Event Producer: Welcome and thank you for joining today's National Industrial Security Program Policy Advisory Committee meeting, also known as NISPPAC. To receive all pertinent information about upcoming NISPPAC meetings, please subscribe to the information security oversight offices overview blog at isoo-overview.blogs.archives.gov or by going to the federal register. All available meeting materials, including today's agenda, slides, and biographies for NISPPAC members and speakers have been posted to the ISOO website at www.archives.gov/isoo/oversight-groups/nisppac/committee.html, and have also been emailed to all registrants. Please note that not all NISPPAC members and speakers have biographies or slides.

While connecting by phone is necessary to attend today's meeting, there is no requirement to log on to WebEx. However, you are welcome to join WebEx with the link provided with your registration as all available materials will be shared during the meeting on that platform. If you have connected through WebEx, please ensure you have opened the participant and chat panels by using the associated icons located at the bottom of your screen. If you require technical assistance, please send a private chat message to the event producer. All links will also be shared periodically through WebEx chat.

Please note all audio connections will be muted for the duration of the meeting with the exception of NISPPAC members, speakers, and ISOO. We are expecting a fairly large audience today, because of this, we will not be taking questions from the public over the phone. Please email your questions and comments to nisppac@nara.gov and someone will get with you. Only ISOO and NISPPAC members will be authorized to ask questions throughout the meeting.

At the conclusion, a survey will be provided for feedback. If you would like to be contacted regarding your survey responses, please include your email in the comments box so the NISPPAC team can get back to you personally. Let me now turn things over to Mr. Mark B. Bradley, the director of ISOO, as well as the chairman of the NISPPAC.

Mark Bradley: Thank you so much, Madam Producer, for your kind introduction and your instructions. Good morning, everybody. Welcome to the 68th meeting of the NISPPAC. This is the fifth NISPPAC meeting that's being conducted 100% virtually. This is a public meeting. Like our previous NISPPAC meetings, this will be recorded. Recording along with the transcribed minutes will be available within 90 days on the NISPPAC reports on the committee activities webpage mentioned earlier by our event producer. We're planning on a five-minute break in the middle of the meeting, which I will flag as we move closer to it. I will now begin attendance for the government members. I will state the name of the agency. The agency member will reply by identifying themselves by name. Once I have gone through the government members, I will then move over to the industry members. After the industry members, I will then proceed to the speakers. All right, ODNI.

Valerie Kerben: Good morning, Mr. Bradley. It's Valerie Kerben here.

Mark B.: Good morning, Valerie. Department of Defense.

Brad: Hi, Valerie. Brad. Thanks

Mark B.: Department of Energy.

Natasha Sumter: Good morning. Natasha Sumter's here.

Mark B.: Morning. NRC.

Dennis Brady: Dennis Brady.

Mark B.: Morning, Dennis. DHS.

Rich DeJausserand: Morning, everyone. This is Rich DeJausserand

Mark B.: Morning, Rich. DCSA.

Keith Minard: Minard, DCSA.

Mark B.: You're faint there, but I got it. CIA.

Felicia: Good morning. Felicia here.

Mark B.: Morning, Felicia. Department of Justice.

Kathleen Berry: Good morning, Kathleen Berry.

Mark B.: Morning, Kathleen. NSA.

Brad Weatherby: Brad Weatherby from NSA.

Mark B.: Morning, Brad. Department of State.

Kim Baugher: Kim Baugher, State Department

Mark B.: Morning, Kim. Department of Air Force.

Jennifer Aquinas: Morning, Jennifer Aquinas, Department of Air Force.

Mark B.: Morning, Jenifer. Department of the Navy

Steve James: Department of the Navy.

Mark B.: Would you please identify yourself by name, please?

Steve: Yeah. Department of the Navy, Steve James, primary representative,

Mark B.: Right. Thank you, Steve. Department of the Army. All right. Nobody from the army. I'm going to now turn to the industry members. Heather Sims.

Elizabeth O'Kane: Elizabeth O'Kane from the Army.

Mark B.: Oh, okay. Great. Thank you. All right. I'm now going to turn to the industry members. Heather Sims.

Heather: Heather Sims, industry present.

Mark B.: Great. Rosie Borrero

Rosie: Rosie Borrero, present.

Mark B.: Great. Cheryl Stone.

Cheryl: Cheryl Stone, present.

Mark B.: Great. April Abbott.

April: April Abbot, present.

Mark B.: Morning. Derek Jones.

Derek: Derek Jones, present.

Mark B.: Great. Tracy Durkin.

Tracy: Tracy Durkin, present

Mark B.: Great. Greg Sadler.

Greg: Greg Sadler's present

Mark B.: Right now, I'll do a quick roll call for the speakers. Make sure we get everybody lined up. Eric Person.

Eric Person: Yes, sir. Good morning, Eric Person's here.

Mark B.: Morning again, Chris Heilig.

Chris: Good morning, Chris Heilig.

Mark B.: Morning, Chris. Bob Mason.

Bob: Good morning, Bob Mason's here.

Mark B.: Morning, Bob. Chris Pollock.

Chris: Good morning, Chris Pollock is here.

Mark B.: All right. Great, Chris. David Scott.

David: Scott present.

Mark B.: All right. Donna McCleod.

Donna: Good morning, Donna McCleod is here.

Mark B.: All right. Paul Dufresne?

Paul Dufresne: Good morning. Paul Dufresne here.

Mark B.: All right. Perry Russell Hunter.

Perry: Perry Russell Hunter for DOHA is present.

Mark B.: All right. Thank you, Perry. If anyone else is speaking during the NISPPAC that we have not heard from, or I did not know about, please speak now.

Greg: Mark B., this is Greg Pannoni. Just for the record, our colleague sitting next to me, Jeff Spinnanger is here, and he is representing the Department of Defense.

Mark B.: Okay. Morning, Jeff. All right. Again, we've requested everyone identify themselves by name and agency if applicable before speaking each time because this is being recorded and then as you all know, we do a transcript and just makes it a whole lot easier for us if we don't have to try to guess who actually talked.

I want to provide everyone with our agency's quick COVID update. For a month now, we've not had any restrictions on in-person meetings for all NARA staff and all NARA buildings. However, most of our staff are still teleworking all the way and are moving into much more of a hybrid state, as I'm sure a lot of you are too. We do not yet know with large gatherings, such as the NISPPAC working groups if the next NISPPAC will be in person because Washington DC is now at a medium COVID transmission level per CDC guidelines but obviously, we will keep monitoring that. And I personally hope very much we can dispense with this virtual meeting and move into actual face-to-face like we used to, but that's to be determined.

Additionally, we've had a few changes to the NISPPAC's membership, Dr. Jennifer Obernier, the primary with the Navy has left. She's replaced by Steve James who's on this call. Additionally, NSA alternate Shirley Brown has also departed. She's been replaced by Blane Vucci.

The NASA primary, Kenneth Jones, is departed as well. At this time, a replacement has not yet been designated. Lastly, and also critically important, as most of you know, Greg Pannoni, the designated federal officer for the NISPPAC. This will be his last NISPPAC meeting before he retires this summer after over 42 years of federal service of which more than 17 of it was spent here in ISOO. Greg has been an integral part of the NISP community. He's been a marvelous deputy. I couldn't have asked for a better one and he's just virtually indispensable. To say he will be sorely missed is an understatement.

Greg, thank you for your dedicated lifelong service. And obviously, we wish you the very best. And we look forward to you continuing the work that you've done most of your professional career.

Greg: Thank you, Mark B. Good morning, everyone. And it's been a pleasure to be involved with NISPPAC, all these many years and even before when I was with DoD. The partnership is invaluable. I think many of you that know me know that I've embraced that from the beginning. Doesn't make sense to do it any other way to involve critical stakeholders. So, I hope to continue working with all of you. I do have a couple of things while we didn't have any real formal action items from the last meeting, we did have one. And then there are the NISPAAC minutes, which were certified from the last meeting to be true, correct, and accurate that were finalized on February 2nd. Next item, a colleague from DoD recommended that we return to three meetings a year. And while we think that's a great suggestion, we are not in a position at ISOO to do that at this time.

It kind of falls in line with another right I wanted to mention. We have two vacancies right now and have those filled by the time we have our next NISPPAC meeting, which will probably be in October. Once the dust settles on that, hopefully, we'll be a better resource to consider returning to the three meetings a year, which I think is an excellent idea. So, there's that.

By the way, this is two and a half years, since we've had sort of semi-live meetings and to paraphrase Frank Sinatra, nothing like having live meetings is good, but we have to deal with the technical stuff well. Okay, we have those two vacancies. One is for the CUI Lead in ISOO. Heather Harris Pagan who has been doing a great job on NISP work has a senior lead for that in ISOO. She is wearing both hats right now and doing a great job helping out with our CUI. We have to have that position filled and then we also have a chief of staff position open.

One last thing we should know, someone more noteworthy than me is retiring effective April 30th. And that is the Archivist of the United States, David

Ferriero. He served for more than 12 years and so, we'll have an acting deputy Archivist. Debra Steidel Wall will act for however long it takes the Senate to nominate and confirm the president to nominate from the Senate to the new Archivist of the United States.

David has been a great advocate for openness and the use of technology to convert records to digital. And you may ask why ISOO and NARA? Well, at the end of the lifecycle classified information, gets declassified, made available to the public. So that's core of NARA's mission is openness and records. So, with that, are there any questions? Okay, thank you. I'll turn it back over to the chair.

Mark B.: Thank you, Greg. This time, we'll now introduce our speakers for updates. I'm going to go to Ms. Heather Sims. NISPPAC industry spokesman will provide the industry update. Heather, the floor is yours.

Heather: Heather Sims, Industry speaking. And it was much easier doing this in my basement in my PJs. Definitely a lot different. It's definitely been a long two and a half years. I have a year and a half to go in NISPPAC, but it's definitely been a pleasure representing you at the national level. It's not easy by any means. We want to thank the other industry NISPPAC members for all the countless hours that we were on the phone and we're collaborating, making sure that we're truly representing the industry at large on small, medium, and large companies. And this year, we're trying to be more transparent in our efforts. There are many companies out there that are not represented by the MOU that support us.

We did create a newsletter to talk about who we are, what we are, and what we're trying to do. We pushed it out through all five CSAs to make sure that we're reaching those companies who have no ideas they're represented at the national level of the policy. So, if you know somebody who doesn't know about NDIA, all the MOUs that are out there, or what Industry NISPPAC does, please send them up so we can make sure we can get them involved one way or another.

