

NISPPAC Transcript November 2023

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 Office's Overview Blog at <https://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 <https://www.archives.gov/isoo/oversight-groups/nisppac/committee.html> and have also been emailed to all registrants. Please note not all NISPPAC members and speakers have biographies or slides. While this is primarily an audio conference, you're 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. Please note all audio connections are currently muted with the exception of NISPPAC members, speakers, and ISOO, who we ask to please mute their own lines when not speaking.

If you are not a member of the NISPPAC and would like to ask a question or make a comment, please hit #2 on your phone to raise your hand. If your audio is through Webex today, you may click the hand icon at the bottom of your screen or send your question to all panelists through chat. Another option is to email your questions and comments to NISPPAC@nara.gov and someone will answer your questions there. This is a public meeting and like previous NISPPAC meetings, it is being recorded. This recording, along with the transcript and minutes will be available within 90 days on the NISPPAC Reports on Committee Activities webpage mentioned earlier. 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 block so the NISPPAC team can get back to you personally. Let me now turn things over to Mr. Bill Fischer, the Acting Director of ISOO, as well as the Acting Chairman of the NISPPAC.

Bill Fischer: Good morning, everyone. Welcome to the 71st meeting of the National Industrial Security Program Policy Advisory Committee. I'm Bill Fischer, the Acting Director of ISOO. I'm also the Director of the National Declassification Center at the National Archives in my permanent position. I will now turn it over to my Designated Federal Officer, Heather Harris Pagán.

Heather Harris Pagán: Thank you, Mr. Chairman. I'll now begin attendance of the government members. I will state the name of the agency, then the agency members will reply by identifying themselves. Once I've 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. ODNI?

Lisa Perez: Lisa Perez, present.

Heather: Thank you. DoD?

Jeff Spinnanger: Jeff Spinnanger. Good morning.

Heather: Good morning. DOE?

Natasha Sumpter: Natasha Sumpter's present. Thank you.

Heather: Thank you. NRC?

Dennis Brady: Good morning, everybody. Dennis Brady present.

Heather: Thank you. DHS?

Rich Dejausserand: Rich Dejausserand present.

Heather: Thank you. DCSA?

Matthew Roche: Matthew Roche.

Heather: Thank you. CIA?

Don Juan: This is Don. I'm present.

Heather: Thank you. Commerce? DOJ? NASA?

Vaughn Simon: Good morning, everybody. This is Vaughn Simon for NASA.

Heather: Thank you. NSA? State?

Robert Tringali: Heather, Heather, can you hear me? Yes. Matt Armstrong will not be at this meeting.

Heather: Thank you. Air Force?

Annie Backhus: Annie Backhus, Department of the Air Force.

Heather: Thank you. Navy?

Robin Nickel: Dr. Andrew Jones. Primary, Robin Nickel, Alternate.

Heather: Thank you. Army?

Laura Aghdam: Good morning. Laura Aghdam.

Heather: Thank you. Now I'm going to turn to the Industry members. Ike Rivers?

Ike Rivers: Present.

Heather: Thank you. Derek Jones? Tracy Durkin?

Tracy Durkin: Present.

Heather: Thank you. Greg Sadler?

Greg Sadler: Present.

Heather: Thank you. Dave Tender?

Dave Tender: Present.

Heather: Thank you. Jane Dinkle?

Jane Dinkle: Present.

Heather: Thank you. Doug Edwards? Kathy Andrews?

Kathy Andrews: Present.

Heather: Thank you. Now I'll do a roll call for the speakers. Mike Faller?

Mike Faller: Present.

Heather: Thank you. Dave Scott?

Dave Scott: Present.

Heather: Thank you. Mike Ray?

Mike Ray: Present.

Heather: Thank you. Chris Heilig?

Chris Heilig: Present.

Heather: Thank you. If anyone else is speaking during the NISPPAC that we have not heard from or we don't know about, please speak now.

Don: Hey, Heather, this is Don from CIA. Also, our alternate Keleigh is on the line as well.

Heather: Thank you. We request that everyone identify themselves by name and agency, if applicable, before speaking each time for the record. For ISOO's telework status update, starting in December, ISOO staff will be limited to teleworking no more than six days a pay period.

I want to remind the government membership of the requirement to annually file a financial disclosure report with the National Archives and Records Administration Office of General Counsel. Before a government member may serve on the NISPPAC and annually thereafter, this must be done. The same form for financial disclosure that is used throughout the federal government, OGE Form 450, satisfies the reporting document. If there are questions, please reach out to me.

Additionally, we have had a few changes to the NISPPAC membership. As mentioned during the last meeting, our prior Chairman and Director of ISOO, Mark Bradley, was retiring that the summer. The Department of the Navy's primary member, Christopher Chrislip, has been replaced by Dr. Andy Jones. Laura Aghdam is the new Army alternate member. State Department's primary member, Kim Baugher and her alternate Mike Hawk retired and has been replaced by Kim Colon and Janice Custard-Lazarchick. Our new Industry members are Doug Edwards and Kathy Andrews, replacing Heather Sims and Aprille Abbott. Heather Sims was also the Industry Spokesperson to the NISPPAC and has been replaced by the current NISPPAC member, Ike Rivers. For those departed members, thank you for your contributions over the years. We look forward to continuing the work you have done with the new representatives.

I will now address the items of interest from the June 5th, 2023, NISPPAC public meeting. The NISPPAC minutes from the last meeting were certified to be true and correct, and were finalized by me on September 1st, 2023, and were posted to the ISOO website on September 6th, 2023. On October 5th, 2023, the ISOO Joint Notice with the Small Business Administration discussing their regulation combining their mentor protege programs was issued. It relates to joint ventures. Please see ISOO Joint Notice 2024-01. Do any NISPPAC members have any questions? Ms. Evans? Is anyone raising their hand on the phone line or sent a question via chat?

Event Producer: We did get a message that DOJ was present, Matthew Crowson and John Skinner, but other than that, there are no questions. Again, you may press #2 on the phone or click the raise hand icon in Webex.

Heather: Okay, thank you. At this time, we will now introduce our speakers for their updates. Mr. Ike Rivers, the NISPPAC Industry Spokesperson, will provide the Industry update. Ike?

Ike: First and foremost, thank you Mr. Fischer for hosting this meeting. Industry NISPPAC looks forward to the collaboration that will come from this meeting. Before we get started, I want to say something that's very near and dear and sincere to me. Most of you know that the last month, right after I was elected to be the Spokesperson, I lost my mother. I want to thank this group of folks, because many of you that are on this call reached out and sent flowers, prayers, and thoughts to my family during the passing of my mother. I want you to know that it has really helped us during this difficult time, and it showed me that our security community is not only passionate about what we do in the community, but passionate about each other. So, thank you very much for uplifting me and my family. We will never forget this. Secondly, as Heather said, I want to thank our outgoing NISPPAC members, Heather Sims and Aprille Abbott for the tremendous job they did during their tenure. And in speaking of Heather Sims, as a spokesperson, everybody will agree that she was definitely a pillar for Industry and helped open doors that were closed.

