Producer: Welcome and thank you for joining today's NISPPAC meeting. Let me now turn things over to Mr. Mark Bradley, the Director of the Information Security Oversight Office, as well as the chairman of the NISPPAC.

Mark Bradley: Thank you very much for your kind introduction. Morning, everybody. Welcome to the 65th meeting of the National Industrial Security Program Policy Advisory Committee, commonly known as the NISPPAC. We appreciate your patience as we navigate through these difficult times. This is the second NISPPAC meeting that's being conducted 100% virtually. At the conclusion, we will provide a survey to find out how this worked for everyone as we did for the last meeting. We've incorporated the comments you were kind enough to send along last time. Again, if you have anything else we can do to improve, please let us know.

If you'd like to be contacted regarding survey responses, please include your email in the comments box so we can get back to you personally. If you'd like to receive information on future NISPPAC meetings, my staff is no longer sending calendar invitations. You'll be able to get all the pertinent information about the upcoming NISPPAC meetings by signing up through the ISOO Overview blog or going to the federal register. Please send an email to NISPPAC, that's nisppac@nara.gov, if there are any questions, any problems about accessing that.

The available agenda, slides and biographies can be retrieved by doing a Google search for NISPPAC Records on Committee Activities and clicking the first link. Again, do a Google search for NISPPAC Records on Committee Activities and click the first link. Not all speakers have slides or biographies. This meeting will be through the phone line only. This is a public meeting, just like all our NISPPAC meetings are that will be recorded. The recording along with the transcript and minutes will be available within 90 days on the NISPPAC Reports on Committee Activities page I just mentioned.

We're planning on a five-minute break during the middle of the meeting, so I will flag that as we move closer to that. I'll begin by taking attendance for the meeting from the government members first. I'll state the name of the agency then the agency member will reply by identifying themselves. Once I've gone through the government members, I will then proceed with the industry members. After the industry members, I will then proceed to the speakers.

Please keep your phone on mute until I have stated your agency. If you do not have a mute button, please hit *6 on your phone to mute and unmute. As a reminder, NISPPAC members, speakers I assume you should have called on the speaker line, not the participant line. We're going to start with a roll call. I'll start with the ODNI. Who is present for the ODNI?

Kyla Power: Hi, this is Kyla Power.

Mark: Alright. Welcome. You're replacing that Valerie Kerben today, right?

Kyla: Yes. Unfortunately, Valerie wasn't able to make it today.

Mark: Not a problem. Okay, thank you. DOD. Who's representing you today?

Jeff Spinnanger: Good morning. This is Jeff's Spinnanger.

Mark: Hey Jeff, how are you doing?

Jeff: Very well, sir. And you?

Mark: Good. Just like you. Okay. Department of Energy, who is representing you?

Tracy Kindle: Good morning. This is Tracy Kindle.

Mark: Morning, Tracy. Right. NRC?

Chris Heilig: Good morning. This is Chris Heilig.

Mark: Hi Chris. DHS?

Rob McRae: Good morning. This is Rob McRae here. I am replacing Mike Scott.

Mark: Okay. Hi, Rob. Welcome. DCSA?

Keith Minard: Keith Minard. Good morning.

Mark: Hey Keith. CIA? Anyone from CIA on the phone call? Apparently not. All right. Department of Commerce. Department of Justice.

Christine Gunning: Good morning. It's Christine Gunning and Kathleen Berry.

Mark: Hi Christine, Kathleen. NASA?

Ken Jones: Good morning. Ken Jones here.

Mark: Morning. NSA, National Security Agency.

Shirley Brown: Good morning, Shirley Brown.

Mark: Hi, Shirley. Department of State.

Kim Baugher: Kim Baugher. Good morning.

Mark: Morning. Department of Air Force.

Jennifer Acquinas: Jennifer Aquinas here from Air Force.

Mark: Morning. Department of Navy.

Randy Akers: Good morning, Randy Akers from Department of Navy.

Mark: Hi Randy. Department of the Army.

Jim Anderson: Good morning. Jim Anderson, Department of the Army.

Mark: Morning, Jim. Now, I'm going to turn to the industry members. Heather Sims. Are you present?

Heather Sims: Good morning. Heather Sims.

Mark: Dan McGarvey.

Dan McGarvey: Good morning. I am here.

Mark: Dennis Arriaga. Are you here?

Dennis Arriaga: Good morning, sir. Dennis Arriaga here.

Mark: Good to hear from you, Dennis. Rosie Borrero.

Rosie Borrero: Good morning, Rosie Borrero here.

Mark: Okay. Cheryl Stone.

Cheryl Stone: Yes. This is Cheryl Stone.

Mark: Hi Cheryl. Aprille Abbott.

Aprille Abbott: Yes. Good morning. Aprille Abbott here.

Mark: Derek Jones.

Derek Jones: Good morning. Derek Jones is present.

Mark: Great. Tracy Durkin.

Tracy Durkin: Hi. Good morning. Tracy Durkin is present.

Mark: Now, I'll do a quick roll call for our speakers. William Lietzau**,** are you here? No. Let's hope he shows up. Stacy Bostjanick**.** Are you here? Perry Russell-Hunter. That's an inauspicious start for our speakers. Devin Casey.

Devin Casey: Good morning, Mark.

Mark: Hey, Devin. Thank God you kept me from going 0-4. Donna McLeod.

Donna McLeod: Good morning, Donna is here.

Mark: Great. Selena Hutchison.

Selena Hutchinson: Good morning, everyone. I'm here.

Mark: Great. Lovely. Is anyone else speaking during the NISPPAC that we have not heard from, or I don't know about. If so please speak now.

We're expecting this to be a fairly large audience. I think last time we had over 800. Because of this, we will not be taking questions. Please email NISPPAC, nisppac@nara.gov with your question or questions, someone will get with you offline. Somebody from my staff.

Only ISOO and NISPPAC members will be authorized to ask questions through the meeting. We request that everyone identify themselves by name and agency applicable before speaking each time for the record, as I said before, this meeting is recorded so it's important that we able to match the speakers up with the question or comments.

Again, as I always do, I want to remind government membership of the requirement to annually file a financial disclosure report with the National Archives and Records Administration, Office of the General Counsel. The same form of financial disclosure is used throughout the federal government, OGE Form 450, satisfies reporting requirements. You're not being asked to do this to twice.

We have several changes to the NISPPAC membership I want to bring to your attention. Now we'd like to welcome Matt Roche as the new alternate representative from the Defense Counterintelligence and Security Agency. He's replacing Karl Hellmann. We'd also like to welcome Felicia along with her alternates, Michelle Carlyon, and John Keesling from the Central Intelligence Agency. Mike Scott, the primary with the Department of Homeland Security, has left us. He's been replaced by Robert McRae. Randy Akers, the alternate with the

Navy, will be leaving us in about a week. Replacement for him has not yet been named.

We are also welcoming our two new industry representatives to the NISPPAC, whose terms started October 1st, 2020, Derek Jones and Tracy Durkin, replacing Bob Harney and Brian Mackey. For those departed members, thank you all for your contribution over the years, we look forward to continuing the work you've done with the new representatives who I've just named.

As a reminder, the agenda slides and biographies for speakers are located on the NISPPAC reports on committee activities webpage. Greg, I'm going to turn this over to you. You're going to address the status of action items from the July 15th, 2020 meeting.

Greg Pannoni: Okay. Thank you, Mr. Chair. This is Greg Pannoni. Good morning, everyone. First, the NISPPAC minutes from the last meeting. Those were finalized on October the 10th and they're posted on the ISOO website. Then we had four action items. The first was for industry to provide instances of delayed processing of National Interest Determinations, otherwise known as NIDs, by cognizant security agencies and offices also known as CSAs and CSOs. This is considered closed due to the elimination of the NID requirement for a substantial majority of otherwise affected NISP contractors, and this is fomented by Section 842 of the National Defense Authorization Act of fiscal year 2019 that removed this requirement for entities that were under the National Technology and Industrial Base. That was action item 1.

Action item 2 was that ISOO would convene a NISPPAC NID working group with industry representatives. A government only meeting occurred on September the 16th. The next working group is scheduled for December 9th and it will include industry representation. We've also decided to rename the group, the Foreign Ownership Control or Influence group, or FOCI working group, to be more representative of the issues that we're discussing. It's not just about NIDs.

Action item number 3 concern DCSA's Industrial Security Letter, also known as an ISL, on insider threat. The ISL is in the process of internal formal coordination at DCSA with the Office of General Counsel. Once promulgated, this ISL will replace ISL 2016-02 and DCSA will engage with cleared industry through the NISPPAC to update tools, resources, and required training.

Then action item 4 was to schedule another insider threat working group meeting. This action is considered closed as the meeting was held on September 2nd. Do any NISPPAC members have any questions about the status of action items? We're hearing none, back to you, Mr. Chair.

Mark: I thank you Greg, for that summary. At this time, I'm pleased to introduce…we're going to go to our speakers, and each will give an update. First on the block is Jeffrey Spinnanger, the Director for Critical Technology Protection for the Office of the Undersecretary of Defense for Intelligence and Security. He will give an update on behalf of DoD as the NISP Executive Agent. Jeffrey.

Jeff: Thanks very much, Mark. Good morning, everyone out there. Happy to be joining you today. Honestly wish I was…I'm not sure when it happened in my life that I've ever wished to make the trek up to Washington, DC, but I wish I was there right now for sure. The importance of this forum and frankly the opportunity for the candid discussions that happen before and during the breaks and after, I miss them tremendously. Basically, it's an opportunity for people to help me be better at my job and I look forward to getting that kind of guidance again here in the future, G-d willing.

With that, thank you again for the opportunity. We've adapted pretty well in the department, I think, and across the federal government to this operating environment that we find ourselves in. Since we are all last together there's been quite a bit that's happened, that I think is notable.