I also want to thank the MOU members of the Industry NISPPAC. Without you, we would make sure that we have that industry voice collected. It starts with the working groups, collaboration, and making sure we get the right people and the right working groups for the right skillset. So, thank you for sending those names so quickly along the way. I also want to thank Greg Pannoni for your years of service. I was a little lost when I first started. So, he gives me the vector checks that I need to make sure that I'm doing the right thing along the way. So, thank you and happy wishes on your retirement.

I also want to thank, and I know Matt Eanes is in the room and you're going to hear from him later. So, we started something about two years ago that wasn't done in the past, making sure that industry had a voice proactively when it comes to national level policy, specifically talking about personnel security

reforms. So, Matt Eanes thanks for your continuous collaboration with industry to review those documents, and historic personnel security reforms. So, we do appreciate that.

I want to be mindful. We talk a lot about DoD, and DCSA on the stage about what's going well. And sometimes what's not going so well. There are four other CSAs out there, and I want to thank them along with DoD. We do have issues. We have concerns, and we have to reach out to them. Thanks for your quick responsiveness. It truly matters to get industry responses to the questions or guidance implementation in a quick manner, to make sure that we're doing the right thing. And speaking of DoD and in this case, DCSA, this past year, we worked collectively in industry, and hopefully, you were reached out to collect what was going well with the 32 CFR implementation. We rolled up an industry report and after-action report of how well the 32 CFR rolled out DoD oversight implementation.

And we sent that into DoD and to DCSA as a guideline on things that we can work on together. What needs to be further clarified in that 32 CFR? I don't know if anybody else read it as many times as I did, but it is not an easy read. And every time I read it; I find something different that I thought I knew. So, thanks to DCSA for providing that quick clarifying guidance when we need something with industry to make sure we're doing the right thing. If you haven't seen that after-action report, I'll make sure you have it before we leave the conference. We want to be transparent. We want to make sure that we're providing the result of the collection from the industry as wide as possible. We're going to try to continue that trend every year on what's going well, and what's not going so well so that we can share those lessons learned and not repeat the issues from our past. So, thank you all for who provided those.

Now, those who know me and heard me speak before, I will always say good things, but then I'll always put a little thing that we can do better in there. And then I'll roll that up with some little good things. And while things are going really well, and we have some good collaboration going on, we can still do better and are going to talk about it. We had a lot of discussion about NBIS, but I'm going to open that up just a little bit more. That's every system that the federal government provides that industry has to touch. We have to do better to make sure that we have a strategic plan. We have to have a great communication plan. And that plan has to cover how we're going to interface with those systems at every level. Oftentimes industries, an afterthought system requirement have built for government stakeholders, not necessarily industry stakeholders. We have to do better.

I myself came from the government. I thought I knew what industry needed. Rude awakening, when I came out and couldn't get into DISS and after four months. It was pretty difficult. So, making sure that we contest things in our environment to make sure that it works for all industry partners that are out there. Many of us spend countless hours doing administrative work, typically to

fix the system that we didn't create. So, I will say that I didn't talk all about NBIS, but any system that the government provides to us, we really need to do a better job there.

I will say one of the issues that we're really concerned about now is to take care of DISS transition. We surveyed about 200 and approximately 250 industry companies, and it was well into the millions of resources and man-hours that industry had to eat up the cost to help get that data integrity, that system correct. And our main concern right now is that's going to be the same for the DISS and DISS transition. So, while we're trying to meet a timeline, we want to make sure that we have an effective, trusted system that industry does not have to fix our own data. So, without a doubt, we all want to get to one system pretty quickly. We don't want to operate in two systems, but again, we want to make sure this system works.

Now on the positive thing, there has been a tremendous amount of work done on the personnel security front. I remember coming to the conference as a government member, and that is all we talked about, how bad the personnel security investigation process was, and how bad the adjudication process was. So, thank you to, I will say DoD at large and specifically VROC adjudication and the personnel investigation piece of that. The tremendous ground has been made and industry does appreciate that. I talked to Heather Greene a little bit last night. She looks more relieved at these conferences now. Not in the hot seat. So that's a lot of work and the industry was instrumental in making sure the improvements were made there as well.

Not that we're going to keep our eye off those timelines. And I know we talked about reciprocity and transfer trust, but I'm very hopeful that Trusted Workforce 2.0 will get us to where we need to get to. But keep in mind, I learned just the hard way also is industry can move at a very fast pace. The government does not move. So, I'll be retired probably once we get to FOC on trusted workforce 2.0. Hopeful, I will say.

And with that, a couple of other things that are going very well, the collaboration. We did have the DCSA stakeholders with the deputy director of DCSA last week. So, we're looking for more engagements like that so we can actually engage and not be briefed. So, looking for that two-way conversation so we can bring up industry's issues, and hopefully come up with some solutions of how we can solve those.

So, thank you to all the five CSAs, DoD, and DCSA for all the hard work this year, working together. But I will say, I'm not done. I know you're ready for me to end there. I'm going to point my attention to industry. We have to do better speaking as a collective voice. Often, we're talking in different voices, different priorities, and we are going to have different priorities, but when we're talking at the national level, and legislative level, we have to be able to speak with one voice.

I'm speaking from personal experience. After I heard multiple complaints from multiple people, I toned it out because when everything's important to industry, nothing's important to industry and nothing's important to the government who's trying to help us resolve that. So, we have to do better. We have to lay the foundation to have a strong united industry front when we are communicating with our government partners.

And we talked a little bit yesterday about how industry is going to be represented at those levels and expanding the aperture a little bit then outside of the industry NISPPAC members being more inclusive of the MOU members. But I will say for those that come behind me, we need to really clarify and tone up those three priorities, three to five priorities, and really concentrate on those.

I will say from personal experience, I am employed full-time by L3 Harris, but I will say I spend about five or six hours every evening to include a weekend really working on issues for industry. So, it's selfless, I will say when I'm there. But then my husband says it's something that I always do. I'm looking for a lot of opportunities when I'm finishing my role to spend my time with my family.

But I say that because people go into it thinking that it's going to be very easy, and things will just flow. It doesn't work that way. It takes a lot of networking, a lot of hard work to get there. But I will also say that because I encourage you, it's probably the best time in my life being able to represent industry at this level. I was bamboozled into the position, but I will do it correctly. So, I will say that. And most importantly, I want to thank everybody again for coming together. This is great. Lots of networking. This is truly where the work happens. So, thank you.

Mark B.: Thank you, Heather. Does anyone have any questions for Heather? All right. Hearing none, I'm going to turn to Jeff Spinnanger, the Director for Critical Technology Protection for the Office of the Under Secretary of Defense for Intelligence and Security. He will give an update on behalf of DoD and the NISP executive agent or as the Mr. Executive Agent, I should say, Jeffrey.

Jeff Spinnanger: Morning, Mr. Chairman. Good morning, Greg. Everyone. Thank you. It's good to be here with you in person, (it's loud). I'm particularly excited for the opportunity to really sit next to Greg. We were chatting just before, and he noted that he's been present for more than half of all the 68 NISPPACs that there have been. That's a lot. I think it may give a little bit more characterization to the level of effort and support that Greg has represented on behalf of the NISPPAC.

And I think about this sort of thing a lot. Longevity, we've relied on a very small number of people for a long, very long period of time to really be stewards of the National Industrial Security Program. And those folks have decided that there are other things that they would like to do in their lives. And so, echoing a

little bit of what Heather said but also noting the importance, this is an important forum. These are important roles. And hopefully, there are folks out here who have interest in them.

Also, Greg stole my thunder and the first talking point I had, which was the subject regarding, maybe revisiting the number of public meetings that we have a year. I completely understand the challenges. One, pandemic challenges, staffing challenges, and the like, by noting again, what Heather said, and then everything that's playing out right here, the fact that we were able to leverage this forum for the purposes of this public meeting is kind of a backdoor way to public engagement, but it works. And it's very, very important. It's important for all the official reasons. It's more important for, I remember the breaks in that wonderfully historic auditorium in the archives, and we have a break in the middle, which I know we don't have a break this time.

Right. Excellent. That's really good. But it's the dialogues that take place right in and around the public setting that are important, and I wrote here transparency in public discourse, they are absolutely vital to the work that we do to the integration of public policy, industry engagement, and actual products. The work on the other end. So, thank you for that update. And please let us know what we can do to continue to kind of keep a drumbeat on this because I think it's quite important.

Next, as a function of the policy. And again, echoing some of the comments that Heather made before. So, I appreciate very much that she's read it more than once. I imagine many of you have done the same. It's not easy to read. It's not super fun to write. Nonetheless, we're pretty happy with where we are. The feedback that we've received so far and really, again, thank you to DCSA, and it's a primary outward-facing role here to be a facilitator, to bring information back, to make these documents as living as they can possibly be. That is important.

We celebrated the fact that we got the rule out there and about a minute and a half later, we began the first amendment. It was more like a week, but not much more than that. And we established an amendment regarding reporting and pre-approvals foreign travel associated with SEAD 3. The timeline was extended to August of this year. We have no changes or requirements that we're aware of for any further extensions or amendments to that effect. I'm very certain that our overseers in rulemaking would take a dim view on any notion of that. And so, you'll hear more about that in the updates that Keith Minard and others will provide here later in the meeting.

But we're not done there. So, we got the first one done. So, we're on the second amendment. And the second amendment is largely oriented around public comments that were received during the issuance process. We are at a stage now where we do what's called DoD-wide coordination. So, the DoD is a giant Federation of components. The services and others. We will work through that

process and take some time. Stakeholders' kind of vary. So, some of the larger companies, but small components have an interest as well. So, we will go through that process. And then we'll repeat that on a federal scale.

So, the process moves forward again with an eye for transparency. We use this forum to provide updates for those pieces that are not in the public space. And of course, as it moves forward and as well, I'd like to continue to provide updates on an obvious one, the importance of cybersecurity within the framework of the NISPOM. We haven't yet found a seamless and repeatable process for industry direct use of classified cloud, but we're continuing to coordinate with our partners at this in DCSA, and although, I want to say I'm not happy with where we are. We are making progress and again, and a nod to, this is a public discussion. So, I'm not a big forecast person. I said that in prior meetings. But I think it's important that we kind of shine a light on ourselves here on what is in many respects, maybe the most under-viewed. And I would, I think, make a pretty strong case that. It's maybe the most important aspect of what we do right now.