Industry NISPPAC will continue to lean on both of them for their guidance and the expertise that they've provided over the years. I also wanted to pass on a welcome

to our newest members, Kathy Andrews, Northrup Grumman, and Doug Edwards from Raytheon. They both bring a wealth of knowledge to this already awesome Industry NISPPAC team. Before I jump in to talk about a few items, I just want to say that the partnership between Industry and government on all levels is steadily. And when I say steadily, steadily moving in an upward motion, we are constantly climbing this ladder when it comes to this partnership, which is tremendous and great for our great nation and national security. The collaboration has been awesome. Now, although sometimes we agree to disagree, the outcome has been all about what is best to protect this great country. So, thank you all for your continued partnership, and we look forward to our continued growth to this strong partnership. One of the things that Industry NISPPAC would love to see moving forward is going back to the face-to-face meetings between ISOO, the CSAs, and Industry NISPPAC. If there is anything that Industry NISPPAC can do to help facilitate this request, please just let us know. We think that this would be great for everybody. Industry NISPPAC just has a few items that we want to address today. I'll address these items and then I will open it up for any of the other industry NISPPAC members for additional comments.

The first item is the 847 FOCI mitigation. Industry NISPPAC is cautiously optimistic about the 847 FOCI mitigation obligations, and we're looking forward to seeing and hearing a government plan. Industry NISPPAC is also willing to review and circulate their plans to give the Industry side of the changes to the acquisition process. Guidance such as Open ISLs, continue to be an issue for Industry. There's still a few that are out there, that are two and a half years old. Industry is looking to see if there will be a better vehicle to get policies and implementation information out. Getting a more accurate timeline will definitely be helpful to us.

We all know that NBIS is four letters that have been on our minds here for several years, but just came true to surface here recently as of one October. We are moving forward with the NBIS transition, but we do have a few challenges with the report process for large companies. Now, Industry NISPPAC and DCSA are working hand in hand...DCSA, VRO, and the NBIS team on this resolution. Understanding without reports makes validating records extremely difficult, i.e., personnel reports. Have to understand without that report, it will be extremely hard to know who is who and what is what in the company. This poses a problem, not only for VRO, but for Industry and the different services. These large companies, that have 5-10k folks, you know, that's really, really hard for those companies to see what is what. The smaller companies won't have as much problems as a large company although those problems still exist with the small companies.

With continued communication, we have been struggling with getting clear detailed information from sites such as the DCSA website, on implementation procedures and system changes in a timely manner. Now, we have been working and continue to work with DCSA by expanding on more communication avenues. We do need to ensure that all communications are filtered down, not only for the large companies, but for the small mom and pop companies as well. That information is critical to

those small companies, yes, the large companies as well, but I think a lot of times we forget that we have those small companies out there. Whatever we do as far as this communication piece, we need to make sure that it's easy and readily available for everybody to make things easier. What I'd like to do now is just to say that we Industry NISPPAC, we are here to help. We're here to facilitate. We're here to, to do whatever is possible within our means to collaborate to make things better. So, if there are ideas out there from ISOO to CSAs, anything that we can do to collaborate together, please let us know. The doors are open, we want them to stay open. We cannot do this alone. Our adversaries are getting stronger and stronger every day, and we collectively have to stick together. We, our team together to send them off on a daily basis. What I like to do now is open it up to the rest of the Industry NISPPAC members to see if there are any additional comments.

Dave T.: Hey. Do you mind if I go first?

Ike: Yes.

Dave T. Good morning, everyone. And, like I said, I would love to be in person doing this, and I think we all feel the same way. First, I have this morning is in reference to the whole insider threat process with Industry and government. One of the and this is a, I wish we were in person, but this is a question, not a finger pointing event. I hate not meeting in person, but we have, the question is, this is, and we've, you know, we've, I know this drumbeat been drum before is information sharing on incidences with people, our contractors back and forth, stuff that DCSA is aware of or other government agencies aware of. They don't share with us. It's reference to the briefing that we had with the ManTech situation, with the shooting at one of their facilities with information that was not received or communicated. And again, this is not finger pointing. These are just, you know, requests. It handcuffs Industry a lot. Everyone's concerned about something like this happening again. So, my question to you all is, you know, how to help us better our facilities, our companies. protect ourselves and protect you. All we have government contractors going to government is if there is any progress been made or any attempt that's, you know, it's going forward. You know, there's a lot going on in reference to information sharing between industry and government.

Jeff: Hey, good morning. This is Jeff Spinnanger. I'm sorry. And I think the, the hesitation in going on is more a function of like I said, virtual challenges and not trying to step on anybody. So, wanted to wait a moment there, just to clear the calm. So that's my way of saying I absolutely agree and hope that this is the last of the virtual. Although I do like the shoes, I'm wearing better than the ones I would have to wear in person. So, two things I have to say. The first being I love the fact that there's a question, you know, frequently I think, again, as a byproduct of us being virtual these, meetings that tend to be transmitted only and not a discussion.

So, so happy for any question, even if it's a hard one, which this one certainly is. With that in mind though and I'll get into this a little bit more, when I provide my

remarks, but, information sharing, you know, sharing, you know is has definitely been a byproduct of a number of the challenges that we've experienced over the last six months. The problem is, of course, been much longer than that. There are some plans at work right now, to attempt to reprise what had been done several years ago, which is to tabletop, this to understand what information elements, are required to be shared. And then addressing the hurdles, in sharing piecemeal that is very much in the nascent stage. If I could, put us on notice here I'm happy to be phoning a friend here later today to my battle buddy, Jill Baker, who leads this up for us in DoD to find out where we are in the planning, and then maybe, kick this over to a working group to give you all an update on what we are proposing in terms of trying to tabletop this at a policy layer and not continue to kind of grind on it at the execution layer, right? Which is, maybe something that we've, have been attempting with not a lot of success over the last, yeah, well, for quite some time, over.

Ike: Hey, Jeff. This is Ike. We really, really appreciate that, right? Because it's something that Industry acts all the time from the different agencies because we all know that each agency does there, you know, has a small portion of, you know, the things that they do that are different. And it'd be helpful. because most of us have companies that are involved in most of those agencies, right? That information sharing will help us get our folks through lines and processes and a lot faster. In this particular case, it could help and save lives for that particular matter. So that information sharing is extremely important. And you coming on, helping us try to navigate that and pass on that open communication to Industry will really help. So, thank you very much for coming on and saying, and presenting that. Is there anybody else from the Industry NISPPAC members that would like to add an additional comment?

Jane: Yes Ike, this is Jane Dinkle. Thank you for the floor. And hello everyone. I really wanted to mention reciprocity and, in general, I wanted to acknowledge the success that we've had in the area of personnel security clearance reciprocity. There are a few challenges that continue, but in general, we do consider this an overall success story. and we'd also like to see similar progress in the area of 705 standards and physical security requirements implementation for special program areas from agency to agency. So maybe we can add that to our work plan going forward to try to achieve the same level of success.