First and foremost, I'm just going to read a short excerpt from a Department of Defense policy document. If you're students of this, I know pretty much everyone on this call largely is that our acquisition partners under the direction of Ms. Lord, the Under Secretary of Defense for Acquisitions and Sustainment undertook just a Herculean effort to address the way acquisitions happen in the Department of Defense to be more agile in those endeavors. Out of that was born something called the adaptive acquisition framework. If you're not familiar with it, I highly recommend that you become familiar with it because it's frankly, the anchor point at which much of, certainly what we think about here within the industrial security program. The capstone document within all the myriad policy that relates to acquisitions, and by myriad, I mean myriad, is the guiding directive what we refer to as the 5000.01. A very brief excerpt from there within the 5000.01, it's under the subheading of develop and deliver secure

capabilities. Security, cyber security, and protection of critical technologies at all phases of acquisition are the foundation of uncompromised delivery and sustainment of war fighting capability. That's not new, some of that lexicon, some of the verbiage there is not new to this audience, this idea of uncompromised delivery has been something that's been…that grew out of what was VSS and my former boss, Mr. Stevens, we give him credit decide whether he is Ben Franklin or Thomas Jefferson in that scenario, maybe both. But the concept has grown into a thing. The importance of the partnership that we see emerging here with our…this renewed partnership that I should say, that we see with our acquisition partners here, putting that in a directive making that official Department of Defense policy really reinforces maybe what most on the call today know. That is that the protection of critical technologies, the development of those technologies, the delivery and sustainment of those technologies is a team sport. For everyone here, again, it's obvious, but I still think bears repeating, the center of how that all happens and begins is the industrial security program. It's interesting for all of the focus on the challenges that we see here in this idea of the rise of great power competition, that we need that reminder, but I think it's very important and I thought it was definitely worth calling out. A policy was issued in September of this year. If any of you who were former government officials know what it's like to issue par policy within any agency, it's a super fun time. A bit like going to the dentist without the benefit of Novocain.

All that, to say that the importance of the NISP has never been greater because when we get to this idea that security, cyber security protection, are the foundation of that. The most important component of that foundation, of course, is the industrial security program. I think that that's going to be further exemplified. It's been some time since we've had a senior acquisition official from the department brief the NISPPAC. I was thinking back, Mark, and I think, maybe I'll be wrong here, but I'm pretty sure Brett Lambert, I remember him coming once or twice back, a long, long time ago. I think just as a forecast of things to come in the rest of the briefing.

If the industrial security program is as important as we all think it is, then that brings us center stage to the NISPOM. For those of you who, as I'm sure all of you know, that we've been working the rewrite and reissuance of the NISPOM for quite some time. We are in sight of our goal. That's really the bottom line up front to get to what's called an

interim federal rule. I described earlier the joys of issuing policy within a defense agency. That is now second to the real joy, which is issuing federal policy for the federal government. I hear a little bit of chuckling. I think that might be you, Mark. We're doing this for the first time. I got nothing. It is a challenging, challenging endeavor. I think that would be the way to describe it. We went into the 60 day comment period back in the latter part of September, and we've been back and forth, receiving comments from many folks and agencies that are represented here today. We are at presently, the NISPOM is back with the Office of Management and Budget. It would be foolish of me to forecast that success is imminent, but all I can say is that all of the things that need to happen to get to success are continuing to happen. I will say that we remain cautiously optimistic. However, timelines would be if an interim federal rule is ultimately granted that will happen sometime, we believe before the end of the calendar year. If an interim federal rule does not happen, then at some point rulemaking will go into abeyance sometime in the springtime of ’21. The process, we'll reset some, and we'll move forward again from there. We've got rabbit’s feet and all kinds of trinkets and good luck charms out there to try to think that we're still on the glide path to get the interim out, and we'll see where that leaves us. That's that.

A couple other things I wanted to push out. Again, since when we were last together, I said the department wants a very public, what we call an offset campaign. The Secretary just weeks and just all kinds of things that had occurred that had frankly frustrated the Secretary and I think of many of his predecessors and he had a watershed moment and said, “Okay, enough is enough. We need to kind of get back to basics.” That's exactly what this campaign in its essence was. It was a reminder of things that, again, most folks are security professionals, which is probably the vast majority of folks on this call, there wasn't anything, any cosmic revelations there, except one, and that was at the highest level of the Department of Defense, there was a call to action to tighten our seals and get it together. Again, just in keeping with what, as I mentioned before on the acquisition side from the 5000, the department, in its issuances, if you hadn't seen it, and I hope that you did, but the department put out a very short notice, so the DoD remains committed to transparency to promote accountability and public trust, however, it is important to emphasize that unclassified information is not publicly releasable until it’s approved for at least by any appropriate authorizing official. As an exemplar of that, those of you who can have visibility on our slide can see that we went through, and we have the

clear for open publications. These are processes that existed. I'm sure there are variations on these processes across all agencies, but not hard to do, but speaking with a uniform and so that we're level set, we're accurate and what it is that we're intending to put forward and put out there, and we do so through the official processes, is something that we really wanted to be able to say as being very very important. Mostly, it was an eye for the concept of accountability here. That accountability, and I realize that the vast majority of folks on this call are not government officials, but it was a reminder to government officials that accountability begins with the person that you're looking at in the mirror. It begins within the government and then makes its way out. That is basic hygiene things, marking, obtaining release, all those internal hygiene components that the Secretary expects to see. With a nod to the folks on the CUI end of this agenda later in the day, you'll be pleased to know that the Executive Secretary of the Department of Defense will not process a package for signature by the Secretary or the Deputy Secretary that is not properly marked in accordance with the DoD issuance on Controlled Unclassified Information. That's pretty good from March until now. That took place in about the beginning of October of this year and that's been really great. Everybody know a name Michael Russo who runs the CUI program for us, and so there's a lot of learning by doing, going on.

Finally, then I really wanted to talk a little bit about where our priorities lie for this year. I know 842 will probably come up again. Greg mentioned it this morning. 842 nests with 847. We couldn't say enough about how much we appreciate the importance of the NISPPAC to get us to where we are today. The patience of industry, the persistence of industry, the facts and data that came from industry and frankly the open-mindedness of our partners, particularly in DOE and DNI, to get us to where we are today with 842, I think is really quite good. It's incumbent on us to examine what it took to get where we are and then we'll use that as a springboard, as we start to think about and move forward on 847 and the broader concept of FOCI. Which, again, I think you'll hear about among later speakers in which we cannot underscore the importance of the working group process and the transparency that the NISPPAC affords us to get to where we need to be on this. Frankly that's a nod to the last bullet on my slide there, where you have SCIFs and SAPFs. The SAP enterprise folks, the Director of DoD SAPCO, are undertaking a broad initial initiative for which a number of attendant security processes are a part. It's not for mine to speak on those elements of the broader objectives of that. Those of you who do a lot of

work with the DOD Special Programs are probably becoming aware of that. For us, I put SCIFs and SAPFs out there. That is definitely been something that has risen up in the era of COVID. It's been out there for a long time. A couple of jobs ago, I remember this being an issue, and it continues to be one today. But with an eye for how we got to where we needed to be with respect to national interest determinations, I wanted to put that out there 1) it's a priority for us to work across and 2), to say that, getting the right data, getting data in cooperation, collaboration with industry will help us to make the right decisions. Both with those for which we have to control it in the department and those for which frankly we're going to need assistance and collaboration, cooperation with, across the other CSAs. We look forward to that moving forward as the year progresses. With that Mark, I'll stop right there, and thank you very much for the time.

Mark: Anybody have any questions for Jeffrey? Thank you, Jeffrey. This is very comprehensive. I'm pleased to introduce now William Lietzau, Director of the Defense Counterintelligence and Security Agency. After Bill is done, we'll have some questions I'm sure. Bill, please.

William Lietzau: Thanks very much, Mark. I appreciate the invitation to talk. I think this is my first opportunity to address the NISPPAC, certainly as the Director of DCSA. I can't remember what the conflict was during the July meeting, but I am certainly pleased to be able to be here today and talk about some of the things going on at DCSA. I think I've got a couple slides. If you have access to them, if you just turn to the one that's at least in my deck, I got my name on one. That's probably not worth pausing on, but if you go to the next one. It's just a graphic depiction of what's happened in the last year or so. I know I've had a chance to speak to a number of the MOU groups that are part of the NISPPAC, so there could be a little bit of repetition for some of you, but for the NISPPAC in general, I think it's worth just pausing to reflect on the fact that DCSA has been undergoing a lot of change any way you look at it. We all have…everyone who's dealing with COVID right now. This will be a special year on anyone's calendar. It changes the way we do business in lots of different ways, but it got piled on top of pretty massive changes. I would say you could say changes to DCSA, but really, it's changes that created DCSA as this slide depicts in the 2 bottom corners left and right. You have the 2 October 1 transfers, one a year ago and one just a couple of weeks ago. A year ago, was the big numbers of people, dollars, where, if you were to technically look at it as a lawyer might, really what happened is Defense Security Service acquired other

components and changed its name into DCSA. In that regard, it went from an 800-man, $800 million organization into 12,000-man, $2.5 billion organization. Then there's other metrics that you can see there. 167 field offices around the country, and things like that, that were added to it a year ago and there's been a lot of transition, as you can imagine, whenever you do that. More mission sets were added just a few weeks ago. The NBIS program came over from DISA. DISS came over from DMDC. You see the polygraph school from DIA. You just talked about, well, Jeff just mentioned the SCIF accreditation. Actually, I don't know if he did mention SCIF accreditation, but he did mention SCIFs, and in fact, just days ago, the Under Secretary of Defense for Intelligence and Security, Joe Kernan, just before he left, signed out a memo shifting that mission over to us, and several other IT systems. Some people don't realize for instance, that yes, we took NBIB from OPM a year ago, but a few weeks ago, a legacy IT system that goes back to 1984 when it was first put in place. Yes, it's the one that was hacked into by the Chinese a few years back, that also came under DCSA's cognizance in the last few weeks. If you just look at the transfers themselves, all of those different organizations and offices that are depicted graphically on that slide have come together to form what's really a new agency, DCSA. Really just finishing up its first year of existence, and only the first few weeks with all of these mission sets together. Even if there wasn't COVID, we would be undergoing a lot of change. If you go to the next slide, slide 3, you see a fairly common representation we use, just a way of graphically depicting the transformation that DCSA is going through. We have it separated into phases. A transfer phase where we're bringing in the different components. A transition phase, which is the same integration that every company goes through when it has mergers or acquisitions. government agencies do the same thing. Then a larger, more profound transformation phase, which is designed to make DCSA be the implementer that everyone on this call would want it to be. If we were going to have the personnel vetting that you would want the United States government to have, if you were going to have the industrial security that we would want the US government to have, basically, that's bringing us solidly into the 21st century with the appropriate innovation and optimization of the different components to what DCSA does, so that we're putting it all together in a way that that best protects our security. I guess my main point would be, we are in a timeline where we have completed most of the transfers. There's a few more things that are happening a year from now. We're in transition, if you go one more slide, I asked them to put out there my transitional