And so, to that, at the last NISPPAC meeting in October, public meeting in October, I reported that a project that my office sponsored at the Applied Research Laboratory for Intelligence and Security, ARLIS led to the development of what we call a vendor-neutral playbook aligned to DISA and DCSA current process guides, including wiring network, connection process, security requirements, et cetera, that are intended to lead to authorization to operate.

I also described that through the process of developing this playbook and observation of several pilot efforts, we uncovered a number of challenges that made the process possible, although arduous doesn't, I think quite capture the challenges at this time. ARLIS made a series of recommendations and requirements. They framed those, they wrote them all down, which is super helpful. And then we put them out and asked NISPPAC to review those in earnest. And again, with some echoing of what Heather mentioned before, I would be remiss if I didn't thank Heather and all the NISPPAC industry members for taking the time to go through in really quite agonizing detail to provide meaningful feedback in the work that we asked ARLIS to sort of as a third-party broker put together. We look forward to getting DISS/DCSA kind of in the room on that, understanding that the process will end when we digest all that. We'll move forward.

So, I will end by saying, I have more updates to provide on this, but again, by bringing it forward in this way, I think we're going to be able to hold ourselves to a timeline and get over the line on what I think is an important issue. We do this right, the number of ATOs, which number in the thousands, and really in the tens of thousands when you aggregate across all the stakeholders that are out there DCSA and others, I don't know that seems likely and so there's a better way. I'm convinced of it.

Finally, two other topics really briefly, and I'll stop, Mr. Chair. And that is, so the department continues to make progress. I know folks in the audience are paying attention to requirements that were levied under NDAA 847, FY20 NDAA regarding foreign ownership control, and influence assessments that are deemed wide. They are largely predicated and intended to be designed on the way in which it's undertaken today, steady-state, and for a long time under the industrial security program. But they're broader, two pieces are of importance to us, and we want to get it right. And that is one as a function of award and two, for all contracts greater than $5 million, including subcontracts. That's a pretty tall order. And so, some of the scales that's laid out there runs just in drastically high numbers.

Not a tremendous amount of accuracy in those in that speculation, but what is... And so instead of starting big and working small since big is very undefined again with some really great partnership from DCSA and in particular, Keith Minard who I want to call out publicly, we've kind of worked out from up. We know what works; we know what's familiar as it relates to FOCI requirements in the Industrial Security Program. There's language in the statute that encourages as a frankly direct us to kind of build out from that same model. And we're building out from there.

With that in mind, again, all roads start with policy. So, we're at the issuance point. We've gotten through all of the editors across the department. Good feedback, mostly. And now we're off to the lawyers. The lawyers understand the urgency of this. When we put some heat on ourselves here, we can create some accountability and we tell the deputy secretary something's important. And so we are on target, I believe for the end of FY issuance. Hopefully I'll have a more firm update and you'll have something to see that's actually out by the time we meet again.

Jeff: Than to see that's actually out by the time we meet again. Again, just like anything else, that's not where the process ends. It's really where it begins. There's a whole mountain of work on that, that is certainly levying on DCSA and then for the industry. So, we want you to be aware. We want industry to be aware. We want the NISPPAC to be aware of this as it continues to move forward. But we don't need action at this time, we need to get over the line on the policy. Where industry and NISPPAC will come into play, we know there's a rule that will be required here. There'll be a DFARS clause that will have to come out the other end. And that will be informed by the policy, not by this. I mean, certainly, everything underpinned by the statute. But if you know how this stuff works, we'll build the DFARS requirements off what's first published in the department's issuance.

And finally, our last topic today, we'd like to bring up again, an ongoing issue regarding joint ventures and FCL requirements. There was a provision or there's a provision in FY22 NDAA. Section 16.9 states that if both entities that form a JV are cleared, the JV company itself does not require a facility clearance. To

address a section 1629 language, DOD is intending to publish a directed type of memorandum to provide guidance on joint ventures that had been awarded via declassified contracts. There's similar language in the small business administration federal rule published in late 2020 that we believe must be addressed in this regulation and guidance. So similar is a wonderful term, but similar is not the same, which means that it's open to just a mountain of interpretation and that's sand in the gears, to put it bluntly. So, the Air Force has encountered and confronted this head-on. So, with that, I'd like to briefly turn over to Ms. Jennifer Aquinas for some input.

Jennifer Aquinas: Thanks, Jeff. I appreciate the opportunity to comment on this issue. The DOD issues contracts to joint ventures frequently. So, questions about this frequently come up. The Air Force was the first contracting activity to encounter this issue. And we successfully worked through an exception to the policy process. That cleared the way, and we were able to issue a classified contract to an uncleared joint venture and allow performance on a contract without a facility clearance. But the regulatory conflict remains between the small business agency and the NISP. And until this is resolved, there'll be continued confusion. We're concerned about contract protests and their impact on admission and cost. At the last NISPPAC meeting in October of '21, ISOO advised that this small business rule was not intended to remove the facility clearance requirement. At that time, ISOO committed to issuing a notice to provide a cost put and I am waiting for an assessment from ISOO today.

Jeff: Thank you, Jennifer, for that. And again, I'll end by saying, and just using this last issue as a really great example. This is a knot to the utility of the public forum, to put this out there in this way, create some accountability in the process. No one's running around with their hair on fire, and we're able to stay in front of what frequently ends up as a litigation matter. And that's really what our end state is. Everyone's trying to do the right thing here, but we see the world where we sit on it. And this is an example as to where those different world views can collide with unintended outcomes.

And so, with that, Greg and the NISPPAC team one, thank you very much for your continued attention on these issues. Thanks for working out the technology wizardry. I have the word technology in my title, and it's a lie. I'm glad that Jennifer's here, so I'm not the only one without a computer in front of them. But to be able to put this together and to be able to shine a public light on these kinds of issues is important for all of us, regardless of where we sit. Thank you very much.

Mark B.: Thank you, Jeffrey. Does anybody have any questions for Jeff?

Greg: Mark B., this is Greg Pannoni.

Mark B.: Yes, Greg.

Greg: It's on now. Sorry about that. It's just a good time to mention the follow-up that ISOO's involved in with this issue of joint ventures and clearing the entity if in fact, it is an entity. I'm told by our attorneys; that some joint ventures can be created by contract and therefore technically are not a legal entity. In any event, I don't want to spend time here getting into the details. We are still working on an ISOO notice that will clarify things. The attorneys have assured us they've spoken to SBA, and it was not their intention that we would not vet a joint venture legal entity. You heard this morning from the speaker about one of the methodologies that he's most concerned about is creating entities by some of our adversaries for illicit purposes. So, we hope to have this done in short order to clarify things. Because admittedly, the SBA rule is a bit interpretive as I'll say with a lot of government regs are. But we are going to get this thing fixed so that it's clear to everyone. Any questions? Okay. Back to you, Mark B..

Mark B.: Okay. Thanks, Greg. I will now hear from Mr. Keith Minard, Senior Policy Advisor with the Industrial Security Directorate of the Defense Counterintelligence and Security Agency. Keith, over to you.

Keith Minard: There we go. Does this work now?

Mark B.: Yes.

Keith: Okay. Good morning. Keith Minard, DCSA.

Mark B.: Yeah.

Keith: Let me start off by thanking Greg Pannoni for his support to the NISPPAC, industry and government members, as well as the entire NISP community. The staff at DCSA would like to congratulate you on your retirement and good luck. I have a couple of key updates this morning on leadership. We've got a new Deputy Director DCSA, Mr. Daniel Lecce, and a new industrial security director lead Mr. Matthew Redding. Both are here at the event. I'm sure you've talked to them many times, or you will talk to them before the event's over. While I get to represent the NISPPAC from a DCSA perspective as the primary member, I do have to say that it takes a large team of action officers at DCSA to make what happens, happens at the NISPPAC, and take on the issues and challenges that come up to look at resolution and actually work forward to make better processes and practice. So, it's just not those on the table up here, but a large workforce that's on the back end, making these things happen.

So, on the first thing, DCSA is back to onsite assessments. So, you should see our personnel out in the field onsite doing your security reviews. And that's a big change for us coming from the last couple of years of continuous monitoring events. So, Heather talked about the NISPPAC AAR year in review, I like to call it from last year. Last fall, after we worked through implementing the NISPOM Rule, we thought about asking the NISPPAC industry for, I'll call it a scorecard or an AAR for FY21. And we've got that scorecard and we're working through it

now. And we're working through all our action officers to look at the things that we can change, things that we can improve, and look into best practices that came out of last year's implementation of the NISPOM Rule. It was a great time to evaluate ourselves on how we do business with industry, communicate, and engage.

This was the first time we've had a major event like this since 2016, an insider threat. And what's interesting is actually Heather Sims and myself rolled out insider threat in 2016. In fact, that change came out at a NDIA event, the week we were in Scottsdale. So, we're in NDIA now, so these things keep going around and circling. So, we do like to thank NISPPAC industry for providing that input we see as a best practice, and it'll continue next year. So next fall we'll ask for the same product.

So, I think one of the biggest things that industry's asking about is we'll talk about one last component of the NISPOM Rule implementation for contractors under DOD cognizance. And that's the SEAD 3 reporting for foreign travel. As Mr. Spinnager said, the amendment to 32 CFR Part 117 deferred the reporting of SEAD 3 foreign travel requirements for 18 months from the issuance date. So, this will begin in August of this year. So, we want to make sure that we have the right capabilities. And part of this was the ability for industry to bulk upload foreign travel, rather than doing one-by-one submissions of foreign travel, to try to better enable the reporting requirements and ease some of the strain. So, the deferral was put out, it enabled the development of both tools. We look like we're still on time for June deployment of the planning tool for its use in August of this coming year, this summer.

Okay. We want to make sure that when that comes out, we're ready for this. We want to make sure we have a communication strategy. We want to make sure we have training and awareness products, whatever we need to better enable implementation by cleared industry. I do want to make a couple of notes that as we look at foreign travel reporting and for the reasons of SEAD 3, we will begin in August going forward. We're not going to ask to go backward. But I will have to note that if you have to fill out an SF 86, all foreign travel has to be reported on that. So, you have to keep in mind the SEAD 3 forward, 86 still requires the period of time required by the forum for submission.