Ike: Thanks, Jane. Anybody else from Industry NISPPAC? Well, Heather, I think that is it for the team. I do want to leave with just thanking everybody on all avenues. The services, the government, everybody that has been involved with this partnership, it is getting stronger and stronger, and the more that we collaborate and get together, we just strengthen this great nation to be in a position, to do great things and to be able to shield ourselves from anything that the adversary throws at us. Again, whatever industry NISPPAC can do to continue to foster this great relationship, please just let us know. And we're there. That is all from the Industry side.

Heather: Thank you, Ike. Candace, do we have anything in the queue?

Event Producer: We have one person who's raised their hand. Greg Pannoni, please go ahead.

Heather: Greg, are you muted.

Event Producer: Hold on one minute Mr. Pannoni. Now can you restart, please?

Greg Pannoni: Sure. Greg Pannoni, Johns Hopkins University Applied Physics Lab, and I hope I'm not out of line, but can you hear me?

Event Producer: Yes, we can.

Greg: Okay. I think Ike Rivers really said it, but the overarching concept of partnership and collaboration, really appreciate what Jeff said about in the area of information sharing, looking at a tabletop exercise, but what I wanted to really say in the context of all that, with the collaboration and addressing critical challenges to put a plug in if my Industry colleagues agree, to invite Industry in as early as possible in the process. So, the example of the tabletop, I think, inviting Industry into a tabletop exercise to provide input on what the critical information that from the Industry perspective would be most necessary and useful would be an example of that, what I'm trying to convey, and perhaps not in a very articulate way. So that was all I wanted to mention. Thank you.

Heather: Alright. Thank you, Greg. Ms. Evans, anyone else in the queue?

Event Producer: There are no further people in queue.

Heather: Okay. Thank you. Mr. Jeff Spinnanger, the director for Critical Technology Protection for the Office of the Under Secretary of Defense for Intelligence and Security, will give the update on behalf of DoD as the NISP Executive Agent. Jeff?

Jeff: Good morning. Thank you very much, Heather. Good morning, everyone. Thank you very much for the opportunity to participate in this. Before I begin my formal remarks, I just want to start by offering some echoes to some of what I shared earlier, both in wishing well and congratulating Keith, Heather, and Aprille on completing their successful tenure. What's interesting is I think in the beginning, Mr. Fischer, you mentioned that there have been 71 NISPPAC public meetings. I'm pretty sure that Keith has been at all of them and has spoken at all of them. So, we're going to try to figure out a way to entice him to chime in from the cheap seats today, but his stewardship and the strong partnership that he had and maintained, along with, you know that Heather and Aprille and frankly so many others is something that we're all challenged. Those of us who remain, you know, on the committee, you know, are challenges to capitalize on their great work and continue to expand it. So, with that, I would say, then welcome Ike, Kathy and Dr. Edwards. I want to make sure I get that right. Very happy to have you joining us.

Our phones are always open, and we are better for the collaboration always. So, I want to say thank you on that front.

I definitely want to offer an echo to something else that Ike said with advocacy of the face-to-face, right? So, the awkwardness of the exchange from earlier today, just kind of highlights it, but also gives some promise. It was great to have a couple questions and some level of conversation, such as we're able to muster, when we're all distributed all over the place, and I think that's great. But I also think there's an opportunity before I dive in here to highlight again something else that Ike mentioned. It does speak to formality, right? So that flow of information are greatly connected both through the NISPPAC the various associations that are out there, great connections, great partnerships that are absolutely invaluable with those larger companies. I do take to heart what Ike mentioned about ensuring that we're able to cast them as wide as we can possibly make it to be able to reach the kind of what are the meat of the Industrial Security program, which are companies that are small in size. Those are the engines that everyone relies on. I hear that all the time. Not always, frankly as a function of conversations on Industrial Security, but on things like supply chain resilience, you know, the National Defense Strategy imperatives that absolutely underscore the essential nature of a vibrant supply chain for the Department and national security mission spaces. All that little soliloquy is a bit of an endorsement of face-to-face, but it's also of the formality that comes with NISPPAC, right?

I'm reminded anytime we do the prep here, that everything we say is on the record. And on the record is absolutely essential, because that's where accountability comes from. So, there's no shortage of collaboration as has already been mentioned, and I'm sure we'll continue to be mentioned and highlighted in some of the great work that I think is going to be reflected across the balance of the agenda. But it's that on the record piece of this thing that as I contemplate my own tenure that I think allows us to move forward and take on very challenging, contentious issues where sometimes we're not all fully aligned, but when we're able to, we're expected to bring them to light, put them to discussion, and then follow up on them through the stewardship of ISOO and the NISPPAC, then we get that we make forward progress and we get things done, and so with that, you know in considering, you know, an in-person, you know, for future NISPPAC, I hope we will revisit, and I can't miss the opportunity to mention as I have over the last several public meetings, the need for possibly increasing the frequency also for the, on the record, no disrespect to the working groups, but it's the on the record stuff that holds us all to task, and we're all able to measure, our progress and note our challenges, and then work through them. So, with that, I'm happy for the opportunity to provide some updates on, you know, a number of those same kinds of areas where we have some kind of weighty issues that we're working on, and I'd like to provide some updates on that.

The first one and foremost is with respect to the ability to use cloud services in support of NISP requirements. As many of you are aware, we have worked through

several instances of direct contractor use of commercial cloud services to support DoD contracts that require access and utilization of classified information. As cloud becomes more prolific in the NISP, and that is a bit optimistic at this time, but the gear is actually beginning to rotate, which is, I think, absolutely essential. We are aware that there are continuing questions regarding requirements for how to go about, noting the permissibility, for the use of commercial cloud services on DoD contracts. To that end, and with the tip of the hat to some strong Industry advocacy from several companies who have many, many classified systems, you know that are used to support the Department customers across the defense enterprise. We have engaged with our counterparts, on the acquisition side of things, and the Office of the Undersecretary of Defense for Acquisition and Sustainment, to obtain some clarity on a couple of legacy DFAR clauses that relate to cloud. I'm not going to rattle off the numbers here. Most of you are familiar with them. We are looking to codify. We originally and aspirationally attempted to see if we could rescind them, say they were maybe overcome by events that is proved to be maybe a bridge too far. There are some reasonable contracting reasons for that. I'm not going to embarrass myself and try to explain in a public forum, but suffice to say, I understand. On the other hand, we have gotten greater guidance from our acquisition partners that they don't actually present an impediment at all. There's some clarification that's necessary, and that's something that we're working through right now. The first and foremost way that this will be observable to NISP members will be through the issuance of an Industrial Security Letter. It's almost done. I'm not a big forecast person, but we'll put ourselves out there. I'm optimistically I'd like to see that. I'd like to say that we will see it before it turns to 2024 on the calendar. That's certainly within the run of the possibility, but it'll be the first one out of the chute for us, issuing an industrial security letter under the new process, mindful of the NISPOM as a federal rule, but we think it's the right one to move forward with because it's a pretty present issue. And so, we will get that done here in relatively short order and I think that will make some headway. That's not going to get us done, though, not by a long shot. We're also working very closely with our counterparts at DCSA and across the components to come up with common, acceptable documentation we think that the 254 is the right place for all the reasons that the DD 254 exists, and we're looking to kind of streamline that, so to anticipate some consistency as requirements for commercial cloud services will continue to grow. And on this last point, and with the tip of the hat to frankly, to Keith Minard, we were chatting earlier in the week, and he proposed a simple, but in my estimation, brilliant, additional step that we can take.