organization chart, and then we're in the thick of transformational efforts right now as a new organization. I guess, before I get into how specifically we're transforming, I would like to just pause for a minute to reflect on the last year. A little bit of bragging on behalf of my agency and the people who work at DCSA, because I would say that it's difficult to change, everyone knows that, change management is one of the most complex leadership challenges that people have. In this case, we've got all this change happening while going through COVID. I think for those who were around my change of directorship with Charlie Phalen took place here in the conference room at DCSA in Quantico where I am now, there was maybe three or four people in the room, and we didn't even shake hands. I think we touched elbows because COVID had just started. It was already difficult on the agency. It became more difficult, but during this period, the way I often describe it, and probably some of you were on a call yesterday with our stakeholders where I did it that way, where we have a…it's like we're in charge of changing the engines in this airplane while it's flying. We've got to keep our missions going, our industrial security mission continues…our personnel vetting mission continues…we've got to continue flying the plane, but we need to change it from a turboprop into a jet while we're flying it and make sure we don't lose out altitude while it's happening. That's what this team has been doing, and that's what I mean by wanting to brag about the work they've done, because during this year of pretty substantial transition that's been going on, our background investigation team has further reduced its inventory from what you all know at one point was a 725,000 case inventory and is now hovering around a steady state, 200,000 cases. You know we were looking, I'm sure everyone on this call is familiar with the amount of time it took to complete an investigation to get a top secret clearance or a secret clearance, nowhere near our IRPTA timelines yet in the fourth quarter of FY 20, during COVID we actually, for the first time in, I think about eight years, hit the T5 80-day IRPTA goal for a top secret clearance. We're hovering around 55 days right now for a secret clearance. Our adjudication facility, the consolidated adjudication facility, which handles about 89% of all of the adjudications in the US government, had a fairly significant backlog a year ago as well. They've reduced it to a steady state, and they fallen well within all the IRTPA timelines of under 20 days, in some cases hitting 10, 11 days for a top secret clearance. Basically, while the transformation has been taking place, the guys who were actually doing the work out there, at the pointy end of the spear, have been keeping the mission going in a way that I couldn't be prouder of them. That's just the background investigation, what I mentioned,

obviously you're familiar, we are the heart of the agency, our industrial security mission that reaches out into all the others, has also been making massive improvements during the same timeframe. Our FOCI mitigation assessments are being done in about a 40% shorter timeframe than they were. Same is true with our facility security clearances. Of course, we've had challenges with COVID and everything, but at the same time, we kept up that processing and are improving, also, the level of sophistication of the vulnerabilities that we're looking at. Part of that as I think a lot of you know, as you've heard in the past, things like DSS and transition and RISO and things like that, that has not always, from my understanding, been received with enthusiasm for good reason, but they're also our attempts to change for good reason too, because we're moving from a vulnerability system that was checklist based where we're simply looking at vulnerabilities. If we call ourselves the gatekeepers, we're essentially looking at whether the walls and the gate is on a firm footing. We've moved into a 21st century where we've got a much more sophisticated threat, and we cannot just simply look at a checklist vulnerability assessment. We've got to look more specifically at the threats, because they're already inside the walls, if you will. They're behind the gate already. In that regard, we have a counter-intelligence capability that has been blossoming in recent years. I could give similar performance metrics for them if we wanted to. They're about 3.5% of DoD's counter intelligence assets, but we're producing about 40% of the IIRs, associated with emerging and disruptive technologies. They'll probably produce about 6,000 IIRs today, about 20,000 raw industry reports. That's something that wasn't even really happening a decade ago.

Then our training mission, CDSE. We also have a national training center and of course the polygraph school, we just adopted. Similar situation there, during transition, during COVID, they didn't really ratchet back the work they were doing. In fact, we've probably this year tripled the number of course completions, as you can imagine during COVID, one of the things you can do is take online courses. There was a much bigger demand signal put out to our CDSE team and they responded by stretching all of our IT systems to the limit as they move forward. Anyway, a lot of great work has been done by the agency. My goal will be to keep all of those trajectories for our mission areas while also transforming the agency into what you want it to be.

I have a new office called the Chief Strategy Office. It absorbed what was previously, some of you heard of a Personnel Vetting

Transformation Office. I was involved in that before I came in as the director here. That office has a number of objectives that we're using to move forward and basically having a greater customer focus coming up with an operating model that's more efficient, that makes sense, continuing better optimizing our leveraging of technology and innovation, and then optimizing the organizational efficiencies we ought to be able to get by coming together. That team is working through the transformation initiatives that are going to take us to where we need to be.

There's another component to it, I should just pause for a second because I know it is an area of concern across the organizations represented in this meeting, and that is some of the IT architectures. You're familiar with the Legacy IT, probably doesn't give a lot of heartburn to most of the people on this call. That's because you don't know what I know about the vulnerabilities of that IT architecture. It's probably the one that gives me the greatest heartburn. The plan originally a year ago was that OPM would continue to run the Legacy IT architecture, PIPS it's sometimes called, that's just a, one of 80 some components to it, but your taxes are paying about $150 million a year to keep that thing up and running. OPM recently told us they weren't staffed to be able to keep it running in spite of the original agreement, so DoD had to adopt it on October 1st. Ideally, we wouldn't need it anymore because I think what you're all familiar with is NBIS, we probably need a new name for that, National Background Investigation System, was supposed to be up and running to replace the Legacy IT system. It's not. It won't be able to replace that Legacy IT system in the immediate future, so right now we've got to keep both of them running.

We also just adopted the whole NBIS program management office on October 1st of this year. Some of you have heard about that program. I think in some ways, some of the advertised capabilities that it was going to provide were based on the technological development, as opposed to operationally relevant capability. In that regard, some of the promises, some of the expectations were more sanguine than they should have been. One of the first things we did, and it was taking place as I was taking over as director, was a rebaselining of the NBIS program, trying to get some realistic expectations on the street, and a more thorough coordinated integrated master schedule that would be capabilities based so that we could actually start sunsetting the Legacy IT structures while we were building NBIS, and then also building it in such a way that we could factor in the new Trusted Workforce 2.0 requirements of

continuous vetting that included some hindsight capabilities that weren't originally factored into NBIS. That's one of the big moving parts.

Then the one that I think has a lot of people understandably concerned, it was brought to my attention. I think Mark, you might've signed that letter from ISOO, I'm not even sure, but I certainly got a wake-up call soon after coming in as director when there was concern expressed from our industry partners that the DISS capabilities weren't quite up to where they should be before we're ready to sunset JPAS. We took a hard look at that, and in fact, I came to the conclusion that the concerns were well placed. We've recently just adopted the DISS program from DMDC, another DoD component, a few weeks ago, and we have done a pretty hard look at that, and come up with a gap analysis and a set up criteria that we're going to use before we sunset JPAS. Right now, I think technically it is still scheduled to sunset on December 31st of this year. I'm pretty certain that it will not be sunsetting there, and we're going to probably be extending that. In fact, I have a meeting with the new Under Secretary of Defense for Intelligence and Security tomorrow, and probably will raise that issue as something we're just going to have to change that target date so that the chalk line that we were snapping at one point was a date-based a calendar chalk line. It was originally going to be October 1st, I think, and then it moved to December. It'll now be a capabilities-based chalk line. But we are going to have to move forward fairly soon as we try to get our IT architecture up and running to support the new DCSA mission.

I know I'm getting to the end of the time, so let me ask you to just turn to that last slide, the fourth slide. This was just recently done. What this is, is the transitional organizational chart. You had org charts for many of the different components. NBIB had its own org chart within OPM. DSS had an org chart. The CAF had an org chart. We have various offices that have joined. Like every major organization, we will undoubtedly be reorganizing again in the future. What I have here though, is a transitional org chart. On day 1 a year ago, Charlie Phalen and I agreed that the thing that made the most sense was to put together an organization that caused the least disruption and change to the ongoing missions at that time. At some point, we'll have a transformational organization that integrates the missions better. This is what I'm calling the transitional organization chart. The bottom row is what's most significant. These are our mission areas. Obviously, the pointy end of the spirit is our regions and field offices. They don't dwell on those very much here. They've stayed the same. We have not merged them yet.

We have slightly different regions and office locations in the personnel vetting space that we have in the industrial security space and in counter-intelligence space. I broke out counter-intel so then you move one line up and you see what I'm calling the seven major mission areas of DCSA. These would be the assistant director level leads. I broke out counterintelligence from what was then seen as a larger critical technology protection. Next one over it's called critical technology protection. That's really where your industrial security sits. I will admit that I almost changed its name to industrial security when we came up with this transitional org chart, but I got enough internal pushback that I was like, "All right, we'll let it ride for a while." That is where a broader, what I can see of as a broader industrial security set of missions resides primarily. Background investigations you're familiar with, but for a brief period, it was a much even a bigger organization called Personnel Vetting, but we've broken it out to be product offerings. Background investigations is probably, manpower wise is the largest part of DCSA. Adjudications is about 600 people, adjudicate mostly for DoD. Most of the people on this call should be familiar with the VROC, which is also why we left that name in place. The VROC is mixing the industrial security component of personnel vetting, but it's also where we're doing the most change right now with respect to continuous evaluation, continuous vetting, and putting new products on the street that can be used by the 120 odd agencies that we support, as well as industry, as we're looking at moving into a continuous vetting framework. DITMAC, you're familiar with and training, I've already spoken of a little bit. These are our major mission areas. These are the support elements are up above. I will say that Program Executive Office, which is what houses NBIS right now, that's a little bit more than a support element, and that if you really look at the mandate for NBIS, it provides architecture that can be used by other investigative branches within the US government, not just by DCSA and the agencies that we support. It's got a little bit of an outward facing component too.

That's the big picture of where we sit today. We're in the process of continuing to transform this organization, but to try to keep the missions going as we are. I'll pause there, Mark, because I do want to leave room for any questions that someone might have.

Mark: Sure. Thank you. Please, anyone have any questions for Bill? I can't imagine that they don't. Bill, you did such a thorough job. You, I guess, answered all the questions.

Greg: Kudos to all of you, Bill, and everyone at DCSA for what you're doing.

Mark: Absolutely.

Greg: The transitional organizational chart, can't help but notice the rest of the world is overlaid there or underlaid. Forgive me if it's already in existence, there was a time when DSS, DIS had a presence in European and Asian theaters. Today of course, global is more than ever and many of the folks on this call are with companies that have global presence. The question is simply is, is there a plan in the future for DCSA to establish a presence in either Europe, Middle East or virtually anywhere in the world?

Bill: Hey, thanks, Greg. That's a great question, and that's actually one of the things we are looking at now. The presence that I think you're describing from the past, if the history that I've learned upon coming here is accurate, to some degree, that's been pulled back and it's supported from headquarters here. We do still have, now what's interesting is as we merge the mission sets, I do have a background investigation presence that's overseas, still overseas sitting there, but even that has ratcheted back a little bit during the COVID situation.