To continue with SEAD 3 a little bit, we actually saw patterns of requests for frequently asked questions. We revised the SEAD 3 reporting questions, and FAQs on our website. We refine them based on input from industry and things that we saw that can better enable and communicate how to do things. And along with that, we've had staff create an intuitive tool that helps industry walk through the types of contact reporting that are required by SEAD 3. It's a yes, no helps drive through a thought process to better understand how to report the SEAD 3 requirements. And I have to say, I think the team at DCSA has become somewhat of subject matter experts on SEAD 3 in the federal executive branch from all the work that's being done. Industry, certainly we appreciate the work

you're doing. It's very important. As we report things Heather Sims upfront here, we want to get ahead of the CDSD bi-year reporting, and then we can see we match through that.

The last thing I have on tools and resources as you may have seen it. The NISPOM actually refers to national policy for safeguarding. And one of the key things that came up was security in depth. In the last month or so, we've actually posted a video audio short on security in-depth. We found those products very useful during the implementation of the rule. Six, eight-minute slides that are narrated for easy use and information updates.

So, the last thing I have actually is, and I know this is something that keeps coming up in a larger area, is that we're still working. You may know that the DOD manuals in NISPOM were rescinded at the end of November. So, we're working through the other policy actions to rescind the former Industrial Security Letters. We've issued new others and we have a couple of more that are coming out. But the reason we're rescinding these, and I'll use some examples, you may have noticed as you read the NISPOM, it talks about certain types of incidents now that may occur on unclassified systems. And the 2013 ISL in cyber, that was the key point in it. Another example is safeguarding. We now point to national policy for open storage.

So, the former ISLs, there are about 34 of them, will be rescinded. And we move forward with the new batch of ISLs. To give a status, we've got two more that are still in the pipeline. It does take some time to get these out. It's the revision to the insider threat. Industry and NISPPAC have reviewed these ISLs. Key point is that it talks about your program as having a plan, your self-inspection, and implementation of the minimum requirements.

We have added the National Insider Threat Task Force Maturity Framework as a reference. And the other is an ISL that covers about nine different topics, from designated government representatives to the destruction equipment, and things like that. TS accountability. I know that's a major thing. So, we've run down our ISLs. We've reduced the amount now. And what we do want to know with industry, when you need additional guidance, please work through industry NISPPAC to help us understand what's needed to better implement the program. Last thing I have is actually later you'll hear from Ms. Donna McLeod on our DCSA personal security metrics from the working group and Mr. David Scott on our systems authorization updates and metrics. Thank you.

Mark B.: Okay. Thank you, Keith. Anybody have any questions for Keith? All right. Next we'll hear from Ms. Valerie Kerben, Chief, Policy & Collaboration Group, Special Security Directorate, National Counterintelligence and Security Center Office of the Director of National Intelligence. Valerie, the floor is yours.

Valerie Kerben: Hi, good morning. Thank you very much, Mr. Chair, and hopefully you all can hear me pretty well. It's a great opportunity to always be here and to provide

the SecEA update to the community. I do want to echo everybody's congratulations, to Greg. It has been a great partnership with you. I've known you for many years and you've been great to work with and wish you lots of good luck in your retirement. And, to echo Heather. It has been great the past few years, collaborating with NISPPAC. We know that sharing information with them has been quite helpful in shaping policy for the Trusted Workforce. We are in this together and we continue to work together on our journey. So, I also like to take the opportunity to update you on SecEA policies and some trusted workforce things that have been issued.

So really since the last time we met in, I think October, a few things have been signed, real signature accomplishments. We had a transforming federal personnel vetting cabinet memorandum. It was signed by the National Security Advisor, Jake Sullivan. So, it's really the Biden Administration's endorsement for us to take bold action across the government to transform and sustain a trusted federal workforce. So, the guidance in this memorandum asked departments and agencies to prioritize and implement trusted workforce. It also asked agencies to designate senior implementation officials who will be accountable for the trusted workforce implementation and ensure all the related efforts at their agencies are conducted and of course successful. So that was wonderful. This was signed December 14th, 2021.

So also just recently, we're pleased to announce that we issued three high level guideline documents. So, these guideline documents were signed jointly from the ODNI Security Executive Agent and OPM as the Suitability and Credentialing Agent. And these three guidelines really describe the outcomes for successful personnel vetting programs.

And they align with the principles found in the Federal Personnel Vetting Core Doctrine that was effective February of 2021. So, as we go through all these other documents and policy levels, they all build upon each other. So just to describe a little bit about the personnel vetting guidelines, it will be the outcomes associated with investigations, adjudications, and personnel vetting management activities. It's essential for these components to work together in your personnel vetting programs to help identify and manage human risk, to ensure Trusted Workforce. We also issued the Federal Personnel Vetting Performance Management Guidelines. And this will be the overarching strategic direction for conducting performance management. We want to measure; we want to make sure we're doing things effectively and efficiently. And from that, we will put out additional standards and strategies and targets for the community. But that will be coming down the road.

And we also issued the Federal Personnel Vetting Engagement Guidelines. This is the outline approach of engagement, which is designed to foster trust in the process. We want to allow the government and help the individuals to enter into the workforce in a timely manner and help shape a culture of personal accountability and responsibility. So, from these three guidelines that were

issued this past February. On February 10th, 2022, we will be coming out with new investigative standards. And I'm sure you're going to be hearing more about it from Matt Eanes and my boss, Mark B. Frownfelter about the new vetting scenarios. But we will be changing the current investigative model. And those investigative standards will be issued very shortly, and then we will come out with additional implementation guidance.

So as a result of all the tremendous effort of collaboration and coordination across the IC and with the NISP community, the executive branch and industry partners, we know we're all working together in the same direction for successful outcomes and also to improve transparency in our process and have a shared responsibility. So, I also want to just note that two other policies, one is in place right now. It's called SEAD 9. It's not in place. I'm sorry, it's draft, it's the whistleblower protection appellate review of retaliation regarding security clearance. So, we should go out to the community, and it was just with OMB, Office of Management and Budget for formal coordination. So, we're just finishing up coordination and adjudication on that. So also thank you to those agencies that helped provide us some comments.

One other area to explain, and I know there's been some information out there already, and it's shared with our NISP community is the clarifying guidance on marijuana. It's for agencies to use this guidance to help them in adjudication. And the memo outlines adjudicative guidance on the recency of recreationally use of marijuana, the use of CBD products and the investments of marijuana related businesses. So, a lot of good information is in this memorandum, it was signed and issued by the Security Executive Agent on December 21st, 2021. So hopefully you all have seen that. And I also want to thank Keith and his team and DCSA. We know you all are working really hard with the implementation of SEAD 3. A lot of great work is done on the toolkit and resources available for the community for implementing SEAD 3. So, I think that's all I have to update you on. It was just a high level, letting you know what was issued and you will be hearing more later. But if there are any questions, I'd be happy to answer them.

Mark B.: Okay. Thank you, Valerie. That was very informative. Up next is Mr. Rich De Jausserand, Deputy Director of the National Security Services Division at the Department of Homeland Security for their update. Rich, over to you.

Richard De Jausserand: Good morning, everyone. Thank you. First of all, we've been asked to comment on a few items here, some updates regarding NISPOM implementation. I'm sure most of you know, but some may not be aware that DHS and DOD have a special security agreement. We work in tandem with DOD, DCSA. Our industrial security branch continues to work with DCSA and their personnel security teams on the implementation of the NISPOM Rule. We have not had any issues to date.

Regarding COVID. During the pandemic, 70% of the DHS workforce continued to work. And on March 27th, the rest of the staff began a modified return to work

schedule. That 30% is mostly on a telework hybrid coming into the office once to twice a week. So that's where we are as of today. Regarding CUI. Although CUI has not been adopted, our information security branch continues to participate in the NARA working groups and is working with the intelligence community to plan for implementation once CUI is officially adopted.

Trusted Workforce 2.0. DHS continues the implementation of Trusted Workforce 2.0. To date, DHS has enrolled about 83% of our security population into the ODNI continuous evaluation system and we are on track for full implementation by FY24. And there was also, Heather had asked us to speak a little bit about our insider threat. Our insider threat and personal security teams continue to work together to develop policy and SOPs. They are meeting once a month to collaborate with each other, so we are on track for that as well. That's all I really have. If there are any questions regarding any of these updates, please submit them and we will provide inputs through answers to you as soon as we receive those. So, if there's nothing else, that's all I have. Thank you.

Mark B.: Thank you, Rich. Next update we'll hear from Natasha Sumter, Director, Office of Security and Erick Person, office of the Insider Threat Program, both the Department of Energy. Please take it away.

Natasha Sumter: Good morning. And thank you, Mr. Chair. Yes, my name is Natasha Sumter, and I do work in the office of security policy at the Department of Energy. And I'm joined today by Mr. Paul Dufresne, who is a part of our departmental personnel security office, as well as Mr. Erick Person who will provide the insider threat update.

So, to begin, thank you so much for allowing us to be a part of the discussion today. We absolutely appreciate the partnership and engagement that we have with our industry and government partners within the NISP. So, thank you. And to Greg, thank you so much for your service. We appreciate your leadership with the NISPPAC. We look forward to seeing you in your cities and your umbrella drinks sitting on the beach somewhere. So best to you in your retirement.

So today I'm going to give you just a couple of updates from a DOE departmental perspective. So of course, we always have a lot of things going on as a self-regulatory organization. We are constantly reviewing national drivers and security postures of our other organizations, but also of course, within our own department, just to ensure that we are aligning with those security policies that have been recently published, updated, et cetera, and to ensure that we are doing the things or exercising those requirements and implementing those practices that make sense for our mission and the security assets that we have within our organization.

And to that effort, we have been reviewing yearly order 470.4B, which is the Safeguards and Security Program order, which handles or discusses a lot of the

industrial security matters that you would see in the NISPOM or the 32 CFR 2004. So, we are currently beginning the process to open that order for a complete rewrite. Yes, I said it. a complete rewrite. We are going to review everything that has ever been issued concerning industrial security matters and ensure that we're doing the right thing, not just for the department and our security assets, but also for our stakeholders and our partners within the NISP.

So, regarding the updates that we have been asked to provide, specifically CUI, we have reviewed the national driver the 32 CFR 2002, and we have implemented that regulation via DOE Order 471.7, which is Controlled Unclassified Information, which was published on February 3rd of this year. And of course, whenever we update our policies, we always collaborate and engage both our industry partners, and our federal employees and SMEs throughout the department and even across agency lines. So just so everyone understands the construct of DOE. DOE is a very decentralized organization. So, we have all these different program offices that implement the national drivers, the departmental requirements, et cetera. But whenever there is a requirement that applies to our contractors, those are conveyed through what is called a Contractor Requirements Document.