That one creates some affirmation of the authorization to use commercial cloud services, but also something we can get done pretty fast, and that is, without modifying the form itself, but rather aiming at modifying the instructions that attend to the form, all the fine print that sits in those back pages, and noting the permissibility of commercial cloud services within the instructions, will be an important step. Again, you know, noting the dangers of forecasting, I think it's a useful exercise to do this in this forum and say that we will endeavor to move

pretty fast on that front. Not quite ready to put a specific timeline to that, but I think it can be quite aggressive. And so, all of those to me represent a lot of forward progress, and this particular issue is, I think, a pretty good example of the value of NISPPAC, because it has, we have been on the record as we've taken this journey. It has been an absolute partnership. We would not be where we are but for some active participation from a number of companies who are willing to take on some risk and uncertainty to work with the government and get us to where we are today. So, we're not done yet, but we are definitely closer than we have been.

So, the next one, and Ike touched on this one...I'm glad you did, and that was the discussions related to 847. If there was one part of my remarks where maybe it would be great if you didn't hear me, it would be this one. And I'm kidding, of course, but just the level set, not sure who in the audience is completely aware, but 847 comes to us from Public Law 116-92, and expanded and extends requirements for FOCI modeled after what all the companies in the Industrial Security program are familiar with. It applies to companies who seek to perform on DoD contracts or subcontracts with a value in excess of \$5 million, including those contracts for which all the required work is unclassified. It requires DCSA specifically to conduct a FOCI assessment and possibly mitigate risks of FOCI of covered contracts for inclusion in the acquisition decision process. This policy, we're mindful of timelines on to this point, right? That is a major change in, although modeled after NISP requirements for FOCI. It's that pre-award aim point versus the post-award process that we're all familiar with, that has caused us to be quite deliberate as we move forward, but at the same time in saying that this is a major and important shift in assessing the department supply chain in a pre-award versus post-award matter. And again, it's echoing some of what Ike said earlier, it's representative of the evolving nature, of the threats we face to deliver war fighting capabilities that we can rely on, G-d forbid we need them. So, with that, mindful of that pre versus post, we have been quite deliberate in this, have reported this out before we continue to do that. The policy work that we're doing today, is in its final stages, right? To be quite candid, we are literally down to one unresolved issue within the policy document, which is a tremendous accomplishment. That tip of the hat to Allyson Renzella, from my team for her doggedness. Laura Aghdam was working with her up until the summer, and then ditched us for the Army, and now Glenn Clay, who's just recently joined us from the Navy, but we're in the home stretch here, having to write some words to pass some legal muster. But we're reasonably optimistic about where that leaves us. This gets to the meat of the matter. And I think the request that was perfectly reasonable, and I think will be very helpful, that came in, Ike that you mentioned, which is the opportunity for being able to understand, you know, what the rulemaking, that accompanies a shift of this type. That's pending. So, we'll take an action out of this call today in addition to what I mentioned earlier with, with respect to insider threat information sharing, but we'll take an action to go back and, and work with our A&S counterparts, because the rulemaking should begin to move forward here in earnest. We have aimed for what in policy parlance is referred to as legal sufficiency review. We are possibly one

email away from that process beginning, and this is where then we begin to parallel track, into the rulemaking phase of this, which will necessitate, certainly, awareness by our Industry partners, but also and more importantly, understanding, so we can all move forward and achieve what was expected by the purpose of the law in the first place. So, with that, we think that that's probably something that we'll bring to the clearance working group, if that is the right one. Allyson just told me, and I can't remember what she said, so if I got that wrong, I apologize, but nonetheless we'll be bringing that here.

We're just about at that point, switching gears. Another topic of some contentiousness, that continues to play out, and that's with respect to joint ventures, small business joint ventures. And so, with the tip of the hat and a thank you to ISSO for publishing a notice on small business, the guidance on the small business federal rule, we're happy to have that. It represents some progress on the issue. It's pretty complex. With a measure of candor, I've read the guidance several times, and it's helpful in subsequent readings. We think we understand the intent. Ultimately for the department, we think it helps to compliment and reinforce, what we intend to push over the line here, in the coming month or so, and that is what we call a directive type memorandum, which will help to further clarify and provide guidance to address the issue. When we're done here, the DTM will provide guidance for both DCSA and DoD components on the process for joint ventures, which meet criteria within the statute that established, you know, where some of the ambiguities, or the conflict exist. It'll provide some guidance there to be able to kind of meander through that without having to go and take the extraordinary step to request exceptions to policies related to the Industrial Security program, something which is an arduous and time-consuming process. It's sand in the gears, it slows things down. And when we're slowing things down where contract awards are, that doesn't serve anybody's purpose, it certainly doesn't serve the Department's, and nor that of this in the small businesses that frankly, we rely on for the award and who rely on those awards in order to be able to, you know, frankly operate. So, we'll continue to keep you posted on that one. We think that that will move relatively quickly once it clears the lawyers. Everyone knows it's important. I briefed my leadership on it most recently on Monday, and so that's where we stand at this time.

Two other brief topics here to touch on. It doesn't feel like you can go a week without saying the words Trusted Workforce, in the next one, another in a sentence. I made it several months without having to do that, and now we seem to do it all the time, but a brief update on the Department's efforts with respect to 2.0. You know the recent 45-day review that we undertook earlier in the summer and the subsequent follow-on actions that the Secretary of Defense has discussed it for us, regarding security in depth, really highlighted the importance of the ways in which we identify mitigated risks, which brings us right to Trusted Workforce. The review provided us with some data and results in the form that we were able to use to form recommendations for policy procedural and candidly, some cultural changes,

within the Department. Much of the focus areas center around personnel security, and line up pretty well, and a bit of clearing calls with respect to Trusted Workforce efforts and aim points. The Department's Trusted Workforce 2.0 implementation efforts, like policy improvements, continuous vetting enrollment, elimination of PRs, have already led to significant measurable improvements in the personnel vetting processes. Remaining initiatives like CV for Nonsensitive, Public Trust population shared services through DCSA, and continued focus on NBIS deployment, aimed to increase efficiencies, reduced burdens on the vetting process, increase overall workforce mobility across personnel vetting domains. Our personnel vetting counterparts are working to evolve the Department's methods for information sharing along this same access, right? So, it nods to our earlier discussion and some of the homework that we'll take out at today's meeting. Under the Trusted Workforce Agency specific information is forecast for incorporation from partner mission areas into continuous vetting, which will enable more robust personal vetting and risk management. And finally, along the same access, Trusted Workforce you know, the bumper sticker for us is that we'll better position the department to develop and maintain personnel ready, you know, to protect our national security. And that's the cost of board, right? So, you know, contractors, military personnel, and, of course, civilians, as well.