I didn't talk too much about some of the changes that COVID brought about, but other than just bragging about the fact that we kept the mission going during COVID without too much of a hiccup, but you can imagine there were a number of hiccups. We did a lot of passing out of laptops and software that needed to replace some of the in-person things that were taking place. Paper copies of things…we made more rapid this shift from paper…if you were to visit Boyers, Pennsylvania a year ago, you could have seen acres of file cabinets that looked like it was coming out of an Indiana Jones movie where the Ark of the Covenant was, and those file cabinets are now gone. They're replaced with electronic records. That's a good thing. All that's a good thing, but part of it is the work we were doing in interviewing targets and the people we interview, I've lost the name for it, but those people over in Europe, a lot more of it was done by video conference and teleconference. We're looking at how we want to go forward. I think all of us have learned things during COVID. We've learned about teleworking and where the limits are to what you can and can't accomplish. Certainly, our presence in Europe has reduced both on the industrial security side and on the personnel vetting side more recently, and as we look at the operating model going forward, we're going to look at what makes sense for the future.

Greg: Okay. Thank you. I appreciate it.

Mark: Yes. Very good. Anyone else have any questions for Bill before we go onto our next speaker?

Dan: Yes, I do. This is Dan McGarvey from NISPPAC Industry. This is without a doubt, very impressive and obviously very challenging. I would say that you're not just rebuilding an airplane. You're almost rebuilding a city. One thought I had, as you go through your transformation process…it's been noticed that it talks about an operating model implementation roadmap. It would be terrific if, at some point in time, you could share that, at least with NISPPAC Industry, as you move along, so that we know where DCSA is going, and also where we could help in terms of supporting your different initiatives that take place. Because you've got on your transition piece, transition for two and a half years, transformation for two and a half years, and even though it doesn't give us specific data, it looks like somewhere along the lines of maybe 2025 or something like that. Understanding where you're going would really help us. Once again, it's been a terrific presentation. Thank you.

Bill: Thank you, Daniel. I appreciate the comment. I also appreciate the request. I want to pull back the 2025 to maybe 2024 and treat that first year as if it's already gone by just because I keep…it's funny, as you said, it would be good to see the implementation roadmaps. I'm sitting here in my office saying, "Yeah, I want to see that out of my CSO office this afternoon too." Because they wanted to delay the meeting yet again and I said, "No, we're going to do it today." Obviously it's not ready for prime time yet. It's a work in progress. It'll be iterative. It has been, but that's a great point. We are getting close to having a more articulated plan in place that we could share. I will keep that in mind, and we'll find a way to…in the public facing charts, like maybe this transitional org chart, we could also put a high-level implementation plan in place. Because that is the next step. It is the one that right now, if you were to say, "Hey, could I look at that plan?" I've got several of them on my desk and none of them are quite right yet, but thank you. We will get there.

Kim: Hi, this is Kim Baugher from State Department. I just want to thank you for saying that you had thought about calling the program, keeping it Industrial Security, because from someone who's been at it for many years, I was a little disheartened when I saw the boxes yesterday and didn't see the words, Industrial Security, because it's a program close to my heart so I'm glad that you struggled with that, and I know it encompasses a lot more than just industrial security, but I was just kind of glad to hear you say that. Thank you.

Bill: Thank you. You've just encouraged me too, because depending how you define industrial security, I personally think it could, that's broad enough that it could capture everything we do in critical technology protection, but there are people here who have different opinions on it.

Kim: I would be on your side on that. Okay. Because I'm an old person that doesn't like change. But thank you though.

Bill: Well, good. What we're obviously trying to do is because this is such a big transformation as was just described, goes out a number of years. This isn't one of those changes where you can rip a Band-Aid off and just do it all at once. We've got to phase it, and so really it was a question of, alright, we're going to do so many changes on this phase but when we start implementing the op model, that's when we probably will nail down what our various organizational components are called.

Kim: Thank you.

Mark: Anyone else have any questions for Bill? Bill, that was an excellent presentation and it's good to know that you're there during these tumultuous times. You're making some real progress and we couldn't be happier, the way that you're running things. Keep it up. Okay. Alright, the next speaker will be Stacy Bostjanick, Director of Cybersecurity Maturity Model Certification Policy. Stacy.

Stacy Bostjanick: Hi, good morning. I'm here to talk about the Cybersecurity Maturity Model. I think everybody is fairly aware of why we're doing the Cybersecurity Maturity Model Certification. I was going to give you an update as to where we stand. Currently we have moved into from proposal making into an interim rule, which will become effective 30 November. We are in the public comment period. I think we've had 36,000 views. I think right now we're up to about 35 or 40 comments. Come November 30th, the interim rule will be in effect, which means we will be in a position to include CMMC as a condition of award. If you look at the slide we're on now, we're talking about the interim rule. As of November 30th, we can include the CMMC in to let acquisition programs as a condition of award. The one thing that we wanted to talk about was, there are several different parts to the interim rule that we're working with. As you all are aware that we have been here to date then doing the DoD assessments, which is the DCMA group of assessors that go out and work with companies to either provide them a basic, medium or a high assessment.

The basic assessment is in line with what the original 252.204-7012 clause said, which is you need to self-attest to the fact that you have a system security plan and a POA&M to be in compliance with 110 controls required by the NIST 800-171.

The medium assessment is where you get on the phone and you talk through your system security plan and your POA&M with the DCMA rep, so they have confidence and comfort with where you are with your plan.

Then a high assessment is where they come out and either come to your facility and do an over the shoulder view of what your system looks like and be in a position to validate that the system securities that are in place that you say they are. They will give you a score with regard to that.

One of the parts of this interim rule with regard to the DoD assessment requires that by November 30th, all DoD contractors submit their basic assessment in the SPRS database. There's been a lot of confusion with regard to that. A lot of people are associating that with the CMMC rule. I've been fielding a lot of questions on the SPRS database. There's a requirement to go into that database, fill out the basic information of your system security plan in your POA&M to get there, and then you have to self score yourself, evaluate yourself, as to what score you think you would achieve on the NIST 800-171 in the current DoD assessment methodology and have that in the SPRS database before December 1st. A lot of the primes are letting the subs know that they cannot have their options exercised on existing contracts unless that information is in the database. If you have anybody questioning, we have information sheets that are going to be on the DPC toolbox website that will give explicit instructions on how to do that. On the CMMC rule, we are going to have a rollout of about 10 to 15 acquisitions in the first year. We're currently working hand in hand with the services and the service acquisition executives to identify three to four programs within each service and three or four out of the fourth estate to begin implementation of CMMC. Now what will happen is as we identify those programs, in fact, Ms. Lord is getting ready to issue a press release with the first three or four programs listed so people can prepare and get ready. An RFI will come out. We have model language that we've prepared and gone through in some of our tabletop exercises in our pathfinders that we've done, that will be sent out to the acquisition professionals for them to be able to put the proper language in their RFIs and RFQs for inclusion in those contracts. The contractor will be notified. They will be able to

issue, submit a proposal. The proposal will be evaluated, and if they are the apparent offer award they will have to have the requisite CMMC certification prior to contract award.

If you look at the second slide, this shows you the phasing of how the DoD assessments are going to be phased over to the CMMC assessment essentially. You can see it's a very slow progression and that the number of contractors that we really anticipate at the CMMC level 3 is not that high. Can you go to the next slide?

I've already spoken to this. This is talking about the SPRS information that needs to go in that database and that every contractor needs to have that listed before December 1 to continue performance on their existing contracts and new contracts as well. Can we go to the next slide?

This is more explanation of that. I think the scoring methodology is one thing that has got some people confused. This information is very important for different companies to have to make sure that they meet the need for that. We'll go to the next slide.

Again, these are all pilot programs where we've asked each service to provide us 3 to 4 programs. There we'll be managing the CMMC level 3, which is just basic CUI. In the first-year rollout we will not address the higher critical technologies until 2022/23 timeframe. Currently we've got provisional assessors being trained by the CMMC-AB. I think we have about 75 to 100 assessors ready to start working. We're working on the C3PAOs. Those provisional assessors have yet to go through their background investigations. We're going to have for CMMC level 1 procurement assessments, they will have to have a tier 1 suitability determination. For anything above that they will have to have a tier 3 suitability determination. The process, and I'm hoping the gentleman from DCSA is still on the line, because what we've agreed upon is that the CMMC-AB will have an FSO that will work directly with DCSA to process and manage those suitability determinations for those individuals performing the assessment. Those assessors will work with C3PAOs, which are the CMMC third party assessment organizations. Those C3PAOs will have to have their systems evaluated at CMMC level 3, because it is our contention that the system security plan information, the assessment information, that they will gather when they go out to these companies to do these assessments, would be needed to be safeguarded at a CMMC level 3 and be considered to be Controlled Unclassified Information. Can you go to the next slide? I

guess one thing I want to make sure I've mentioned that COTS products are excluded from CMMC. They do not require CMMC certification.

The slide you see here is our rollout plan. We plan to have 15 acquisitions in FY '21, 75 in '22, 250 in '23, 479 in the last two years and then after FY '26, all contracts will require CMMC other than the COTS products that I mentioned previously. Okay. Can you go to the next slide?

You can see here on this slide, what we talk about is the percentage of companies that we anticipate being level 1 through 5. It is our contention that about 60% of the DIB will only ever require CMMC level 1, which is their receipt of the federal contract information. One of the things that we're working on with Mr. Spinnanger's office is to come up with a guide for the acquisition community because probably the toughest nut to crack is that when you have CUI at the CMMC level 3, 4, and 5, how…when you disaggregate that data and you start mapping it through the supply chain, where does it lose the requirement to be CMMC level three? Where is it no longer CUI? I guess one of the best examples that I can give to luminate what I'm talking about is Ms. Arrington went out to TRANSCOM and had to meet with a welder. He was quite frustrated because he didn't realize why he needed to have cyber security. He said, "I'm just a plain welder." When she went to visit him, she said, "Well, how do you know what to weld?" He said, "Oh, they send it to me." She said he had his Apple Mac laptop up on the counter and she could see his Facebook messenger blinking and his Amazon delivery popped up while she was standing there.