And regarding the 471.7, the CUI order, it does have a Contractor Requirements Document that conveys those requirements to our contractors, which will eventually be updated in the updated contract, but also issued with the new contracts that are provided to our contractors. So, we were asked a few questions concerning CUI implementation or CUI within the department. And one of the questions was regarding oversight from a CSA perspective. Another question was asking about the reporting requirements and mechanisms, but also to clarify the definition of the term of unauthorized disclosure. So, from an oversight perspective, as I mentioned, we do have the order that is currently in place. But also, we have other governing documents, including DOE policy 226.2, which is the Policy for Federal Oversight and Contractor Assurances and DOE Order 226.1 B, which is Implementation of Department of Energy Oversight Policy. Those documents provide the oversight structure for both our federal operations and our contractor assurances. And while those documents are published, we do keep them updated and maintained as well.

So, we have an Office of Independent Assessments, which provides our oversight activities as well. So, they do not have any line management or policy making responsibilities or authorities. However, they do provide the oversight of those requirements that are published in the various security related orders for the department. So, our federal and contractor operations are an integral part of DOE's assurances for our safety and our security programs. And we ensure those documents are updated, we ensure that those assessments are completed or conducted within a timely manner because we have to provide those assurances to not just our senior leadership within the organization, our workers, but also to the public and of course you, our contractor partners. So, through these independent oversight programs, we enhance our safety and

security programs by identifying any concerns or issues that may have arisen during an assessment, but also providing corrective actions and a way forward to addressing or mitigating those issues. And that is also included in our CUI order.

So, another question that we were asked to address was what the reporting mechanisms for industry issues are, lack of Marking, handling guidance, et cetera, to our customers. So, DOE Order 471.7 contains those reporting requirements to the site and program office oversight officials. And in addition to that, we have other reporting requirements to the Office of the Inspector General and other requirements that align under the order that I mentioned earlier, which is the 470.4B, which is respectively my order. That's the one that I'm responsible for updating. And that order has an Incidents of Security Concern program that is leveraged to identify various issues to include, which will include CUI reporting requirements, et cetera.

And finally, we were asked to provide some feedback on how we define unauthorized disclosure. So, 32 CFR 2002 section four actually has a definition. And the Department of Energy leverages that language to define what it actually means to the department. So, the unauthorized disclosure occurs when an authorized holder of CUI intentionally or unintentionally discloses CUI without any lawful government purpose in violation of restrictions imposed by safeguarding or dissemination controls, but on the contrary to limited dissemination controls as well.

So, with that said, that is the updates on what's happening in some of our policy worlds, because there's always something going on, but also just to provide some responses to the questions that were posed regarding CUI. And you'll later hear updates from Erich Person regarding the Insider Threat Program and also Mr. Paul Dufresne from our departmental personnel security offices. And barring any additional questions, I will turn it back over to you, Mr. Chairman.

Mark B.: All right. Any questions for Ms. Sumter? All right. Next, we'll hear from Mr. Chris Heilig, Chief of the Personnel Security Branch giving the Nuclear Regulatory Commission update. Chris.

Chris: Good morning.

Mark B.: Good morning.

Chris: I'm the speaker at the end for the Clearance Working Group.

Mark B.: Yes.

Dennis Brady: Mr. Chair, this is Dennis Brady. I've got something prepared for the NRC.

Mark B.: Okay. Dennis, please.

Dennis: Thank you. Good morning, everybody. Thank you, Mr. Chair.

Mark B.: You're welcome.

Dennis: I'm just going to cover where we are with the COVID return to work. Because the NRC has returned to work in a hybrid work environment, with most of the staff in the office a minimum of two days a week. That means on any given day, the number of staff physically in our NRC facilities is just over half of what it was prior to COVID-19.

Dennis: The agency currently doesn't have any plans to change from this COVID work, or the hybrid work environment. It seems to be working very well with the staff, we're able to achieve our mission in providing oversight to the nuclear industry.

For the CUI program, we are on track, NRC has their policy statement published and the rule has been approved by our commission that supports the NRCs transition to CUI in September of 2022. But the NRC operates internally under management directives, as DOE uses the rule. We have our management directive in place, training has been all established, and it supports both the NRC employees and contractor communities.

Under SEAD 3, our foreign travel report approval tool has been published and is active for cleared employees, and a large portion of our cleared contractor population. The remaining contractor population which is our cleared licensees will be captured under that program later this year. That was the last element of the SEAD 3 requirements that we had to implement, so by the end of this summer, we'll be fully compliant, capturing all the required reporting data, and the agency approved SEAD 3 foreign travel reporting requirements.

That's the end of my report, I don't have any other updates from either insider threat or on the trusted workforce. Thank you.

Mark B.: Thank you Dennis. Anyone have any questions for Dennis? We're next going to turn to Felicia from the Chief, Office of Security policy giving the CIAs update, and then after she talks, we will have a five-minute break. Felicia, the floor is yours.

Felicia: Good morning. Thank you for this opportunity, Mr. Chairman. Also, we would like to also echo what everyone else has been saying about Greg. We want to wish you all the best in your retirement, and we want to thank you for all that you have done for NISPPAC and for your engagement with industry, as well as with the government. And so, today I will be making brief statements on behalf of the agency, in reference to the NISPOM implementation, as well as controlled unclassified information, and then we will give a brief statement on trusted workforce. After that time, if you have any additional questions, we ask that you submit those questions through the proper protocol, or as instructed at the beginning of this forum.

So, in reference to NISPPAC implementation, the CIA industries securities staff is actively engaging in the implementation of the new NISPOM as a federal rule. We're working closely with our procurement executive to have our contract security clauses amended to reflect the new guidance. We are also hosting a series of industrial workshops designed for company security officers, and the information will be discussed at these upcoming events. As far as guidance regarding the SEAD 4 updates, we are incorporating that information into our current policy, and the SEAD 4 as you know is the national security adjudicative guidelines. Regarding controlled unclassified information, we're working closely with the ODNI, our representatives, once they issue policy guidance, we will begin that implementation.

Trusted workforce 2.0. We are continually actively participating in multiple government-led working groups focused on providing substantive comments and review of Trusted Workforce 2.0 draft policy. And in those discussions of agency and government-wide capabilities in achieving future trusted workforce requirements. Our focus at present is in achieving the early 2.0 milestone of full enrollment of agency members in our continuous evaluation program by the 30th of September of 2022, as required in the January 2021 executive agent memorandum. As we wait on issuance of accompanying standards which will define requirements to an operational level, we remain focused on review and comparison of current vetting processes against the draft 2.0 future standards. So, we might plan and project any agency shifts in technology, resources, and processes, by the deadline of 2024.

We remain mindful that ensuring a trusted workforce within the CIA and throughout the government requires that we all maintain strong and sustaining relationships with our industry partners. As we gain additional operational level details in the soon to be released policy, which will tie us to our industry partners, we will begin a series of conversations to ensure that we will work together to achieve these requirements. We want to thank you for this opportunity and your attentiveness. That's all from us, from the CIA.

Mark B.: Thank you so much. Does anyone have any questions for Felicia? I hear none. We're going to take a five-minute break. I've got on my watch here, 11:16, so we get back in five minutes, we'll next hear from Bob Mason.

Moderator: Please you don't have to leave the room because we're going to have to start immediately.

Mark B.: Okay. So, a five-minute break will begin now.

Moderator: We can get started.

Mark B.: Okay. Welcome back everybody, up next is Bob Mason, alarm system auditor and UL 2050 subject matter expert with Underwriters Laboratory LLC. Bob, yours.

Speaker 2: Please take your seat.

Bob Mason: Thank you very much Mr. Chair. Thank you for this opportunity for UL to speak during this event, where I'll be talking about the national industrial securities systems standard, UL 2050. It's the fifth edition. We'll be talking about four types of monitoring, the first monitoring of the standard is chapter six, it's government contracting monitoring stations, it's a government contractor location that has the ability to monitor UL 2050 certificates within a 240, four-hour radius from that location. The alarm service company that issues the certificate also has to maintain the receiving equipment at the monitoring station. So, it couldn't ABC Alarm Inc maintain the equipment and not write the certificates like CBA Inc is writing the certificate. So, it has to be the same alarm company that issues the certificate, also maintains the equipment for the receiving equipment, and for a government contracting monitoring station.

And the government contracting monitoring station is maintained by the alarm service company, so they verify compliance for the physical construction of the monitoring station, and they also maintain the alarm receiving equipment, verify fire protection, make sure there are clocks in place, primary and secondary power, communication circuits, and personnel. Those are the key fundamentals of the GCMS. This government contracting monitoring station also is required to monitor the alarms that opens and close. It's all the alarms in unauthorized openings, dispatching investigators, trouble signals and service calls, and creation of records.

A government contracting monitoring station is not able to monitor any UL certificated outside of the four-hour 240-mile radius of the station. A national monitoring industrial station, however, is able to monitor outside those 240 miles and four-hour radius from the station. They are also UL listed for CRZM. So, UL does go out and verify compliance on an annual basis at these stations to make sure that for the fundamentals of the monitoring station, so physical protection, alarm receiving equipment, fire protection, clocks, primary and secondary power, communication circuits, and personnel. These facilities and these monitoring stations are also required to monitor all the alarm systems, openings and closings, alarms in unauthorized openings, dispatching investigators, trouble signals and service calls, and creation of records.

And then the third option for monitoring these types of certificates is a central station, a commercial UL listed central station. They can be listed for a UUFX for fire, a CPVX for burglar alarm, or CVXU for residential monitoring. The commercial UL central stations follow a UL 827 standard. They are also required to monitor the alarm systems, opens, and closes, alarms in unauthorized openings, dispatching investigators, trouble signals and service calls, creation of records. They're also required to monitor the physical, UL also verifies compliance with the central stations on an annual basis for the category. So, these central stations also have to have a DD254 in place for clear operators up to the secret level.

Then the fourth type of monitoring is law enforcement. Law enforcement is not able to monitor opens and closes, they only can monitor alarms and troubles. Law enforcement also, any time using law enforcement is required prior approval on the alarm system description form for NISPOM. And again, I've only seen one, and that was 10 years ago, I'm not sure of the one that's being operated on as of right now. But those are the four types of monitoring, and if I get invited again to speak at another event in the future, I'd like to talk about the four types of investigating.