Finally, the last topic that I wanted to raise today was just to highlight the second NISPPOM amendment. It's progressing. It's pending approval now from our senior leadership, to be published to the Federal Register. So, we're within the workflow. It's all pencils are down now, subject to any questions from our leadership. We anticipate it to be signed whenever we're able to kind of cycle it into the, to all the other things that, that our senior leaders have to contemplate right now on a pretty, topsy-turvy, world stage. The amendment includes updated language on safeguarding, offers some clarity with respect to open storage requirements, including procedures for leaving an open storage area unattended during business hours, and allows for delegation of open storage area approval authority for FSOs, if agreed to by the Cognizant Security Agency. All of these changes are reflective of recommendations that came in through the comments, which is a good and open and transparent dialogue. Ironically, once published, there's an opportunity to comment on the amendments. So, the process continues, and I know I can speak for Allyson and now Glenn, that they're super excited because, rulemaking is, well, it's a process. And so, but it is also reflective of the need for continuing dialogue. Those rules become that common script that we all operate, you know, in terms of. And so, making sure that we're getting the language correct, in a way that will hold up over time is important. And we need your help and assistance for that. With that concludes my remarks. Happy to answer any questions and thank you very much for the opportunity to participate today.

Heather: Thanks, Jeff. Do any NISPPAC members have any questions or comments?

Greg S.: This is Greg Sadler. Jeff, can you elaborate on the last item you touched on regarding the open storage approvals? I just want to make sure I capture that right.

Jeff: So, not with a great deal of depth to be very, frank with you, Greg, I just know we had comments that came in that looked for us to offer clarifying language that it is absolutely permissible for the open storage area approval authority to be delegated to an FSO, right? So, based on the Cognizant Security Agency direction. So, some level of documentation of that, I'm thinking of DCSA coming in when they want to conduct an assessment, right? Understanding what was permitted to be left in open storage, or left out, excuse me, you know, would be subject only to documentation. I'm happy to take a note back, and we can either update my remarks when we go through this, just to be able to offer some more clarifying language. And of course, we're always available to provide more detailed offline, although that won't serve, everyone else in attendance today. Thank you.

Ike: Appreciate it, Jeff. Thank you.

Jeff: You bet.

Heather: Do any other NISPPAC members have any questions for Jeff?

Ike: Hey. Hey, Heather, this is Ike.

Heather: Yes?

Ike: Hey. Hey, Jeff. We, I haven't seen, or I don't think any of us have seen the NISPOM amendment. Is that a possibility for us to see that?

Jeff: So, if it is? Absolutely, we'll get it out straight away. So, my normal answer would be to say just an unqualified yes. I just want to make sure that I hope you can appreciate, want to preserve some decision space from my leadership, since we've made it through all of the coordination steps at this point. you know, and we're, we're literally at the phase where we're just asking for signature. I don't want to do anything that would upend that because it's taken kind of a long time to get here. On the other hand, if we're allowed to send it out as a draft, we'll do so today, and gosh, if we were in person, I would just sort of be looking kind of over my glasses at Allyson, and she would probably be able to give us an answer right now, but, but yeah, you bet.

Ike: Okay, thank you.

Jane: Jeff, this is Jane Dinkle with NISPPAC, and I had a question about the cloud services and how we document those, or the ability to use, the cloud services, and you mentioned that you'd engaged with acquisition and they were updating or working on the DFAR clauses and that the ISL is almost done, and we'll see that by January one, or you said before the calendar hits 2024, and then you mentioned about Keith Minard updating the instructions to the DD 254, so all of that will come out at the same time?

Jeff: So, probably not. So, I let me kind of reverse the order there. One, you know, so this modification instructions, I, to be candid, it was Keith's idea, but someone else has to do the work, and he specializes in that a little bit, but it's a great idea and it's actually a pretty straightforward thing to undertake, so, I'm hesitant to put a clock on that now though. I think we'll be able to do so even, you know, when the working groups next convene here if they meet in the month of December. So, we should be able to have a clock on that. With respect to the ISL, yeah, I'd like to hammer down on that one. You know I didn't, maybe I didn't touch on it with enough depth, but the process for issuing ISLs now requires us in a good way, but we need to make sure that we get OMB coordination before we move to putting an Industrial Security Letter out. And so that is a wrinkle in the way in which, that isn't the same way that we've done it in the past, and we're stepping through that right now, both so that, we, the royal, we, the Department, certainly coordination through NISPPAC, but also, in this engagement with OMB we can identify a repeatable process. Because ISLs are an important tool as I think has been alluded to, we have a number of them in the pipeline. We went forward with all of them back earlier in the fall, and I think maybe overwhelmed the system a little bit the same time that we were also pressing with OMB on the NISPOM Amendment. And so what we needed to do was to kind of sequence that out a little bit, certainly with deference to DCSA if they felt differently, but for my office, this first one, the cloud ISL is, at the top of the stack for us, for the reasons that I've already outlined, and I'd like to see that go forward and see it, teed up for signature this calendar year. Absolutely. With respect to the DFAR, though, I want to make sure that there wasn't any confusion. There are no changes proposed for the two DFAR clauses that relate to cloud services. Neither one of which is proposed for change because neither one of which impedes the use of commercial cloud services in the NISP. What is necessary is for us to come up with some consistent language and mechanisms to note and annotate the permissibility for the use of cloud on contracts requiring access. And that's what we have focused on at this point.

Jane: Much appreciated. Thank you for that clarification.

Jeff: Of course. Thank you.

Heather: Alright. Do any other NISPPAC members have any questions for Jeff? Alright. Next, we will hear from Ms. Lisa Perez, the Senior Policy Officer for the Policy and Collaboration Group with the Special Security Directorate, National Counterintelligence and Security Center with the Office of the Director of National Intelligence. Lisa?

Lisa: Good morning, everyone. Thank you, Heather. So, this is Lisa Perez of ODNI. To Keith, Aprille, and Heather, thank you for your great work on the NISPPAC and for your collaboration during your tenure. I wish you all equivalent success in your new role. Also, thank you to Ike for sharing Industry perspectives. It's much appreciated. And to Jeff, thank you for the detailed remarks and answers

to all these questions and support for the Trusted Workforce 2.0 initiative. And speaking of Trusted Workforce 2.0, under the initiative, ODNI and OPM issued guidance to agencies for how they should collect and report metrics in alignment with the previously issued Federal Personnel Vetting Performance Management Standards. So, the guidance will help improve data consistency and reliability across the Executive Branch. So, the two key changes include setting substantially more aggressive and aspirational timeliness targets for the end-to-end personnel vetting process and establishing a metric measuring the average time needed for agencies to reach an onboarding decision. So, the new metrics will be iteratively rolled out based on agency readiness, moving toward the full implementation in fiscal year 25.