She said it was on AutoCAD program. She said, "Can you zoom out on that so can see what the whole thing is?" He had the entire structural design of one of our tactical aircraft. She said, "Well, don't you think our adversaries will want to get ahold of that or get in and change the tolerances or the specifications of your weld, so now your quality goes down and you no longer can garner work, and it erodes our industrial base? Or how about if he just wants to steal your CAGE code information so he can redirect your payment to his account and steal your money." One of the poignant parts about that is why did that welder have the entire tactical design? If the prime had only taken the time to cut out each weld and send him the necessary information that he only needed to do his job, could he not have been in receipt of CUI and had been… that that would not necessarily have been CUI those welds in the spot weld? That's one thing we've got to work with our program managers and our primes to identify at what point does that

CUI, when it's dis-aggregated from other things, no longer hold the trappings of CUI, and can only be CMMC level 1. It doesn't make good business sense. We probably can ill afford to have every number of procurements at CUI CMMC level 3, be CMMC level 3. If I'm just producing a bolt, then I only need to be CMMC level 1 and we don't need to have that contractor go through the expense of being CMMC level 3 certified. Okay. Can you go to the next slide?

This again is just a breakdown of the CMMC rollout and where we expect it to be. Can you go to the next slide?

This is a breakdown by entity side. I know we've gotten a lot of consternation from the small businesses as to “what does this mean to me”, and they feel like they have a lot of a heavy lift and expense to become CMMC certified. But if you look at this, I'm not sure that many of the small businesses will ever have to be anything higher than a CMMC level 1 and the cost for that is actually fairly minimal. We also have a lot of programs right now with Project Spectrum and the NIST MIP organization and the PTAC that will be trained on CMMC so they can provide assistance to these small businesses as well to help guide them through the process, figure out where they need to be and what CMMC level they feel they need to have. There's also language in the NDAA that talks about a grants program with funding to assist some of these small businesses, but as you all know, we haven't gotten that approved yet, so we can't hold our breath on that one quite yet. Can you go to the next slide please?

Producer: That looks to be the last slide.

Stacy: Okay. Barring that I will wait for any questions. I'm hoping I'm like the rest of the people. Nobody has any, right?

Greg: I'll break the ice again. It's Greg Pannoni. Again, thank you very much, Stacy, great briefing. I don't want to overplay this, but looking at that last slide that we see on the rollout by entity size, could you amplify a little bit on what the criteria is for what is a small entity versus another than small? Or if that's too much for right now? I guess, because I'm a little confused in terms of whether you're small or not small, you still could be working on a very significant piece of technology, and I don't know, I find it very interesting that none of them, as you pointed out whatever, go above a level 3.

Stacy: I think that I mischaracterized that is if that's the way you saw it, no.

Greg: I'm sorry, very few would go above a level 3. I see there are some in out here.

Stacy: Right. In our roll out plan in the first year, we are only going to concentrate on things that are level 3, because our training and our information for the level 4 and 5 for CMMC was those highly critical technology is not mature enough yet. We're only going to roll out at level three 3 for FY21. That was our decision right now. What we have to look at is when you start talking about those things that rise to the level of the CMMC 4 and 5, and they're associated with the level of criticality of that technology, through our research and information, what we've determined is not that many companies are actually going to be participating at that high level. Remember that doesn't mean that they can't participate on the program, but we don't anticipate that their participation would require them to have a certification at that higher level. Mainly the big primes are doing the work at the really critical highly technical area. That's not to say that you won't have 1 or 2, right? Those types of things are going to be levels 4 and 5 are going to be extremely expensive and we're anticipating that the costs up to level 3 will be incorporated in the overhead and GNA rates and the indirect rates of the company. When you get to levels 4 and 5, those would most probably be a direct charge to the program just because it is such an expensive expense for the company that they will probably have a very difficult time affording it. The program will probably bear the brunt of the uplift. They'll have to pay on their own to CMMC level 3, but 4 and 5 will be a direct charge to the program.

Greg: Thanks for amplifying on those points. I appreciate and caught that. That's where I was going to, thinking about the expense involved in level 4 and 5 for those small companies.

Stacy: The one thing I did find interesting was there was a group of, and I'm going to probably be a little politically incorrect, but I'm going to call them cyber geeks on LinkedIn. They were lobbying for the CMMC team to move some of the requirements from CMMC level 4 down the CMMC level 3, and we were all snickering because we never expected anybody to say, "Hey, you need to make level 3 harder." I'm quite sure that once we get through the public comment phase, we're going to reassess CMMC level 3 and it is quite possible that those additional 20 controls over and above the NIST 110 are going to get looked at pretty closely.

Greg: Okay. Again, thank you. I appreciate it.

Stacy: You're quite welcome.

Kim: This is Kim Baugher from the State Department. At the risk of, in front of the people, showing my ignorance, I'm just confused by this whole thing, which is on me, but okay. This all talks about DFARS clause, which is DoD, and it keeps talking about DoD. I mean, I'm not DoD. I'm State Department, a non-DoD agency. How does this get implemented and do the contractors that have State Department contracts don't fall under DFARS.

Stacy: It makes total sense that you would ask this question. To begin with, this is going to be a purely Department of Defense requirement, and that's why it's being implemented in the DFARS upfront. What I will tell you though, is we have a lot of interest across all of federal government. Are you familiar with the Federal Acquisition Security Council? Have you heard of that?

Kim: Yes. I think that we've been involved with them with some other clauses.

Stacy: Sure. Yes. State Department definitely has a play in the Federal Acquisition Security Council. That is a council set up to help improve our cybersecurity and our acquisition and supply chain risk management across the entire federal government. CMMC came into play because we instituted the 252.204-7012 clause, which is DoD only, that said, if you're going to handle Controlled Unclassified Information, you have to meet this NIST 800-171, 110 controls in your network to be compliant to handle it, which says you have enough protections in your network to keep people from stealing this information that we hold as important. That came into play at the end of December of 2017. There an IG review, and then a Navy cyber readiness review that went out and said, "Hey, let's see how contractors are doing with their self-attestation and the implementation of this clause that they were supposed to do. They basically found out they weren't doing it. They were self attesting that they were, and they weren't because they just didn't understand or they wanted the business and they figured it's a self-attestation, nobody's ever going to come look, so we'll just say we are when we aren't. As a result of that, a couple of key companies were held to task under the False Claims Act because they attested that they were compliant when they knowingly knew they weren't. I think it was Rocketjet Aerodyne got hammered for that for about $14 million, and I think Cisco got in trouble for it, for knowingly having a vulnerability in one of its products that they never bothered to fix. As a result of that, our Secretary of Defense

said, “Hey, we need to figure out a plan to be able to get out and start checking that these companies are actually doing what they're saying they're doing.” The DCMA assessment group, they call themselves the DIBCAC, they began going, and they began with all the major primes, going and doing these assessments on the basic NIST 800-171, but we quickly realized that they didn't have the bandwidth or the infrastructure to do all 300,000 companies in the DIB. We got together with Johns Hopkins APL and Carnegie Mellon SDI, and we formulated the CMMC model, which is the 5 levels of CMMC from 1 to 5, 1 being just federal contract information, which is a requirement in the FAR 52.204-21 that everybody across the federal government is supposed to be in compliance with, up to CMMC level 5, which is requirements for highly technical, critical technology, and those requirements include things like a 24-hour stock. It spans the spectrum of what kind of CUI and how sensitive it is and needs to be protected. For State Department right now, it's not as big of a deal for you to pay attention to. But what I will tell you is, that there is a lot of chatter across the entire federal government…DHS is closely watching what we're doing…Treasury, we've been in touch with, they're very interested in adopting CMMC…and then the Federal Acquisition Security Council is also watching because a lot of people are looking at CMMC as maybe the foundational piece to help our nation's industry become secure against a lot of these cyber attacks. I think around the world there’s like $600 billion a year in intellectual property is stolen and within just the United States is $175 billion of intellectual property is taken by our adversaries. I know you're probably aware that the F-35 has had horrible problems because we now have an airplane that looks just like it in China, down to the fact that they have the same problems with their canopy on their cockpit that we do. They even copied in the same flaws that we have. CMMC is a stepping stone to buying down the risk and stopping our adversaries from running away with all our data. You are correct at the onset. When we roll this out in the next several years, it's not going to apply to State Department contractors. If some of your contractors have worked for both DoD and the State Department, then they will be required to become CMMC certified. That was a long-winded answer to your question. I hope I answered it correctly for you.

Kim: Yes. My technical mind’s a little tired today, but yes, I mean, that's helpful because sometimes, especially in the National Industrial Security Program, we're a non-DoD agency, but we're part of the NISP, and our contractors, if we have a contractor that only has State Department contracts, then that wouldn't apply to them. But if they had State

Department and DoD contracts, that would apply on their DoD contracts only then. But there is a FAR clause that you gave us that if it's the FAR, then if State Department ever did it, it would have to be in the State Department, which is the DOSAR, as opposed to DFAR.

Stacy: There is a potential and I think with the Federal Acquisition Security Council, that it will eventually become a FAR clause. I think everybody's watching to see how we do, if we fall flat on our face or we do a fairly good job of getting this implemented, then it will probably proliferate. I will also tell you we've had a lot of international interest. We've got countries coming out of the woodwork that want to implement it in their country as well.

Kim: Okay. Thanks a lot.

Stacy: You're welcome.

Mark: Okay. Thank you very much for that exhaustive presentation. I think it answered a lot of questions. Again, thank you very much.

Stacy: You're quite welcome. Anytime.

Mark: At this time we're going to take a very brief five minute break and then we will resume with our next speaker, which will be from the ODNI. Be back… it is 10:29 so, what's that, 10:34? Okay, then we'll resume. Thank you.

Welcome back after that five minute break. Quick admin note is apparently some of our slides and biographies aren't uploaded yet, so, but they will be on our website within the 90 days. If you have any questions, please just reach out to us. With that, I'm going to turn to our next speaker from the ODNI. Kyla, you are ready?

Kyla: I'm here. Thank you.

Mark: You're welcome.

Kyla: Thanks Mark. My name is Kyla Power. I'm filling in for Valerie Kerben today. I heard a couple of mentions regarding the National Center for Credibility Assessment, so I'll go ahead and start with SEAD 2. Just a quick update on Security Executive Agent Directive 2, Use of Polygraph in Support of Personnel Security Determinations for Initial or Continued Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position. This SEAD was previously issued in 2014 and was recently revised in light of the transfer of the National Center for

Credibility Assessment, NCCA, from the Defense Intelligence Agency to the Defense Counterintelligence and Security Agency. We just updated the authority section to reflect this transfer. SEAD 2 was distributed to departments and agencies via the security executive agent mailbox. ISOO also distributed to NISPPAC members and in October, so just recently, we published this SEAD to the NCSC website, so you can find it there.