The other thing I'd like to also talk about is the two proposals that were sent out a couple of years ago, one is automation systems. Automation systems to bring into the new UL 2056 edition. I haven't done this, but these are just proposals that I'm waiting for approval on by the government. This is for redundancy for chapter six, government contracting monitoring station, and national industrial monitoring station, which is chapter seven on the UL 2050 currently. This would allow, like I said, redundancy for any equipment for failure, the intent of the additional paragraphs was monitoring stations to equip with redundancy, and this will assure if at any time the computer system were to fail, there is a backup system that will automatically be in place to continue processing of signals. Not only for the automation system, but also the communication circuits, whereas internet service providers, on having two internet service providers rather than just one, that way if one of the service providers goes down, it would automatically switch over to the secondary internet service provider, or our, even MFVN, two different MFVNs or a combination of one or the other.

So, that's what I had today. I heard that we were kind of stuck with time, so I was trying to do this as quickly as possible, but as clear as possible as well. But that was my presentation. And again, thank you for this opportunity.

Mark B.: You're most welcome Bob. Does anybody have any questions for Bob? Okay, thank you Bob. We will now hear from the general services administration's chief of policy standards and engineering branch, Mr. Chris Pollock, who will go over the safe ordering process for industry. Chris.

Chris: Thank you Mr. Chairman, and a thank you to ISOO for giving me the opportunity to give a quick update on the GSA safe ordering process for the storage containers and vault doors used to protect classified information.

In the interest of time, I'm going to just hit a couple of highlights of the presentation rather than go through it step by step. So, can we skip to slide number four real quickly? There you go. So, this is sort of the synopsis of the procurement requirements. First of all, you have to have the requirement to store classified information within your contract, usually that's in a DD254, some other government agencies do use other forms, but primarily that's in the DD254. You also have to have an activity address code, or the associated DoDAAC. These DoDAACs or activity address codes are assigned by your government contracting officer, and this is probably the biggest sticking point in

placing an order through GSA for the containers. So, it's important that you maintain good communication with your contracting officer, to make sure you've got your DoDAAC assigned, and that you're using the appropriate one.

Again, you must have the ability to pay, which is kind of self-explanatory. We do allow payment in all kinds of different methods, including PayPal, and their connections to bank accounts, or different types of credit cards. And this process goes through, this presentation goes through both the online and offline ordering of GSA containers. Primarily for this audience, that would be the offline process, which includes going out of the DD, the form 1348.

Just one more quick comment, it's about the process, then I'll address a couple of other specific questions. But through COVID, we found that it is absolutely critical that when you're placing an order, you mark a section to provide a good point of contact. Throughout COVID with different rules regarding building opening and handling of material, and the whole process potentially getting changed, it's critical that we have a point, that our manufacturers have a point of contact to be able to work through any issues that arise.

So again, that's real quick. Again, these slides will be presented, go through it in pretty good detail. But if you have any questions regarding the process, send them to nisppac@nara.gov, happy to address any questions. We do have a couple of questions regarding some specific issues, first of those is the cost of GSA approved containers. I'm kind of probably preaching to the choir a little bit here talking to the industry partners, but we have seen some unprecedented changes in the cost of steel over the last couple of years, depending on which index you look at, the cost of steel is up about 200% since March of 2020. We've also been affected by the shortage of electronic components, that's caused some redesign and retesting, and additional cost for our lock. Overall, this has resulted in about a 30 to 40% increase in the cost of our GSA approved containers. Yeah, not where we want to be in, we're keeping track of those indicators to see if at some point in the future we can reduce the cost, but right now we're looking at again, a 30 to 40% increase over the last two years of the cost.

Delivery, yes. During COVID, delivery was affected for sure. Our manufacturers had the same issues that most of the rest of the world had regarding staffing shortages, particularly welders, machinists, painters. GSA tries to maintain a 30-to-45-day delivery time, that's what is in our contracts. During COVID, that time slipped sometimes as far as 90 days, but we were working to get back to the 30 to 45 days. Most of our manufacturers are meeting that on a pretty consistent basis, but yes, some of the deliveries over the last couple of years have been delayed.

The final comment I have is with regard to ISOO notice 2021-01, which is the removal of the black label on all the containers from service. I understand that there's been quite a little bit of confusion regarding trying to identify the

containers, and they need to be replaced. The best place, the best resource to find out information about that is the DOD lock program technical support hotline, that's available to both DOD government, and industry as a resource. And I would ask ISOO if they could include the webpage and the information for the DOD lock program in the minutes to the meeting. And that's all I have. Back to you Mr. Chairman.

Mark B.: Oh, you're most welcome Chris. All right, now moving into the portion of the meeting where we get reports from the NISPPAC working groups, however, we will not be discussing all of them. We have provided slides with highlights of them all. We will only be discussing clearance and NISP information system authorization, also known as NISA working groups at this time. Greg, if you would take that part away, I'd appreciate it.

Greg: Thank you Mark B. And for those of you who don't know, we've had these two working groups, the NISA and the clearance working groups. These have been standing working groups for probably 15 years. I believe it was Tom Langer and another industry rep who I cannot recall, who came to ISOO at the time when the clearance processing was off the charts. And similar issues with the information system's authorizations. And it was right around the time where I think IRPTA was coming out too, as far as timeline requirements. And anyway, I think we made a lot of progress by putting focus on it, and we've continued to have these groups, and there's been some ebb and flow. I think right now we're in a pretty good state with the timeliness at least in the personal security clearances.

So, our working group, the clearance working group, we generally made at least once between NISPPAC meetings, and some of the things you've already heard have been discussed at those meetings. One thing I don't think we've mentioned is the SF 312 nondisclosure agreement. One of the things coming out of COVID that we heard from a few agencies was, there's the requirement to have a wet signature on the form, and that was delivered to the Department of Justice when we updated, or the initial regulation for the EO 13526 32 CFR part 2001, they wanted that in there for legal purposes. Anyway, technology has advanced, we have meaningful ways using cryptography technology to enable the use of a digital signature. We coordinated with ODNI who essentially owns the form, as well as the Department of Justice, and I'm pleased to say that effective May 9th, the directive language will be affected. It's been amended, and it will allow for the use of a digital signature as long as you're using cryptography technology that in a meaningful way can ensure authenticity.

That said, what we're referring to is either the use of the CAC card, or the PIV card, along with a pin number. So, government- issued cards, those two cards for now. And if an agency can demonstrate another card, then that's fine too. And the wording of the directive, it's left up to the agency if they want to deploy this. Now we'll say, we'll be putting out an ISOO notice on or about May 9th, the effective date, simply because unfortunately, it will not actually be able to be

operationalized in all likelihood of that date, because ODNI has informed us it's very unlikely they will have the changes to the form made. There are some changes obviously needed, because with a digital signature, you'll no longer need a witness, for example. So, anyway, some progress there.

Let's see, a couple of other things. I mentioned in the past, ISOO, we've been undergoing reform in the way we collect data. We collect a lot of data, it's true, to the point that sometimes agencies complain a little bit, because we have so many reporting requirements. We do after all have to report annually to the president each year, so we're not just making this stuff up ourselves, there's requirements that we have by way of executive order to do this.

Anyway, through that process, one of the things we've been looking at besides the overall data reform initiative for collecting information, is cost. And as it relates to NISP, there are requirements in the two executive orders, one for the NISP and one for the CNSI classified program, that concern cost, and these requirements cascade down into the directives, the applicable directives. So, we've been meeting just the government only, to discuss a way forward to get better estimates of the cost of entities under the NISP, ICSA, that cost to implement the NISP. So, in other words, if we didn't have a NISP, those costs wouldn't exist because those requirements wouldn't exist.

So, we are at a point where the DOD, our colleagues at DOD, put forward an outline that captures both the major buckets of cost and does it in a way we believe that will impact industry the least. So, we're coordinating that with the other CSAs and we're planning to meet next week. And just to give you a little flavor of what we're talking about in terms of the buckets. Security-wise, every entity has to have a facility security officer, depending on your facility, you have ISSMs and other individuals that document custodians and what have you. There are obviously vendors, the investigations, there's the adjudications, and continuous vetting. And these are things that we think, we the government, will share this with industry once it's ready to be shared. We can get this data without really bothering you. We should be able to get that on our own.

And there's a few other things we're looking at, information systems technology that process classified information, what additional costs are there because you're processing classified information. Perhaps physical security aspects, and then training, right? I think the training, we can also get on our own by using some extrapolation of the number of cleared people, times X amount of hours per year, times a rough dollar figure per hour of salary pay, to get to those things. So, we're hopeful to get that and that will give us some better estimate of the cost on the in, and I know there are some debates about ultimately government's paying for it, but the way the wording and the directive and the orders are written, it should give us a better way to come up with estimated cost to implement the requirements, the main requirements of having a NISP. So that's a good thing.

Another thing, I'm not sure if Heather brought it up, but during our clearance working group, it was discussed and I've heard it in other forums, like the DCSA stakeholders meeting for industry. Let's be honest, apparently from what I'm hearing, we have a concern right now with the processing times for facility security clearances, and the rejection rate as well. So, what I'm recommending, we've done this before with other parts of the program, is to form a small ad hoc working group, and I'm asking this of our chair, to focus on what are the issues? What are the major impediments that are causing this rejection rate? We can analyze this hopefully rather quickly, study it, see what's going on. Is it the FOCI aspects of clearing the entity or what other aspects are going on there? So, I'm hoping that we can do that.

I'm going to stop right there and if there's any questions from NISPPAC members, I can take them.

Heather: Hey Greg, Heather from the industry. I have a couple of questions just to go back. You talked about how funding the NISP is inherently a government responsibility. Many of us are aware that there's a lot of unfunded requirements that come out and so that's why it's ever more important to understand when the five CSAs or anybody that touches industry understands when you add a requirement that is not policy or contractually required, that it's so important to consider that industry is paying out of pocket sometimes for those. But I need to remind industry, if we do get an unfunded requirement or a new process change after the contract has been awarded, you can go back to your government customer and renegotiate that contract. It's very important to make sure that the company is not eating all those costs.

And I'm going to take it back to the JPAS and DISS transition and to NBIS transition. Industry did eat a lot of that money and resources when we corrected that data. So, it's very important to make sure something that very minute, really adds to the cost of doing business with the government in this space. So, it's very important to make sure we do that.