And then onto the next thing I was asked today to speak about the SF312. So, the SF312 12 is currently undergoing some updates and is currently going through the DNI approval process. We do not have a projected release date right now, but I just wanted to make sure that was on your radar. After issuance, I'll provide an overview of changes to the NISPPAC, and the updated version will be made accessible through our website. So meanwhile, the current version of the form may be digitally signed in accordance with 32 CFR 2001.80, and through coordination with U.S. General Services Administration, the link from the dni.gov website takes you to the current version of the SF312 Classified Information Nondisclosure Agreement that is configured for digital signatures. So, when clicking on the link on the GSA webpage, the document will open in web browser view, and it will be formed fillable, but we've had some questions. So, we've learned from these questions and emails that some have experienced that they're unable to apply the digital signature in that particular view. If this is the case, I just want to remind everyone, you can save the document from the web browser to your system and you can reopen it in Adobe Reader. In Adobe Reader, the digital signatures can be applied. Adobe Reader is downloadable from the same GSA webpage. And, probably through ISOO I'll provide a copy of this explanation, with a screenshot displaying the GSA webpage. And then I'll also provide a link to the GSA webpage as well as a copy of the brochure we have prepared to provide an overview and answer frequently asked questions regarding the SF312. And then as a follow on, once we've actually updated the SF312, we plan to move on to our Form 44 14 for those of you familiar with it, but there are no specifics about that one yet, and that is really all the updates for me today. Are there any questions for me?

Heather: Alright. Thank you, Lisa. Thank you. Any questions for Lisa? Alright, up next is Mr. Rich DeJausserand, the Deputy Director for the Enterprise Security Programs and Policy of the National Security Services Division, with the Office of the Chief Security Officer at the Department of Homeland Security, who will provide their update. Rich?

Rich: Thanks, Heather. Good morning, everyone. I do not have any official updates for the group; however, I do have some information for the group. The Office of the Chief Security Officer under the Management Directorate, we have

completed our move from seventh and D Washington, DC to the new TSA headquarters in Springfield, Virginia. The Management Directorate now occupies the sixth floor, and we are here until further notice, and we will also continue in the telework posture for the foreseeable future. That's really all I have. If there are any questions, I'm happy to answer.

Heather: Alright, thanks, Rich. It looks like there's no questions for DHS. Any questions? Alright, Mr. Mike Faller, a program management specialist with DCSA NBIS Planning and Deployment, is now going to provide an NBIS update. Mike?

Mike F.: Hey, good morning, everybody. Yes, this is Mike Faller here with the DCSA NBIS Planning and Deployment Office here to provide a briefing on NBIS this morning. So, appreciate the ability to join here today. I just want to reiterate a couple things that Ike mentioned earlier, as far as the partnership goes between our team, and our organization and Industry, especially the NISPPAC team. We've had a tremendous relationship with those folks over the last year, as we've moved forward with NBIS. We meet with the group multiple times a week to do meetings and updates. And we're also communicating back and forth on a daily basis. So, getting some great responses back, getting a lot of good information, from the Industry folks on some of the challenges that they're seeing with the system. We've made a number of strides to get folks onboard here for the 1st of October. And, you know, just like I said, great partnership. Several weeks ago, we actually hosted nine folks from the NISPPAC team in Boyers, Pennsylvania at our processing facility. Had a two-day session with them, covered a lot of great information about FY 24 and how NBIS is going to be rolled out over the next fiscal year, talked about a number of issues and concerns, from both ends, and then we also talked a lot about training and communication. So, I'm going to cover some of that stuff here today.

I did provide a slide deck if folks want to take a look at that. If you're following along on the slides, we can go ahead and move to slide number three, which is our past, present, and future slide. Just so, just in general, we wanted to cover where we've been, where we are, and where we're going, with the NBIS program. So, just real quick, where we've been last year, we started scaling Industry companies in March 2023. The memo from Director Lietzau came out on May 5th to the NISPPAC informing Industry to complete transition to eApp for case initiation by October 1st. Like I said, extensive communication with the NISPPAC team, with our industry partners to get the word out and work with Industry to get onboarded. So, we do have the majority of Industry onboarded into NBIS now. We removed the case initiation function in DISS on October 1st. eApp has officially replaced e-QIP as the standard form collection platform. With that, it improves the security data validation and user experience. And, we're working closely with the VRO team, who has been processing background investigations and CV requests in both NBIS and DISS for the time being. We are continuing to see cases come through on DISS. We are clearing out that inventory at this time. While there's no new initiations, they're being initiated in DISS, you know, we do still have some of those

cases that were in progress prior to the first, but we're continuing to see those progress. Right now, we're looking at 99% of case initiations coming through to us via NBIS. So good success story there.

And as far as the onboarding piece goes, we do still have a few companies that we're working with to make sure that they do get transitioned over to NBIS. I think a few of them held off over the last couple months because they were not planning on initiating any investigation requests or CV requests. but we are continuing to track and monitor those folks. We're working closely with our Industrial Security team who is working with the FSOs at those companies to push out the guidance needed for them to onboard into the system. So, we're continuing to progress there. Right now, there is still some swivel chair activities, common term that we use here, which will be used for quite some time here, as far as you know, functions that are available in both DISS and NBIS. One of the things that recently did come up, we have provided guidance, for onboarding personnel and for bringing new folks into the system as far as actions that need to take place in DISS versus actions that need to take place in NBIS and in some cases, both systems. We're very much focused on the initial piece where we're bringing subjects on board, but we also need to focus on what happens whenever subjects leave a company. One of the things that came out of the most recent NISPPAC group that we had on Monday, was to provide some guidance for that. So, we're continuing to do that, working on that.

We'll, as always, work closely with our POCs on the Industry side to make sure that we're providing the right information in an understandable and effective format, so that, that continues. I did see that Ike mentioned the reporting issues. And we agree. The reporting issues that have occurred over the last couple of months here have been an issue for Industry as well as our other customer agencies. The output on those reports is currently capped at 10,000, which is not acceptable for several of our Industry companies that have many more employees, than that. Our customer agencies fall into the same situation. Some of our large submitters have the same issues. So, one thing we do want to mention is we are working closely with our solutions team to do two things. Number one, we're working to expand the output from 10,000 to 100,000. We are also working on expanding the timeouts to 15 minutes. The lag time issues which are coming back from Industry, you know, again, unacceptable needs to be resolved, and we're also just overall that that feature is expected to be tentatively rolled out in our December release, which is NBIS 4.6. So, we're again working very closely with our solutions team to make that resolution and make sure that that information is available to industry and all of our customers.

So, future, a couple things, coming up. First thing, the big future item that we have for FY 24 is going to be subject management. All of that information and functionality that folks are seeing in DISS today on the Industry side and some of our non-DoD folks are seeing on the CVS side, we're going to end up transferring over into end NBIS this year. This includes data migration and mapping, as well as

the transition to NBIS as the official system of record. Folks will remember whenever we move from JPAS to DISS several years ago, there was an official notice that came out identifying DISS as the system of record. That same information will come out for NBIS in the future. The data is 100% TBD at this point in time. It's dependent on the functionality of the system and the capabilities involved.

