. They can download them from our site and use them to check their systems before we come out. We've also created an automated configuration tool for industry's use. This is really geared toward those ISSMs and those facilities that don't have a great deal of information security expertise to allow them to take very simple systems and configure them to the NIST RMF framework security controls. We're also hosting that within OBMS. So just from an information standpoint, the SCAP tool and the compliance checker, they've been downloaded about 1,100 times out of our business management tool, and the automated configuration tool has been downloaded over 300 times out of our business management system. So we’re seeing some value. Those have been up just in the last four months. So we’re seeing some good value that industry’s finding with that.

Then finally, we initially in our version 1.0 of our process manual, we had asked industry to create POAMs, plans of actions and milestones, for their transition to the risk management framework of information systems. We removed that requirement because that’s really an internal industry planning. It’s something that we don’t need, we, DSS, don’t need to track.

(SLIDE?)

Metrics. These are metrics for our FY17. Again, when we began, October, and I will tell you that the first two months that we were under the risk management framework submission guidelines, we received zero submissions. So these are literally the four months, over the past four months. Submissions are starting to increase. You see what’s under DSS review, what’s under an industry action, that means they’ve submitted it to DSS, DSS has returned it to industry for updates, corrections, or more information, what we’ve authorized, and then what has ultimately been cancelled. That industry has determined that they’re not moving forward with the system.

The dates for authorization decision, that’s a DSS timeline. So that does not include -- if we’ve returned something to industry, and industry takes 15 days to return it back to us, we don’t count that time. Our overall, the overall metric that we’re looking at for the time, from an industry submission to a DSS authorization decision, is probably closer into the 65-day time period. It seems it’s a little bit -- that is much higher than our previous, what we would make an authorization decision in 30 days, but it is a very -- I will tell you, it’s a wildly fluctuating number, because it’s such a small sample. It’s only 34. So we authorize normally about 2,000 systems a year, so 34 leaves us a lot of room where one or two extended authorization decisions really impact the overall number. Next slide, please.

(SLIDE)

Training products that are coming out for the NIST RMF control. I will let you know, from CDSC, that the dates have slipped to June for the introduction to the NISP assessment and authorization process, and September for the applying assessment and authorization in the NISP. That’s been due to some budgeting considerations where we've been under the CRA, and CDSC has been unable to finish up some contract work. I believe I will, Mr. Chairman, pending, I can take questions now, or I can yield my time to my colleague with DoE for his presentation.

Bradley:

No, Karl, it's supposed to be Democratic. I mean, anybody have any [teeny?] questions for Karl?

?:

I just have a quick comment. You look at the metrics and -- appreciate, Karl, what you guys are doing on the RMF. I think this is just transitional, but you basically have between the cancelled and the return to industry for more work 50 out of the 137, greater than one-third. We were sensitive, the working group, sensitive to that. We realize that number's got to be driven down substantially. So, just a comment really.

Hellman:

Yeah, good. That is something we looked at with version 1.1. It's trying to provide some more direction, and version 2.0 will -- again, we're taking lessons learned and incorporating that in there.

Bradley:

Anything else for Karl? All right, John.

Abeles:

Thank you, Mr. Chairman.

Bradley:

You're welcome, sir.

Abeles:

Thanks. My name is John Abeles. I'm briefing on the Department of Energy approach to classified authorization. Let me give you a few words about DoE before I get into the authorization process. DoE has a number of diversified missions. So you have missions that range from nuclear stewardship, to environmental management, to scientific exploration. So there are a lot of different approaches being used. So the way we look at most of our standards and our approaches is we establish high-level goals and mandates, and then we allow the senior departmental managers who have line management accountability to come up with the implementation mechanisms for each of those.