Just transitioning to Trusted Workforce 2.0, I know that was mentioned earlier as well. The executive steering group continues to meet virtually monthly and is committed to continuing to overhaul the security clearance process. The executive agent's staff, along with the PAC PMO staff, continued to meet regularly to work on policy constructs for the next set of documents in the policy framework for Trusted Workforce 2.0. Along those lines, the Federal Personnel Core Vetting Doctrine went through interagency formal review with OMB, and in conjunction with PAC PMO, we've provided a review with NISPPAC members to socialize the draft policy. Right now, we're waiting for final signature by both executive agents. Once that's done, it'll be published to the federal register.

Also just wanted to remind everyone that in February, ODNI and OPM jointly signed executive correspondence, titled Transforming Federal Personnel Vetting: Measures to Expedite Reform and Further Reduce the Federal Government's Background Investigation Inventory. This EC introduced important Trusted Workforce 2.0 reform concepts and measures to drive early adoption, including compliance with periodic reinvestigation requirements through continuous vetting for individuals in national security positions enrolled in a CE program that meets minimum standards. Fact sheets describing and summarizing this EC were distributed to departments and agencies, as well as the public. We also provided a congressional notification access to oversight committees along with the EC.

We're also working on an additional executive correspondence regarding Trusted Workforce and the transitional stages of Trusted Workforce 1.25 and 1.5, as well as the future state of Trusted Workforce 2.0. This EC will provide policy and implementation guidance for moving towards continuous vetting to include how agencies will do automated records checks, and agency specific checks.

Transitioning a little bit from personnel security and Trusted Workforce 2.0, I just want to make a mention about a couple of things regarding

national interest determinations. As Greg mentioned earlier, Section 842 of Fiscal Year '19, NDAA, just some additional requirements came into play out as of October 1st. In light of Section 842, ODNI will no longer process national interest determination concurrence requests or covered National Technology and Industrial Base, or NTIB entities, operating under a special security agreement as a condition for access to SCI. That's happened, but I do want to just reiterate that ODNI is still continuing to process NID concurrence requests for those companies that are not affected by Section 842.

That's pretty much all of our updates. We're still not operating at full capacity due to COVID-19, but we promise to continue the dialogue and provide updates on the industry forums like this one, as well as host meetings to share information with our partners as we move forward with things like Trusted Workforce 2.0. With that, I'll take any questions.

Mark: Any questions for Kyla? Okay. Thank you very much. I appreciate it. Good presentation. Next, we have Heather Sims, the NISPPAC industry spokesperson will provide the industry updates. Heather. There's an audio trouble here.

Greg: Mark, do you want me to go in the meantime?

Mark: Yeah, Greg.

Greg: Okay. I'll try to be brief to keep us on track and hopefully Heather will get back on.

Mark: Okay. Got it.

Greg: I'm going to do the part with the NISPPAC working groups and some of the discussions that took place there. You've heard from the DoD and ODNI on some of the high-level points that we discussed at the Clearance Working Group. I'm just going to say CWG from here on out. We had that meeting on October 28th and we'll also get some metric data on clearances and information systems in a few minutes here.

We also discussed at the CWG an issue about the Small Business Administration joint business venture final rule. This was a surprise to us at ISOO and NARA. I'm not really sure why NARA did not see that rule before it was promulgated, but in any event, the rule appears to eliminate the requirement for an entity eligibility determination, what we've always called a facility security clearance, for a joint venture, if the entities to the joint venture already have entity eligibility

determinations. However, this contravenes the requirement in the NISP rule, the 32 CFR Part 2004. Therefore, we and ISOO, will put out a notice, we expect to have a forthcoming notice that emphasizes the continuance of the entity eligibility requirement for all legal entities to include joint ventures that enter into classified contracts with an agency of the federal government.

Another item we discussed at the CWG was NISP entity cost collection methodology. This is a requirement for both the government agencies and NISP contractors, specified in both the NISP and the classified national security information executive orders and their companion directives. We are holding a government only meeting on December 2nd to further discuss the cost methodology. Totally transparent. We've had two prior meetings.

The goal here is to have consensus within the government on this topic of cost expenditures, this, by the way, as part of a larger effort within ISOO, in terms of data collection, to take advantage of technology and facilitate how we go about collecting various metric data that reveals how the CNSI, the classified programs, and the NISP program and the CUI programs are doing as we report those to the President annually. After, we the government, we want to achieve consensus on the cost expenditures that industry spends to implement the requirements of the NISP. ISOO will then host a meeting of government and industry to garner industry's input on this matter. Then finally, the NISPPAC will be provided a recommendation on the way forward for collecting these data cost elements for industry's NISP implementation.

Turning to metrics, we'll hear from DCSA on their security clearance and information systems metrics, along with NRC and DOE, on their security clearance metrics. Last…the NISA, the National Information Systems Authorization working group, had a discussion with a National Security Agency representative regarding sanitizing solid state drives known as SSDs. This issue was initially surfaced by the NISA working group industry members in a white paper to ISOO on the use of cryptographic erase as a potential acceptable remediation method for SSDs involved in classified spillages. The NISA working group plans to continue the discussions with the CSAs on this topic. As I said, we're going to hear now from DCSA for their NISA update, but first we'll have, excuse me, NRC provide their clearance metrics, followed by DOE, and then DCSA. I'll hold off on questions at this point. NRC, are you on the line?

Chris: I am. Can you hear me?

Greg: Sure.

Chris: Yes. Okay. I will not go through the entire slide deck. I'll just focus on that first overall 90% of the reported clearance decisions slide so I don't take up too much time. In general, in terms of initiation, we're doing quite well over the last fiscal year. In adjudications, we've had a few slip ups. You can see that we've exceeded 20 days a couple of times over the fiscal year, primarily in quarter four. I don't have a specific reason for that. I think it's a couple of things, staff taking leave, cases just slipping through the cracks. But overall, we're meeting or exceeding our adjudication timeliness, and despite all of the hurdles we've had to overcome over this past year of transitioning to basically a hundred percent from home I think we've done quite well. Again, quarter four of the fiscal year, we've experienced some blips, but I think having moved into fiscal year '21, we'll get back on track where we're hitting or exceeding our adjudication timeliness. That's essentially it for the NRC. Again, since we've done well over the last fiscal year, I don't have really much information to provide or reasons why we aren't meeting those goals.

Greg: Okay. Thanks. Let's move to DOE. We'll do the questions as I said at the end.

Tracy Kindle: Good morning and thanks, Greg. If the slides are up, if we can just move to slide 2. I'll go through the slides and give everyone an update. As far as our initial T3 and T5, our adjudication timeliness went up by two days, but we're still exceeding the timeliness goals. As far as top secret adjudications, we also increased those by two days and again, we're meeting the timeliness goals.

As far as the secret investigations, we saw a 2 day decrease in adjudication timeliness for the quarter and in T5 reinvestigation, we have some substantial improvements in the adjudications, and we dropped from 40 to 14 days. Last, the initiation timeliness with T3 Rs decreased by six days and we're also meeting that timeliness goal. If we can go ahead and move to slide 3.

Over the last year we've exceeded the initiation goal and the adjudication goals, and we expect those trends to continue. Slide 4. On average, we've met our adjudication goals as it relates to the initial T3 at 15 days over the last year, but we did have some bumps in the road as it related to adjudication for the month of June and July. We've been

on a downward and steady trajectory since August for initiation timeliness and expect that downward trajectory to continue. Slide 5.

As far as the T5 re-investigations, we are meeting the initiation goals, but again, as you saw in the 2nd and this slide, we did have some challenges over the last year for adjudications, but since May, we've been meeting both the initial adjudication timeliness goals, and we expect that trend to continue as well. Slide 6, please.

As far as the T3 where investigations on average, adjudication has decreased from 18 to 13 days and overall, we're right below the initiation timeliness goals at 13.5 days. This concludes our briefing for DOE and standing by to answer any questions.

Greg: Okay. Thank you, Tracy. We'll do the questions, like I said, at the end. Let's move to the DCSA clearance metrics. I believe Donna McLeod. You're going to be doing that.

Donna: Yes.

Greg: Thank you, Donna.

Donna: Good morning, Donna McLeod from DCSA. Actually, I'm just going to touch on additional metrics that the Director actually shared on his comments this morning. I'm going to present information on behalf of the background investigations, adjudication, and the Vetting Risk Operation Center, VROC. For the background investigation, as the Director shared, our timeliness inventory remained stable for Q1. Our numbers for the T5 initials, again, the director shared this, timeliness numbers are 81 days for T5 initials. If we would remove those cases that were impacted by COVID-19, that number would drop to 77. Cases impacted by COVID what that is is in our inventory, we have some work that we can't complete because the sources or the information we need to get to, we can't get to it because the places may be closed down or inability to contact subjects and sources. What we have done is we are holding those cases in our inventory, so in doing that, when the case is closed, that's going to impact the timeliness of our cases. That's primarily on our T5 population. Approximately 10% of our T5 cases completing Q1 were delayed due to COVID. The T3 cases are not impacted as much. Our T3 initial timeliness is at 55 days and the goal is to be at 40. Again, we're still working through the inventory, but we are impacted by some delays due to COVID. As the Director shared earlier, our inventory right now is around 200,000, of this number, roughly 32,000 are industry investigations.

Moving on to adjudication. The inventory for adjudication, the DoDCAF continues to apply portfolio management techniques to deliver national security suitability and credentialing adjudications. The two portfolios are divided into the readiness portfolio and the risk management portfolio. The readiness portfolio represents those adjudication actions designed to get people to work while the risk management portfolio, manage risks within the Trusted Workforce.

Currently, the total industry inventory is at 27,000, 72% of which is within the readiness portfolio and the remaining 28% is in the risk management portfolio. For adjudication timeliness, FY20 Q4, the DoDCAF adjudicated tiered investigations for industry at an average of 14 days for initials and 34 days for the periodic reinvestigation. The DoDCAF is operating a full mission capability with modified operations to our customer service center due to COVID. We expect to continue to be fully mission capable throughout COVID-19 and to continue meeting adjudicative timeliness requirements for our investigations and products and services for the year.

On to VROC. The VROC is staying laser focused with all the VROC industry functions to include investigation submissions, interim PRs, CE deferments, processing incidents report, and customer service and balancing all of the timeliness to support the mission readiness and identifying and mitigating insider threat concerns. For the investigation submission and interim determination, the total industry for FY20 investigation requests permission is 190,000. 90% of all initial investigations had an interim determination made on an average within 5 to 7 days. But we did have some system challenges in October, which have since been resolved, but they did result in a longer than usual lead time for interim determination. We're now averaging 25 days for interim, but we anticipate to be back at our steady state within a few weeks. We appreciate your patience during this time.