Also internally, we're going to be working on quite a few items on the internal side of DCSA. So, we're going to be working on the background investigation piece, continuous vetting and adjudications at the DoD, at the DCSA CAS. So, a lot of information to carry forward there. Over the next year, 4.4 million data points need to be carried forward from our legacy systems. There are 32 legacy systems that we need to account for and pull forward. One of those, pretty close to me here, as a prior background investigation employee is PIPS. We have over 200 terabytes of data that need to get carried forward from PIPS into NBIS. So, big, heavy lift there. A lot of information is coming forward, a lot of functionality. You know, some of these systems, for example, PIPS has been around for over 50 years. It's been patched over many times, a lot of functionality that needs to come forward. So heavy lift there as well. So, we're working both internally and externally to move forward on our systems.

If you're following along, let's move on to slide number four. All about the data. So, data that, as we move forward, data migration is a key component to the success of NBIS. So, a couple things that we have migrated so far. Subject pre-filled data has been pulled forward from e-QIP to eApp. So, if a subject had a previous investigation request initiated or completed in e-QIP, that prefill information is going to carry forward. So same as e-QIP. If you have a reinvestigation or a new request, you log into the next request. Your typewritten information is carried forward and available for you to update the standard form. You do have to answer the yes, no questions as you did before, and make sure that you make any updates as needed. Also, subject affiliation has been pulled forward from DISS to NBIS in September. We mapped subject data, or I'm sorry, we mapped subjects, from the system SMOs to the corresponding NBIS orgs in September. This is completed using a flat file at this point. There was a major push in September that pulled all of the information over, actually around 98%, which is actually pretty successful for us, when it comes to moving data. The remaining 2% has also been resolved at this point in time and subject affiliation is now present on the subject management tab in NBIS, so folks are able to go in and see that information at this point. We're continuing to update this information in two ways. Both information coming back and forth between DISS and NBIS on weekly files. This is expected to continue until real time update is in place. That's targeted later in calendar year 24, probably the first quarter of the new year. So, data to be migrated.

A lot of information, that's listed on the slide here, no need to really go through it. It just kind of covers everything basically. In short, anything that's on DISS at this

point in time is going to have to be carried forward into NBIS. So, working very closely with our data team to make sure that we do have the one-to-one transition on that, and that that information is carried forward into the correct location where our users can see and take action as needed. So, a couple of actions for today. As mentioned, you know, the swivel chair is still in play, working back and forth. Some of our customers are going to have to work on several items in DISS, some items in NBIS, some items in both. We have a number of pieces of documentation and guidance that are out there that we've presented to the users. Primarily our training materials are available in the STEPP system as well as ServiceNow, also known as ESD, knowledge articles that are out there for folks to use and gain access to. So also, on the slide bottom right there is a hot link to STEPP, for the IR guide that is available to folks. Certainly, want to make sure that everybody gets a chance to take advantage of that and the other documents that are out there on our training site.

So, if we move on to the next slide. One of other things we heard from both Ike today and then also from our NISPPAC members that joined us up in Boyer several weeks ago was communication. A big issue that we had as recently as a month ago was that our website didn't really have a lot of great information on there about NBIS. It's probably one of the biggest areas of concern for us over the past several years, and the information that was on the website was very minimal. So, we are working with our Office of Communications and Congressional Affairs team, otherwise known as OCA. And we've been working on the website to add additional information on there. One of the latest things that came out several weeks ago was the addition of the NBIS tab. So, if you go to DCSA.mil, go to the homepage on the top page, you can kind of see it on the slide here. There is an NBIS tab that's available anywhere you are in the system. If you hover over that, you get a dropdown menu that has a lot of information and good information for all of our customers that are out there. We have a federal onboarding link, and then we also have information for Industry onboarding on there as well. A couple things that we've added to that, first off, VRO has helped us tremendously with adding some additional Industry specific documentation that's out there that will help folks with the initiate review function in the system. We also added a hot link in there to provide a redirect to the Voice of Industry.

Over the past several months, we've been putting a lot of great information out into the Voice of Industry about updates to NBIS, updates to processing. It's already available on our website, but sometimes you have to go through several locations to get it, so, we added that link on there as well. We're really looking at this as a springboard to more output in the future. A couple things that we're looking at in the future term, we're looking at adding releases and updates, versions, and hot fixes. You know, we have a new version of NBIS that is expected to come out quarterly in the future. We're also working on a number of hot fixes at this point in time. We're working through some weekly hot fixes, to try to make certain updates to the system to improve functionality. Something else that will be added onto the

overall dropdown is NBIS training. There's going to be a subpage on there. We've been working very closely with the NBIS training team to get that information updated and provide quick links to STEPP, ServiceNow, and other locations on our website that have important information for all of our customers. So that information will be coming out. Something else we're working through is to add additional guides and resources. If you look through our website now, a lot of the guides that we have out there relate to e-QIP: how to fill out my form, how to complete the SF86 is very e-QIP centric, because that was the system, we have been using over the last 20 years. So, you know, what we're working on is getting that updated to eApp. So that will continue to go forward. We're also working on updates on the NBIS news page. We do have some information out there already, so we do have, we do have that out there. One thing we do have available on the news and publications is <inaudible> promotional message from NISPPAC. So that is also out there. So, more information to come in 2024. I know we're getting close to the 10-minute mark, so I'll just kind of move it along so we can have some questions here at the end.

If we go to the last page, one thing we do want to mention, we do have some new contact numbers, for our help resources coming up. The Boyer's phone numbers have changed from a 724-area code to an 878-area code. This information is on our homepage on DCSA.mil that covers specific help desk folks. Many Industry folks have used the CET and the Applicant Knowledge Center over the past several years. We do have their contact numbers for them. It's listed on the slide here, and it's also listed on our homepage of DCSA.mil. So, we certainly hope folks get a chance to use that going forward. And that is it. That is what we have as far as the slides today. And happy to answer any questions anybody has.

Ike: Hey Mike, this is Ike.

Mike F.: Yes Sir.

Ike: Hey Mike. I just want to commend your team and DCSA for hearing Industry. I know that several of us from Industry NISPPAC was part of talking about the enhanced communication and we really appreciate the fact that you heard us. You guys evaluated what needed to be done, and it's great to see that you're taking the steps to ensure that no one is left out in Industry. So, we appreciate the fact that you heard us and you're putting some of those things to good use. So, thank you for that.

Mike F.: Yeah, thank you, Ike. I appreciate that very much. And honestly from our end as well, your input and communication are only helping us and helping the community. So, you know, it's definitely a two-way street here. So, we certainly appreciate the partnership we've had with the team on this project. I've been in this space for quite some time, and this is probably the best partnership I've seen as far as going back and forth and the pace of communication between our two groups. So certainly, appreciate it and look forward to continuing to keep improving. Thanks, Ike.

Greg S.: Mike, this is Greg Sadler. I've got two questions, brief ones, I believe. The first one is when you referenced the system of record change, that's it's TBD, from a DCSA perspective, is that TBD notional 2024 or more confident TBD 2025 fiscal year?

Mike F.: Yeah, I would not have a solid answer for you on that one, Greg. It is at this point is just TBD,

Greg S.: Okay.