But getting back also to the facility clearance process, you talked about having that small group, the ad hoc group to work on the improvements of the process, the 60% rejection rate but also the IT portion of that where if you have a simple change to make, you have to start that process all over again, also adds to the time of trying to get somebody sponsored. But I'll also add that without a good foundation in that facility clearance entity vetting process with the 845 or 847 coming forward, we want to assurance from the industry's perspective, is that going to be the same body at DCSA doing the same process that's going to be doing the FCL and FOCI vetting process, because if it is, we need to ensure that DCSA has the resources to properly do that because otherwise in industry, we're going to see some supply chain issues with bringing in subcontractors to do some of our contract needs. Thank you.

Greg: Well, if there's no other questions, I think the way we've got this set up is DCSA is going to provide some system metrics next and followed by DOE and NRC.

Mark B.: Yes, that's right, Greg. We're going to hear now from David Scott with DCSA for DCSA's information systems update. David?

David Scott: Yes. Thank you. Since the last NISPPAC, I gave a brief update. We've realigned regions from an AO perspective. I wanted to announce the AOs and which region they align to. Mid-Atlantic region is Mr. Ezekiel Marshall, formerly the capital region. In the Eastern region, we have a brand-new AO that's come on board since the last NISPPAC, Alexander Hubert. In the Central region, William Vaughn, and the Western region, Stacy Omo. Those are your regional AOs that if industry has questions or concerns to work through the regions all the way up to NAO as needed.

Next slide. I just want to really just kind of explain our partnership with the NISA working group. It has been very instrumental working through some major challenges over the last few months where industry has requested more insight into metrics. And in December we had a process DCSA could change a workflow, package workflow. Due to our strong relationship with NISA working group, we were able to collaborate, communicate effectively to make a change in January. That was, I think, monumental. And that change happened in January with zero downtime and industry was fully engaged. And it really is already starting to prove positive value because industry has now direct insight to where their package is throughout the assessment and authorization process. So, we've heard nothing but positive impacts there. And we're looking to build upon that on many other enhancements within eMASS for industry and for us internally. Currently, we're still going to be trending and baselining our metrics. And at the next NISPPAC I'll be able to provide more insight to include DCSA time.

One kind of late thing that I'd like to bring up to the community here is we've had some concerns with access to eMASS computer-based training which is now hosted in the RMF knowledge service. And there's been access issues from the industry. Just want to report that we have been working with DISA, and we've recently got approval to host in the step environment from CDSE. And we are actually working on that right now. And as soon as we get approval to hit the live system, we will work with the NISA working group to publicize that.

Next slide please. Another positive engagement that I'm happy to report is with the NISP connection process guide. This guide is instrumental in providing a hands-on process flow for any contractual requirement to interconnect with a system within the NISP. This is something that I think is much needed. And due to the collaboration with the NISA working group, we received a lot of feedback over the course of the last three months. And now we are looking to formally publish that through the processes of the federal registry. So that is where we're at with that. We've moved forward with the NISA working group, and we're looking forward to coordination there.

And then lastly, where are we going next from an NAO perspective? We're going to continue eMASS updates and job aids, and we're going to utilize eMASS as their help desk page to put information out to industry as fast as possible to all 4,000 users. So please pay attention to eMASS and that front page for any guidance job aids to really make the job easier. We're also working internally right now on an update overall to DAAPM 3.0, and we're going to partner with the NISA working group for that as well to really close up any gaps in processes and procedures that industry sees and that we also see.

And then lastly, Command Cyber Readiness Inspections, the last report that I provided at the NISPPAC that we were planning to go out and start executing CCRIs. We've actually already executed one, and we're already planning for the rest of the FY to conduct many more. And then also our FY 23 planning for our approved SIPRNet node. And we're going to continue to partner with the NISA working group as our primary working group for information exchange and collaboration to approve our process and procedures. And that's all I've got pending questions. Thank you.

Mark B.: Thank you, David. We're now going to hear from Donna McLeod with DCSA for their vetting statistics.

Donna McLeod: Thank you. Thank you. This is Donna McLeod from the background investigation program, and today I will be providing the metrics for personnel security with DCSA. And that will include the vetting risk operations, VRO, of background investigations and adjudication. So, to start with VRO, vetting risk operations, the investigation submission and interim industry populations are approximately a million. And that's why 22 investigations request submissions of about 100,000. 90% of all initial investigations have an interim determination made on average within five to seven days.

Please remember to submit your fingerprints for initial clearance prior to submitting an investigation request. We cannot open an investigation or issue an interim determination without required fingerprint results. And FY 22, we triaged approximately 8,000 incident reports. Under the continued vetting, DCSA is responsible for implementation of DoD CV program. Currently approximately 975,000 industry subjects are currently enrolled in CV and with 156,000 PRs deferred to date.

As of January 22, all PR submitted to VRO will be deferred into CV. We reached full enrollment of DoD clear population into a trusted workforce CV compliance program in FY 21. And we continue to work the set to a steady stay of new enrollments moving forward for our CV alert management, post CV enrollment alerts are generated based on established threshold, which aligns with federal investigative standards and adjudicated guidelines. Currently we average approximately 6000 PR’s and a 6% alert rate. Criminal and financial are the most common valid actionable alerts that we receive. And FY 22, we received 19,000

industry alerts of which 8,000 were not previously known information, which would be placed to 41%.

Onto the background investigation. Our total inventory for background investigation continues to remain within a stable state. Q2 started and ended at approximately 171,000 cases, and we fluctuated between 166 to174 throughout the quarter, with the current level also is at 171,000 cases. For industry cases in Q2 that we have into 27.6 thousand cases one which represents a 1.5 thousand decrease from our Q2 start and currently 26,000 cases. Much of this decrease is due to the PR decrease numbers that are coming in. And Q2 industry announced that they will no longer be submitting PR investigations and have shifted towards the continuous vetting.

Prior to Q2, we received 8 to 10 thousand industry PRs for quota and during Q2 we received just 600 cases. So, you can see the decrease. In regard to the CI timelines for industry, remember, these metrics are based on end to end, meaning the cases that have gone all the way through the process to adjudication for that particular quarter. So, FY 22 for Q2 our T5 end to end time limit is at 155 days, that is 30 days for initiation, 108 days for investigation, and 17 days for adjudication. T3 initial for the same time period and the end time limit is shown at 117 days, 32 days for initiation, 68 days for investigation, and 17 days for adjudication.

This is a big improvement over where we were two years ago. When we look at the T5 end to end time limit numbers, we were at 221 days, and then our T3 end to end time limits were at 132 days. Time limits have been trending upward due to multiple reasons within the organization. We have increased processing time for our security and suitability in investigation index files, known as our SII files. Analysis was conducted, and it shows a direct correlation between this and increase in time limits particular to T5. Additional staff has been assigned to continue working down the inventory of the SII files. We also experienced a valid printer issue in our biggest facility-

Donna: ... which resulted in 150,000 vouchers being delayed on over 41,000 cases. And it was largely impacting the SEAD 3-time limits. COVID impacts to the background investigation. COVID restrictions beginning to ease across the country were likely to experience a reduction in the number of cases that are being held due to COVID. In the past eight weeks, our COVID health cases have dropped by 85% and now stands at only 420 cases, but the investigative clock has not stopped due to COVID, and it does impact the investigative time limits. Over the past two years, DCSA employees have adapted and remained flexible and demonstrated agility to continue meeting mission requirements. Since last summer, we successively sustained operations through significant surges due to COVID and constantly adapting to close all COVID impacted cases as quickly as possible.

Onto our adjudication program. As a whole adjudication meeting time limits goals except by the Congress office of management and budget and the director of national intelligence. To our industry adjudication portfolio, we are largely meeting timeliness goals with a few exceptions. In FY 22 Q2, our initial adjudication timeliness was 17 days for T3 and tier five investigations, and 33 and 28 days for T3R and T5R respectively. We are forecasting initial adjudicative timeliness to remain in compliance with congressional mandates. For periodic re-investigations we expect timeliness performance to continue to remain close to or above OMB's target of 30 day.

Adjudications completed over 95.2 thousand in national security adjudications, which include incident reports, customer service requests, continuous vetting products comprising more than half of the denial and revocation information sources. The top three reasons personnel are being denied or revoked remain financial considerations, criminal conduct, and personal conduct. Coupled with meeting timeliness requirements, adjudications continue to execute national security adjudication decisions with high level quality, delivering 100% appropriate determination rate in all adjudication in support of our customers.

Our current industry inventory is at 19.4 and it comprised customer service requests, incident reports, tiered investigations, and continued running alerts. The industry inventory has been relatively steady for the last four quarters, and we closed approximately 94,000 cases this year. On behalf of the personal security mission space for DCSA, thanks again for your partnership as we move forward and for trusted workforce transformation initiatives. We remain focused on preparing for the NBIS and trusted workforce implementation. To this end, we are working collaboratively with our partners in NBIS customer agencies, our industry partners, to continually improve our focus on our customer service and support operational needs. And that concludes my part of the overview.

Mark B.: Thank you, Donna. Next, we are going to hear from Paul Dufresne, Personnel Security Field Assistance Program Manager, Department of Energy, to give us his metrics. Paul?

Paul Dufresne: Good day, everybody. Thank you for the opportunity to provide you with this information. As you can see over a quarterly trend, the department of energy has been meeting the 20-day standard for the adjudications on initial investigations, as well as the 30 days on the standard for, excuse me, for the re-investigations. On the next slide, you'll see where we started out on a monthly trend for the top-secret investigations, the T5s, where we weren't meeting the adjudication timelines. However, averaging out over the 12-month time period you're looking at an average of about 17 days total.

And I'm going through this rather quickly because it's just to keep everybody on track here. For the tier three investigations, it's the same thing. We started out roughly just over the IRTPA standard. But since then, we've actually over the last

12 months been meeting the IRTPA. And for the T5R investigations, we did see an influx of investigations come in during the early part of the FY. However, we continue to maintain meeting the OMB standard for re-investigation adjudications, and the same thing with the T5 investigations we did meet it through... or excuse me, T3 investigations, we did meet it throughout the entire fiscal year.