On to our PR deferments. For industry, PRs deferred to CE today over a 100,000 have been deferred. VROC will send the FSO a JPAS message when subject investigation has been stopped in JPAS, and the subject is enrolled in CE. FSO can share the fact that the PR has been deferred into CE with the subject. All industry deferred PRs are enrolled in a fully compliant CE program. For CE, about 2.3 million DoD subjects are enrolled in continuous evaluation data sources via DoD system, meeting partial CE data category requirements. Approximately 455,000 of which are industry subjects, which represents approximately 21% of the population. All industry deferred PRs are enrolled in all seven data

categories in compliance with the SEAD 6 for further support reciprocity. You will see enrollment increased significantly in this FY as we work to achieve a goal of all clear population into a Trusted Workforce compliance. What we need from you is to be responsive if you have any overdue PRs, or if we request an out of cycle SF-86 to be submitted. Enrollment requires a minimum of the 2010 version of the SF-86, which we do have most of them, but since the 2010 was not deployed until the 2012 timeframe, we may have to come back and ask for updated new SF-86. Industry and government customers can confirm CE enrollment in their history in DISS. Government customers can email VROC with CE enrollment verification. CE industry FAQs are posted on the DCSA website under "I am a FSO FAQs". The CE questions are numbers 35 through 46. As a reminder, please remember to get provision in DISS. JPAS will be decommissioned and it's imperative that everyone is provisioned. That concludes my metrics update for DCSA.

Greg: Okay. Thank you very much, Donna. We'll roll right through to the NISPPAC NISA, National Information Systems Authorization Working Group and then we'll do the questions. Selena Hutchison, are you on the line please?

Selena: Yes, I am.

Greg: Okay. Please, go ahead. Thank you.

Selena: Good morning, everyone. I want to start by congratulating cleared industry for the hard work that we put in on eMASS. I want to share a fun fact of the NISP version of eMASS is the second largest instance in DOD. The largest instance is the Navy, it's been in effect for over eight years and they have over 7,000 users. Our one-year anniversary for the NISP eMASS was in May of this year. We have the second largest instance due to the number of containers. We have 6,300 systems included approximately 3,400 users and 2100 containers, and the container is based on cage codes and systems put there. This would not be possible without the hard work that's been provided by cleared industry over the last year to make this possible. I want to thank you for that. Clearly, most of you are not winging it. But for those of you who are, we ask that you really pay attention to the eMASS rules and help us keep this system where it should be. I just want to begin with that.

Most of you know, that Karl Hellmann left the agency in September. I've been acting for Karl since that time. The Southern region AO Ron Donnelly retired in March and David Scott has been acting there.

Tyquisha Summerville is acting in capital right now. We have approximately 82 ISSPs on board. We are averaging about 1 ISSP to 75 systems. What you find is that the ISSPs are also working AIs and ECPs and ESPAs and CM and outreach. Our average days authorization is about 60, so we're still within that timeframe. If you would go to slide two, please.

The DAAPM released in September covered two specific things, primarily type authorizations. There were some inconsistencies in how it was being applied, so we want to clear that up. The Federal IS that was also clarified in that version has been a major issue for us. We continue to see a misinterpretation of what a Federal IS is. This is, a Federal IS will lead to government to government conversation, and any exception to that policy will be granted by USDI. Keep in mind too, that a Federal IS exception to policy would be only a temporary measure to get you to compliance. I wanted to stress that.

Slide 3. eMASS we just talked about briefly. Clearly, most of you are doing very good work here. We have a small staff, so in those instances where eMASS is not being used in the proper workflow, it creates problems for everyone. Some of the common issues we see is incorrect registration, improper routing to the wrong field office, system descriptions are improperly recorded, using the incorrect overlays, missing artifacts. All of these things just add to a situation that we don't need, so a little bit more care and rigor would be very helpful here. We ask that you visit the eMASS site and use those documents that we put up there for your own internal training that will help the consistency across the regions, and also help us do a better job during our reviews.

On slide 4. Nothing much has changed for us during COVID except for the delay in getting to on-site activity, and keep in mind that when we do go back to work full time, we will have to adhere to state and local policies as well. We are working to continue to extend these systems, working to get the ISSPs to triage and give you guys an answer without waiting until the last day to turn these plans back. All these things are being worked. You see some numbers here from each of the regions.

In summary, I just want to say, we want to continue to work with you identifying gaps, correcting those gaps, and consistency in policy. We are going to be focused on improving quality as the year goes forward and having all the leaders in the region work toward these inconsistency issues that we're seeing. We're trying to reduce the impact of how work comes in ISSPs, which is why we consistently ask that you submit a

complete system security plan, because we're not resourced to review 10 controls and send it back to you, and then have you send it back to us. Those type of processes just eat the clock up. That's all I have. Hope I didn't rush through that too fast.

Greg: Thank you, Selena. Are there any questions about any of the working groups or their updates? Hearing none, I think we have another slight change. Heather has been emailing me, Heather Harris, from our ISOO, indicating that Perry Russell-Hunter would like to go next. I defer to you, Mark.

Mark: Yes. Let's get Perry on. Yeah. Sure.

Greg: Let's promise Industry. Next time you will be the first on the agenda.

Mark: Yep.

Perry Russell-Hunter: I can return the favor by being very brief. My DOHA update is that we are finding ways to be productive in the age of COVID and I have to give a very public shout out and thanks to the leadership and the personnel at the DoDCAF because thanks to Marianna's leadership at the CAF and the professionalism of all the adjudicators there, we've been able to stay current in the legal reviews of the statements of reasons in industry cases. That turns out to be really important because when the statement of reasons is issued, it is the notice to the individual, the contractor employer, employee rather, of what the government's concerns are, and so we don't want that to be a mystery. We didn't want there to be any delays there. Just to give you an example, in fiscal year 2019, DOHA conducted over 2,500 legal reviews of statements of reasons for the DoDCAF, that was 2,571 to be exact. But in the current fiscal year, the fiscal year just ended, fiscal year 2020, DOHA was able to conduct 3,248 legal reviews, and we and the CAF are completely current in terms of issuing statements of reasons. That's really important for getting the word out for the employees as to what's going to happen next in administrative due process.

The other thing that's going to happen next year and we've been working diligently toward this, obviously COVID has been a factor in this, is that at some point next year, DOHA will start issuing the industry statements of reasons directly to industry contractor employees. Those of you who remember back before 2012, remember that DOHA used to do that in the past. We will be returning to that mission with an agreed transition taking place between DOHA and the DoDCAF, and we are working out the details and the implementation on that right now. The

agreed implementation of the process obviously was delayed by the pandemic.

The good news though, is that the pandemic did not stop us from returning to holding in-person hearings which we did in June of this year, in addition to some rigorous health and safety protocols, which quite frankly, we took from the federal district courts that were in the highest COVID areas, so we require masks, we have gloves available, we have plexiglass, and we also have a new amplification system in the hearing rooms. Of course, the reason for that is because we've discovered that it is important to keep people masked, even when they're speaking and testifying, but the amplification system helps them be heard and understood. That's actually working very well, and we've successfully continued to hold in-person hearings.

We're also developing and expanding on our existing remote video capability. The idea is that right now, many of you know that we've been using video teleconference technology for many years to reach out to remote places where contractors are located, but now we've just procured a brand-new video teleconference system that will work more effectively with the JSP firewalls and be able to go more places. We're also working on the ability to conduct hearings remotely, where people will be able to be invited into a secure system from their remote computers. That has not yet been unveiled, but we're working on deploying that in the very near future. That's all I have. Thank you.

Mark: Thank you, Perry. Greg, do you want to go to Devin next, just so we can finish this part of it and then go back to Heather?

Greg: Sure. Heather, are you on the line though, now? Are you able…?

Heather: I am. Can you hear me?

Greg: Why don't you do Heather, Mark? I would suggest at this point.

Mark: All right, Heather. Let's get you while we can. Please, go.

Heather: I appreciate that. I was on the line for some reason I couldn't get unmuted. Good morning. It's a pleasure. I'll try to go as quickly as possible to cover my material. It's a pleasure to provide the industry perspective today on a variety of NISP topics, many of which we already talked about. I'd like to go ahead, and I know it was already mentioned before, but to thank the outgoing industry NISPPAC members Robert Barb, Bob Harney, and Bryan Mackey for the years of support, and then

also welcome Derek Jones and Tracy Durkin. We do look forward to the next couple of years working with a dynamic team.

I want to say my perspective on industry has certainly changed over the past three years since moving from government to industry and finding a balance knowing firsthand government's role in the NISP was now having a glimpse of the demand and limitations put on cleared companies who truly want to do the right thing. The past year, the NISPPAC industry members, along with a memorandum of understanding industry association members, have worked hard to bridge the gaps between government and Industry. Industry's encountered an enormous amount of change in March of which was certainly needed, but nonetheless, the past few years have been pretty hectic on Industry. Industry is encouraged though, however, by the increased level of partnership and collaboration by the government at large. I do have five current, top five NISP priority watch list items for industry on the slide that was provided, but they are no particular order. I've said it a few times already this year, but I also want to offer our thanks again to the PAC PMO, ODNI, and OPM for the willingness to proactively understand impacts the industry on personnel security reforms as it begins. Industry understands we have a long way to go until full implementation, but we're sure that our voices will be heard throughout the process.

Next on foreign ownership control and influence was typically reserved as a concern to only limited amount of cleared companies or new companies waiting to be cleared that were usually under foreign ownership. Industry has already begun to see a shift in the government's FOCI to the control and influence portion. Where the Code of Federal Regulations, the CFR Part 2004 clearly defines ownership part of FOCI, it really doesn't do justice in defining the influence and control. Industry would like ISOO's assistance in having a better understanding and definition of control of influence towards FOCI and how it applies to the NISP. Without a clear and consistent objective of what we're trying to mitigate from all five CSAs and with a better understanding for industry of what they may be subjecting themselves to, it leaves a lot to the imagination. Understanding the risk tolerance, thresholds, and basis for the risk will be one of the areas industry would like to focus and discuss at the next scheduled NISPPAC FOCI working group meeting. Transparency to cleared industry and the government customers and advance the anticipated process changes only improves the ability to properly mitigate risk on the front end.