The other thing that's interesting about DoE is we use a number of contractors. We use a concept called GOCO, government operated -- sorry -- government owned, contractor operated. So what this means is that although the contractors receive direction from energy and federal people, they do most of the actual work implementing that, and you see that in a number of DoE laboratories and sites. So they're mandated through a directive system at the high end for federal and contractors. The mandates start with policy orders, manuals, and that sort of thing. If you look at those documents, they are broken basically into two pieces. Most of those are mandates that apply directly to the federal government, the federal staff, and there are contractor requirements documents that supply implementing details and implementing requirements to the contractors, which they have to respond to.

And for cyber security, there are two real policies and orders. Policy 205.1 and Order 205.1B are the two documents that really specify what people have to meet in terms of classified and unclassified cyber security. DoE cyber security has been, for years, and currently is based around the NISP risk management framework. So risk management is the center of the approach. Next.

(SLIDE)

So mandates. You start with risk management, and you look at what’s done. So our risk management includes the training, the assessment, and responding to risks, and so risk appetite, risk tolerance, is set at a high level. It’s up to the senior departmental managers to identify how they’re going to implement that within their organization. From a governance standpoint, governance is both federal and contractor combined, so industry is actually combined with them. There are a number of different governance organizations that the OCIO works with, the National Laboratories, the federal facilities, the program offices, and then a number of the different internal offices. For example, OCIO, CFO, those support offices at headquarters. IG, GC, so those were all pretty common.

If I look at the basis for what we do in authorization and assessment, it comes down to implementing NIST 80053, 53A, which -- to measure the controls, and then CNSI 1253, and we’ve actually worked with both the intelligence community and with NIST in the development of these documents. So we’re intimately familiar with them.

Finally, implementation. Because the wide diversity of -- (next slide).

(SLIDE)

I’m missing a slide. You have slide implementations tailored?

Taylor:

There isn’t a slide for that.

Abeles:

Oh. Okay. Well, this is missing a slide, I guess. Sorry. Implementation is tailored by the OCIO. So, for example, if I look at the OCIO, which covers headquarters and covers many of the program offices at headquarters, you have the order, which sets up the mandates, or sets up the requirements. Then the OCIO develops a series of their own documents, a risk management implementation plan, so each of the SDMs, each of the CE department, the managers, is charged with developing, of identifying how they’re going to implement the risk management framework within their organization, then coming up with other documents, for example, a program and cyber security plan, which spells out the specific controls, the specific requirements, the things that they need to have to address risk. I guess I’m open for questions. I tried to do this quickly anyway.

Bradley:

All right. Anybody have any questions for John on DoE.

Pannoni:

Just real quick, John. You've got this thing marked unclassified deliberative pre-decisional. I don't want the group to have any concerns about how to handle this thing. It seems a little unusual, but is DoE okay? You know, we've got this up here now.

Abeles:

Yes. Yes. It's just, that's what I was told to use for this, quite honestly.

Pannoni:

Okay. So we're going to largely ignore that. Yeah.

Abeles:

That's okay. (laughter) I should ask Mr. Chair to concur.

Bradley:

We've already gotten there.

Abeles:

Okay. All right. Thank you, [Canada?]. Where I see it, anyway. We do CUI, we do classified.

Bradley:

We've to our last working group report. That will be the Insider Threat Working Group. Greg Pannoni from ISOO.

Pannoni:

Thank you. I'm going to be as brief as I can. So the working group, we've met now three times, last in February, with CSAs and industry. Our goal continues to be facilitate consistency and implementation of NISPOM Insider Threat provisions for contractors across the CSAs and to maximize the sharing of relevant and appropriate Insider Threat information among the CSAs and industry, as applicable. So the working group continues to provide a forum for frank, open dialogue between both government and industry. Government agencies talk about their expectations, industry about theirs, and progress in setting up Insider Threat programs. Everyone agrees that the working group should continue at least through these early stages of program implementation for industry, and it's too early yet to identify any quality measures for industry programs and results.

I will say one consistent theme across both government and industry is the difficulty of information sharing. As we know, this is a basic tenet of effective Insider Threat programs. So it is an item that the working group will continue to discuss and attempt to find and propose methods for improving information sharing.