What I'd like to do is also give a quick update on what we're doing for trusted workforce implementation. We have our order, the DOE order 472.2 is sitting with the deputy secretary right now for approval and signature. We had plenty of representation across the department to include our industrial partners that were involved in this process. And we wanted to thank everybody for that. Since we last met, the department has actually begun deferment of periodic reinvestigations. We're working with our internal IT people, as well as DCSA to get our wrap back implementation rolling. And with the help of our trusted workforce working group, we have wide representation across the department so that we continue to try to meet all the milestones, and everything being put out by the executive agents so that we can actually, once we get our entire clear population into the trusted workforce 1.5 state, we can actually start working on the uncleared population, the T1 to T4 population.

But we're looking forward to being able to move forward with that. But we're right now at a 1.25 state, and we're looking to be 1.5 compliant by the end of the FY, hitting that milestone of September 30th. With that, I'd like to go ahead and turn my time over to Eric Person from the office of insider threat program here at DOE.

Erich Person: Thanks, Paul. Appreciate it. Good afternoon, Mr. Chairman. Again, as Paul, my colleagues said, I'm Erich Person, Department of Energy, and specifically with the office of insider threat program. Before I begin, I'd also like to congratulate Greg on his retirement and thank him for his service. Very quickly just an overview. DOE's office of insider threat program is the support office for the department's program or insider threat program per the direction of what we call our designated senior official or DSO.

Our principal focus is to serve in an organized training, equipped motives, and to ensure among other things or among other items that the department's insider threat program is consistent with national insider threat policy and minimum standards, as well as concomitant with national directives and DOE requirements. Also, I should add that transparency and prudent information sharing is a principle focus as we pursue the insider threat program mission at our department, the department of energy.

Our office works closely with our DOE security policy and personnel security colleagues. In fact, personnel security or per sec, and physical security representatives are core members of what we call our local insider threat working groups or LIT WIGs. The LIT WIG represents the tip of the spear, if you

will, for the program in the field, that is at the various national laboratories and DOE sites across the country.

Currently our office is pursuing a number of initiatives to advance the department's mission, our insider threat program mission, to include revising the DOE order 470.5, that is the departmental driver, the vehicle that helps us to or enables us to pursue executive order 13587, which of course stood up nationwide insider threat programs at all departments and agencies across the executive branch. So again, we're pursuing that in earnest and looking forward to a positive conclusion and revising that order. Again, it was published in 2014, so it's about eight years old. And so, it's in need of some retooling.

Lastly, our office via DSO guidance and direction maintains a robust outreach effort to our public and private sector colleagues and friends. We certainly understand and appreciate the value in fostering those mission focused relationships. I'll close there and thank you for your time.

Mark B.: You're most welcome. All right, next is Chris Heilig, Chief of Personnel Security branch, Nuclear Regulatory Commission, please provide your update.

Chris: Thank you. So, in the interest of time, I will not go through all the slides one by one, in terms of timeliness numbers. The gist for last quarter was our numbers did slip a little bit. We ran into some problematic cases that took longer than normal or expected, and we had some issues getting a hold of people with the COVID restrictions. But now that everything's reopening, I think our trend will be back to normal and meeting our adjudication times moving forward.

In terms of trusted workforce, we are 1.25 compliant, and working actively with DCSA to meet the 1.5 compliant deadline at the end of this fiscal year. And we don't see any reason why we will not hit the 2.0 deadlines as well. Also, I would just say we're excited to hear about the SF 312 moving towards a digital signature. I think that'll speed up our internal processes quite a bit. And those onboarding with our agency will feel that speed up. That's really all I had. And I'm happy to answer any questions.

Mark B.: Thank you, Chris. Appreciate that. All right. Now we'll hear from Mr. Perry Russell-Hunter from the defense office of hearings and appeals, also known as DOHA. All right, Perry, yours.

Perry: Thank you so much. I really appreciate it. I want to start by recognizing Greg Pannoni's for his over four decades of exemplary public service to the NISP and to the nation. Greg represents the very best of expertise in industrial security and information security and the public in general. So, Greg, I want to thank you because you've improved so many things in your time at ISOO and at the various things that are now called DCSA. I want to join Heather Sims in congratulating DCSA on ongoing improvements to invest and adjudication and their increased focus on quality in both areas. As you all know, DOHA renders final decisions

independent of DCSA, and that independence in hearings appeals and final decisions is very important. But a focus on quality in both the investigation and adjudication increases DOHAS ability to do its job as effectively and efficiently as possible.

So, DOHA is still making maximum use of telework except for the personnel who are conducting and supporting the in-person hearings that are obviously a core part of the DOHA mission. We're fully masked at all times in all hearings. And we employ a full range of safety precautions in those hearings and in the office. So, in these ways we are maximizing safety to all involved in the hearing process and at DOHA. Leveraging telework has not affected DOHA productivity, which is thanks to the great partnership between DOHA and the department of defense consolidated adjudications facility, or DOD CAF.

Statements of reasons or SORs are still going out in typical numbers. And we are timely with 257 statements of reason reviews currently pending. That number is well within the typical on hand SOR review workload. So, while the monthly numbers may vary slightly, we are current and most SOR reviews are completed within the month received. However, at any given time, there may be a smaller group of SORs for which there are requests for additional information, requests for permission to use other agencies' documents, and other good reasons why a serious issue case needs some work.

Just for context, between 2017 and 2019 pre pandemic we reviewed a typical average of 2,600 SORs per year. In fiscal year 2021, DOHA legal reviewed and revised 3021 statements of reasons, which is higher than an average number. And in the calendar year 2021, we reviewed 2,578 SORs. So, DOHA kept up with all the draft SORs sent by the CAF for legal review and worked at a typical operating pace despite the pandemic using DoD safe as a delivery system to ensure a secure workflow.

While the pandemic was impacting the hearing process due to travel and because DOHA was challenges with conventional video teleconferencing, DOHA made good use of the defense communication system or DCS throughout fiscal year 2021 to conduct remote online virtual hearings for clearance holders and clearance applicants in locations where travel would still be unsafe, or which could not be reached using conventional VTC. With the sunset of DCS, DOHA is now holding hearings using Microsoft Teams 365. DOHA has also continued to hold in person hearings throughout the pandemic whenever and wherever possible, and we will continue to do so. And that is the report from DOHA.

Mark B.: Thank you very much, Perry. All right. Up next is Greg Pannoni, Associate Director for the Control Unclassified Information program at ISOO. Greg.

Greg: Okay. Thank you, Mark B. CUI. So just a couple of things, a couple of three things I want to mention. As stated before, ISOO has a lot of reporting requirements, and one of those is CUI implementation. So, we have to report that to the

president as well. And we'll be doing that very soon. Most agencies and departments have begun implementing their CUI programs. As we talked about a little yesterday, yes there are some challenges. And speaking of challenges, I do want to emphasize because I've heard not just in this forum but in other folks will say, "Well, we don't get information as far as the identity of what CUI. We're just told to protect it." There is, just like with the classification program, there's a CUI, I should say, challenge provision. And so we encourage to do it informally, but there's a formal process as well. And it's written into the regulation, and every agency knows about it.

So, I highly recommend that if you're seeing requirements and contracts, but they're written in a very generic way that lacks specificity, that provision exists for a reason. And anyone who comes into possession accesses CUI or they're not sure if it's CUI or questions it, they have that avenue to pursue. It may be a little clunky, but it's there.

I also want to mention the CUI federal acquisition regulation is a FAR case. It's still moving through the process. I know it's taken a long time. We don't control that in ISOO. The council is led by GSA along with DoD and NASA, but we're doing as much as we can to move things through, and don't have any specific timelines for when that FAR clause will be completed for CUI. But in the meantime, DoD has the DFARS clause.

The other thing I want to mention about CUI that I've tried to do when I became involved is to try to... because I recognize there's a lot of clunkiness, if you will, to the thing, so many categories. And one of the things I try to do besides establishing deadlines since we're going to have a program was to neck down the number of CUI specified categories because that just in my view adds to the confusion. And so, we've been working on that, and we have reduced some specified into CUI basic. So, there's CUI basic. There are two types of CUI, basic and specified. And specified is supposed to mean because there's specificity in the law, government-wide policy or regulation that dictates either how to protect the information and/or limited dissemination. And most often it is that limited dissemination part.

And we have found a way where we can use basic and still preserve the controls if the basic controls are still acceptable in a lot of cases. So that's all I want to say. And if there's any questions, we'll go ahead to try and take them.

Jeffrey: Greg, thank you very much. I'm glad that it came up. I just would simply add, right? So, the department continues to take a measured approach as it relates to CUI. Again, we would be remiss if we didn't thank ISOO for its support in the limited implementation as the department continues to pursue, I'd know again, with an eye for transparency, it was very encouraging to hear the updates from the other CSAs today, such as they are, right? Kind of wart and all it is challenging, it is cumbersome, but we can't be acknowledging of, one, the growing reliance on unclassified information that supports the missions that are

represented across the CSAs and not understand the absolute need to be able to identify with specificity the information that will then trigger things like cyber [inaudible 02:12:07].

And so, I appreciate the nod to the DFAR rule that the department has. The DFAR rule is written in a very specific and a set of ways, largely predicated on identifying cyber security. But we get ourselves into a bit of a vicious cycle because we haven't... We really need to focus on the identification piece of this thing [inaudible 02:12:26] a fair bit of our prioritization at the time.

Mark B.: Thank you. Okay. Thank you, Greg, and Jeffrey. All right. We're now at the point of the meeting where we ask NISPPAC members to present any new business they may have. Did anyone have any new business for us?

Heather: Hi, this is Heather Sims, industry. Just real quickly, I want to make sure it's part of the record I missed during my opening comments. A special thanks to Dave Scott for his partnership and great improvement in collaboration through the NISA working group, as well as Keith Minard on 32 CFR implementation and continuing clarifying guidance. But I also wanted to note during the GSA presentation, I wanted it noted that GSA is now a sole source provider for containers for industry. And I want it noted that a 30%, 40%, 50% rise in the cost is instrumental. We're looking at industry trying to get containers for new contracts, existing contracts. So, it is definitely an impediment to our operations as well as the timelines ever increasing to get those containers. Thank you

Mark B.: No, indeed. Okay. Thank you, Heather. Right. Do any other committee members have any questions before we close out this meeting? All right. Hearing none, our next NISPPAC is scheduled for November 2nd, 2022. We are hoping to have the next NISPPAC in person, but we'll also obviously have a backup plan for the 100% virtual if we have to. And as a reminder all NISPPAC meeting announcements are posted in the federal register approximately 30 days before the meeting, along with being posted to the ISOO blog. With that, I'm going to adjourn the meeting. Thank you all. And please stay safe.