Moving on to our supply chain risk management. It's been a hot topic for many years but we're seeing action to the implementation of the many statutory and regulatory requirements. DoD already mentioned about the DoD adaptive acquisition framework and Industry realizes that many of the regulatory requirements are embedded in the acquisition process now, and not necessarily the NISP, but it does have a direct impact on the NISP at large, in the supply chain of the NISP contractors. One specific example is NDAA Section 889, where cleared companies are making self-attestation that they're not utilizing their end products and services. Where Industry is struggling with the government provided all-encompassing list of products and companies to ensure we're assessing into the same things and being consistent with our understanding of what is banned. We do ask DoD to provide some guidance on what products and companies we should be looking for in our supply chain. There is concern that industry may be missing a product or service, and thus we'll be putting our facility clearance and ability to bid on future contracts in jeopardy. There are other areas of focus on the supply chain, but this is really at the forefront of Industry's mind today.

Moving on. Not only is our operating environment affected by the COVID pandemic, we're also challenged by the changes in the security landscape. Thanks to the government partners for quickly adapting many of their processes and procedures during this uncharted time. In particular, thanks to DCSA for listening and adjusting, to keep industry operations still viable. Additionally, thanks to the DCSA Director for his transparency during the stakeholders meeting yesterday on how you're continuing to evolve from a service to an agency and absorbing the mission. Industry does understand that it takes time for transformational changes in government. We do appreciate the updates. I want to add that traditional security and cybersecurity are no doubt shifting and the ability to maintain and pay those highly technical required workforce employees to meet the emerging regulatory requirements will no doubt have an impact in the foreseeable future. As baby boomers are retiring, they are being replaced by a much younger workforce who enjoy the agility of working remotely, have the expectation for higher salary and are not often wanting to work in a structured security environment. When we talk about implementing the correct security mitigation strategy to counter the threat, we also have to start having that conversation about properly funding contracts to account for the right workforce, along with the best security posture to produce those products and services uncompromised for our

customers. This also goes to the conversation of getting the support that security is not necessarily just an overhead within Industry.

One notable area that Industry has been exerting an enormous amount of resources to manage all the government systems developed and utilized to manage the NISP. Thanks to ISOO and the NISPPAC members for forming the NISPPAC NISP Systems Working Group. It was enlightening to see actually all the NISP systems that were out there being used by industry. Whether it's an increased partnership on these systems being developed and tested, there was still one standout concern for Industry and government customers alike. The transition from JPAS to DISS is still a topic that requires much more conversation and a plan of action that includes functionality corrections, data integrity fixes, and training to be understood by all customers and government alike.

I'm moving pretty quickly here, but I'm moving over to my focus areas. Industry over the last year is focused on efforts of mutual benefit in addressing our collective concerns for the benefit of the entire cleared industrial base through increased engagement. We're finding, together we're stronger and have a bigger voice when we work together. I ask the NISPPAC industry members are utilized the greatest extent possible to address industry's NISP concerns with the government to ensure the full complexity of the NISP are considered when devising new and improved processes.

Also, the industry associations reach out to other associations and industry NISPPAC members when working on the NISP effort that affects cleared industry to ensure we're all on the same page. It is a consistent comment from government that I hear that often we have conflicting industry viewpoints. Being better aligned brings us closer to become the trusted and respected NISP partners. While Industry's making strides on collaboration with government, we're still finding many industry partners are fearful in speaking out during assessments and to self-identify vulnerability to government overseers, as some tend to be punitive in nature instead of working to the common goal of the mitigation.

Many times, we have very talented security staff within the industry, many retired government senior level executives that have many years of threat mitigation experience but are often overlooked for used to being in industry. We must work together to respect each other's experiences and expertise. Industry is hopeful that in the future, as

oversight models are evolving, that we get to the point where we can partner and provide full transparency of our security concerns, have a better understanding of a threat, and work toward a truly risk mitigation model to preserve national security.

Industry continues to track new legislation and policy changes that will have an overarching impact on our operations. It's vital that the CSs are transparent to the greatest extent possible, and at the local level, there's consideration for what the primary role of the contract is, which is to produce a product or service to the government, albeit uncompromised, but we have to find some balance. What really, I'm trying to say is when a new policy is developed, operating efficiency requirements added, not only is the policy changing, but industry also encounters additional add on non-contractual requirements, newly implemented training requirements and so forth. After a while these items add up and could potentially lead to contract delays on deliverables due to unforeseen requirements that were not anticipated in the original contract award. While Industry sometimes understands the importance of additional requirements, we ask for a well thought out plan that takes into consideration the impacts to Industry's operations.

With the additional requirements, industry is also experiencing overlapping interactions sometimes with oversight and possible fracturing of the NISP, and we ask that agencies try to deconflict; engage with each other before making contact with Industry. Prior to COVID, some contractor sites were visited by multiple government agencies reviewing the same material processes. Now we're about to add CMMC, and gearing up for CUI oversight, and we look at NISPPAC to work on potential resolution to avoid any duplication effort by both the government and industry at large.

That was pretty quick. I cut some things out, but I also want to thank everybody for the time today. We look forward to a new year and looking forward to 2021 and strengthening our relationships with our government partners. Thank you for your time today.

Mark: Thank you Heather, for that presentation. Anybody have any questions for Heather? Thank you, Heather. Devin, we're going turn to you to give us a CUI update.

Devin: Yes. Happy to. Good afternoon everyone. My name is Devin Casey for the CUI program. Just a quick update on where we are standing with the

CUI program. Currently, our office is still receiving some of the CUI annual reports from agencies. The primary deadline has passed. However, there are some extensions that have been granted. Those should all be in by the end of the calendar year. We use those to get a better understanding of where agencies are in their implementation of the CUI program and provide a general update through our annual report to the President, the ISOO one about the status of agency implementation for CUI for the government. We did have two CUI notices come out in October: CUI Notice 2020-06 and 2020-07. 06 covers the marking practices for waivers, when waivers are in place to alert users to the presence of CUI and CUI Notice 2020-07 covers the use of alternate designation indicators, or ADIs, with CUI when they're authorized by policy.

One of the big things that's definitely been going on in the CUI world has been DoD's implementation of CUI. We've gotten a lot of questions into our inbox and on some of our blogs as well about specific questions about DoD's CUI implementation. I'd like to point everyone to DoD's website, dodcui.mil, where they have a "Contact Us" there. There's also a link on the top of that website, where you can look for the points of contact for the different components at DoD and their CUI point of contacts there, as well as a bunch of information about DoD's CUI program. It is generally where I'll have to send you if you send us a question about DoD's specific implementation questions or concerns.

Final update. CUI FAR case is still a little bit delayed based off of the prediction on the unified agenda. We're nearing the closing time of comments for that, and it hasn't come out yet as predicted. Still delayed. GSA will have a new estimated timeframe coming out shortly, and you can always find out an update or anything new about the CUI program on our CUI blog.

We'll also be scheduling shortly a CUI stakeholder meeting for December to go over updates to the CUI program as well, which is a great way to stay up to date on any development at CUI program. That's all I have.

Mark: Sure. Anybody have any questions for Devin?

Jeff: This is Jeff Spinnanger. I have a question, but just a comment to echo something that Devin said, and thank you for mentioning it. For those of you who have questions pertaining to the DoD CUI program, I cannot emphasize enough the importance of heeding Devin's outstanding

advice and going into the DoD CUI webpage for your information. Point of comparison, we're like at the beginning of our sophomore year of high school and the NARA page for CUI is grad school. We are focused very much on implementing and aiming at full requirements. If you go to the NARA page, where Devin points, pertaining to the DoD program, I think you'll find yourself very confused, very quickly. Over.

Mark. Thank you, Jeff.

Greg: This is Greg Pannoni. I don't want to belabor, but it is true, as Devin points out, we do get a fair amount of inquiries in ISOO through the mail electronic mailbox and we divert them back to DoD. It comes from government and industry alike, but if you could just put the word out whether it be Industry through your various MOU groups, just to start with…most cases, it's going to be DoD and, or the DCSA rep, but not make ISOO/CUI office your first stop, because it doesn't do anybody any good because DoD needs to be aware of these issues, and we just have to turn it around to them if we should receive it. Over. Thanks.

Mark: Great. Okay. Anything else on CUI? I think we've got seven minutes left before we lose the bridge call. That said, let's turn quickly to any new business. Does anybody of the committee, the board, have any issues they'd like to bring up? Hearing none. Does anybody, and I'm referring here specifically to DHS, NRC, and DOE, want to update us on any of their feelings during the COVID crisis here? How are you adjusting to it? Are you adjusting to it fine? Are there any glitches, any problems?

Tracy Kindle: Sir, this is Tracy Kindle from DOE. We had initially given a COVID update at the last NISPPAC and basically the Secretary authorized of course maximum telework flexibility. He also had issued some guidance as it relates to COVID that went out for about six months, and some of those things that the secretary had issued were extended last month for another six months. We're still continuing on with the things that we're doing from a COVID perspective.

From a PERSEC perspective, we did adjust some of our reporting requirements, timelines, and due process actions for clearances. In addition to physical security and classification perspective, we adjusted our required inventory, self-assessment, and some of the training timelines that we were having our contractor partners adhere to. That's it for DOE as it relates to COVID. Really, we're pretty much in the same status we were as we started in March.

Mark: You and everyone else. I'm sorry. Does anybody else wish to chime in on that?

Rob: Hey Mark, this is Rob McRae, DHS. Similar to everyone else we continue to be in a remote work environment. We really experienced no identifiable impact to our ability to continue supporting the industrial security side, and we don't see any lag in processing 254s and then continuing to support our industry partners. That's about it from us.

Mark: Okay, great. Okay. Anybody else? Hearing no one else. Let me wrap this up. Our next NISPPAC is scheduled for April 14th, 2021. We're going to be dropping down to two NISPPAC meetings a year instead of three, as has been done for the last 10 years or so. We canvassed all the committee members, and that was the consensus…that two would do it. If for some reason, two are not sufficient, we'll revisit that. That's not set in stone, but that's what we're going to aim for this coming year. The April meeting undoubtedly will be 100% virtual. I don't see this COVID crisis ending until at least late spring, early summer, and that's being optimistic. Let's see. Obviously, once we get by the crisis, we will begin to hold meetings in person again at the McGowan Theater. As a reminder, all NISPPAC meeting announcements are posted in the federal register approximately 30 days before the meeting, along with our own ISOO blogs. You can always log into our blogs, just probably get the latest information. Before I adjourn, is there anything anybody else would like to say, comment on, or bring to our attention before I put the gavel down on a meeting with three minutes left? Hearing non,. I'm going to adjourn this meeting and wish you all a happy holiday season. Thank you very much for your patience as we struggle with this technology that we've got. Again, I think the meeting went very well, and I appreciate all your help and cooperation. Okay. That's it. Goodbye.