And last, because of the overlap with Insider Threat and personnel security matters, at our next meeting we are going to hold jointly in June with the personnel security working group. Any questions? Yes, Dennis.

Keith:

Dennis from industry, Dennis Keith from industry. Given what we heard today about SEAD 3, is there consideration being given in the Insider Threat working group about those reporting requirements and so on?

Pannoni:

Yes. SEAD 3 is even bigger than Insider Threat, I would say, but it does present challenges for industry. Number one, we have to figure out the vehicle for actually making it effective for industry to start doing that. That, in and of itself, is something we’re discussing right now. With the policy coming on line June 17th, typically it’s the NISPOM itself that’s the vehicle, so we have to work through that. Other things, for example, there’s a passage I believe in the SEAD 3 that says for the covered individual, the report, any CI concerns, which appears to me beyond just the company, the employees of the cleared company, which we’ve always looked upon as a basis for reporting requirements, with the exception of suspicious contact reporting. So we have to figure that one out. Are we saying here that for NISP industry we’re expecting cleared employees to report indicators of CI concern, or individuals of other companies? That’s a real challenge.

So I don’t really have the answers for you today, but I think we are sensitive to all these points. And just the foreign travel, in and of itself, what’s official foreign travel, what’s unofficial, what the forms of pre-approval have to, how they have to occur. I think we have to figure out a way to do this as efficiently and still be able to garner the information that is relevant to an Insider Threat concern. I don’t have the answers honestly, but that’s as much as I can say.

Keith:

Thank you. In summary, it’s hard.

Pannoni:

We can do it though.

Keith:

Okay. Damn right. Thank you. Thank you.

Bradley:

Anyone else have any questions for Greg? All right, now we're going to turn to our general open forum discussion, which exactly says what it says. Anybody like to say anything, discuss anything? Raise your hand. Sir? Would you identify yourself?

Lawrence:

Mitch Lawrence, industry. In the past, [performance.gov?] has been posting the score card on the basis, and it has been posted since Q4. I just wondered if that's been discontinued, or are you getting that?

?:

We collect them up.

(inaudible)

Eames:

Matt Eames, PAC. I'll repeat his question. He was asking if the performance.gov is going to continue. There hasn't been a posting since Q4. The new administration came in. They took at look at whether it was an effective measure mechanism. They've come to a decision that it will move forward, and they're in the process right now of assessing what the capitals will be. So it's in flight right now, determining what will be a capital, what won't, based off the priorities of the new administration. So performance.gov will continue to exist and operate underneath the [PIC?], but the goals may change. So stay tuned.

Lawrence:

Okay. Thank you, Matt.

Eames:

You're welcome.

Bradley:

Anyone else like to raise anything at all? Yes, ma'am.

Taylor Dunn:

Zudayaa-Taylor Dunn, NASA. I understand the question about intern clearances. What is the timeline for interim clearances, and is there -- I believe Michelle said that they’re being metered for submission. What is that process?

Bradley:

Who would like to take that on?

Minard:

Heather Green from PIC -- this is Keith Minard from DSS. Heather Green from our [PISMA?] office left, but right now we’re metering based on our financial resources yet available to us to process. I believe interim clearances are being processed through the metering as a priority, but we still are relying on the backlog at OPM for the investigations. But as long as the interim clearances doesn’t have any derogatory information, as long as the submission doesn’t have any interim derogatory information, we are normally processing them interim access for secret. At that point, due [BSMO?].

Bradley:

Anyone else? Going once. Okay. The end of the open form discussions. All right, closing remarks of the chairman. I thought this was a very good meeting. Obviously you all have a lot on your minds, and, again, it illustrates and underscores the value of the NISPPAC to be able to raise this in a forum where we can actually come together and discuss this kind of thing and you can raise questions. So anyway, well done by our presenters and also by our people who raised questions.

The next NISPPAC is scheduled for July 12th, which is right around the corner really, and then November 14th here at the Archives, in this room. Unless there's anything else, I'm going to adjourn the meeting. Adjourned.

END OF AUDIO FILE