Mike F.: We're not tracking it, in any sort of ballpark figure at this point.

Greg S.: Okay. No, I appreciate that and completely understand. The second one is NBIS is obviously a bright, shiny, hugely impacting object that DCSA has been chartered to roll out. And as Ike said and you've reported it's moving and the communications improving et cetera, does the agency believe that it's drawing resources or, <inaudible> resources away from the other systems that DCSA's charter to not only administer and keep alive, but roll out, we've got NISS, which is bumpy, and we've all agreed on that in various forums. We've got NCCS, which is in a rollout state that's a little delayed. We've got requirements gathering for what; s the acronym NI2 two or NISS 2.0, whichever vernacular. Are there enough resources within the Department to manage those priorities? And if so, just offer the opportunity to comment on it.

Mike F. Sure. Thanks for the question, Greg. And yes, we are working both legacy and NBIS at this point, and we are going to continue to do so for the immediate future. Not seeing a real end date on that. I mean, we do have, you know, decommission actions that are going to be coming out here. They've actually already been posted internally on how we're going to officially transition from one system to another, but we are also keeping those systems in a warm state as we move forward. I mean, there is still some data that we can pull from there and things like that need to be accounted for. You're absolutely correct that while we are going through this, swivel chair process between systems, we do need to have certain functions and fixes resolved going forward. We do have teams that are working on both sides of that, and we're continuing to do that, and we will continue to do that, into the future.

Greg S.: Thank you, Sir.

Heather: Any other questions for Mr. Faller from NISPPAC members? Alright. We will now hear from Mr. Matt Roche, the Division Chief of NISP Operations, Industrial Security, for the Defense Counterintelligence and Security Agency, also known as DCSA. Matt?

Matthew: Good morning. Thank you, Heather. And I want to take a moment to just introduce myself and offer my thanks and recognition to a few folks. So, first I'd like to thank Keith Minard for his nearly 40 meetings that he's supported and attended, and his guidance and leadership as I transition into this new role. Right

now, I'm the NISPPAC alternate, but Keith's been kind enough to offer me up to the director as permanent, but thank you, Keith, as always, outstanding work. Also want to welcome Ike. Ike and I, as is some of my colleagues, are in constant contact. And we will continue to do so, and I believe, we can make a lot of progress going forward, continue the momentum that Heather Sims built. I also want to thank Mr. Bill Lietzau, who's retired from the director position here at DCSA after 40 years of public service. Remarkable three years to include the COVID period, and we thank Mr. Lietzau for his service. And then lastly, just make comment that the deputy director, Deputy Director Leche, who is now our Acting Director, has not missed the beat. He's kept us focused on our strategic plan and our top priorities, and those top priorities, in this culture, values, essentially the people aspect of our mission, and then, of course, integration. But you can see our strategic plan and read it in its entirety online if you're interested in that. But the director has made clear that we're sticking to the plan.

So, again, my name is Matthew Roche, and I work in the Industrial Security element here at DCSA, and you're going to hear from our counterparts, already heard from Mike Faller. Great job, Mike, and I'll keep my comments brief because a lot of information is being put out, and we want to make sure Mike Ray has enough time as well. So, I'm going to talk about, first to say thank you to Mr. Spinnanger for talking about ISLs. I don't have to repeat those comments, but everyone knows where we are with that.

In terms of security reviews, we finished up last year with 3,638, and want to thank Industry specifically for accommodating those security reviews. And overall, it's been a good year. Looking forward to 24. Our expectation is to complete 3,400 security reviews, and in addition to that, working on integrating NAESOC into the oversight process as well. And you'll be hearing more about that later. We do have an ongoing working group with NISPPAC. We'd like to thank them for their service related to our efforts to build a security rating score. We believe that by working collaboratively on this effort, we will be able to get more consistent results and overall raise the security posture of the National Industrial Security Program defense industrial base.

Secondly, in terms of products, and I want to make clear again that this was, one of Keith Minard's efforts, and this was the DCSA Industrial Security began October 1st, sending out what we call the annual industry checkup tool to about a thousand facilities a month. So, the idea being that those facilities that were issued a facility clearance in that month would get a friendly reminder on what we call the checkup tool. So just like as you get notices for your annual checkup with the dentist or the doctor, or for your car, the intention here is to focus on reminding folks of the standards, requirements, related to the National Industrial Security Program. So, we're in our what will be the starting our third month here, and we're looking at some really good feedback from Industry on that and getting some good data.

Secondly, contractor self-inspections. This is another focus area that we internally are focusing on to increase the number of certifications that are uploaded into NISS that validates that the company has completed their self-inspection. We also consider this a focus area, to allow for increased compliance, and a higher security posture over time. As I mentioned with the checkup tool, that'll obviously be highlighted in there as well.

Lastly, CDSE, they continue to turn out some really quality and timely courses. I just want to highlight a couple of those. One is the CS100.CU and that's the Risk Management Framework curriculum. You'll hear from Dave Scott in a minute, but essentially this course was focused in on the Revision 2 of the NIST 800-37, and it prepares you to focus in on the preparatory process that you go through before you enter into the risk management framework, so good stuff there. We also have a SAP course, and OPSEC awareness for military members, DoD employees and contractors, and there's also a series of shorts on CUI. So, kudos to CDSE. I encourage everyone to check those courses out on their website. So, pending your questions. That is all I have for now.

Heather: Alright, thanks, Matt. Any questions from NISPPAC members for Matt?

Ike: Hey, Heather, this is Ike. Hey again, Matt, the cadence that Keith Minard provided, and Heather's timeframe and the cadence that you're providing to sit down with Industry NISPPAC once a month to just collaborate and go over some of these items have been very, very valuable not only to our team, but to Industry. So, thank you for you and your team and, and Keith and his team for putting that together so we can sit down and iron out some things. And thank you for listening to us when it comes to the security review process, right? Industry, it's been one of those talks every year about the security review. And finally, together, collectively, we are working together as a group to try to figure out and fit and fix and make this best for both sides of the ballpark here. So, thank you very much for that. I couldn't let this meeting go without saying that collaboration is very, very helpful. And we will continue to let the industry know as well, right? We know it because we see it and we work on it every day, but it's up to us as well to continue to pass this information down to Industry so they can hear it as well. And we'll continue to do that. So, thank you, Matt.

Matt: You're welcome, Ike. And thank you. And, just for everyone's identification, when we went into COVID, we started a regular monthly cadence to talk to NISPPAC Industry, and we decided it was so valuable that we would just keep that going. So, the first Thursday of every month, we get together and provide each other updates and things that we can help each other with. So, thank you Ike for that. Appreciate it.

Heather: Alright, thanks. Any other NISPPAC members with comments or questions? We're now moving into the portion of the meeting where we get reports from the NISPPAC working groups. However, we'll not be discussing all of the working groups at this time. We have provided slides with highlights of all of them.

You have already heard from some CSAs and CSOs on the high-level points of what was discussed during the Clearance Working Group on September 6th, 2023. We'll also hear from DCSA for their security clearance and information system metrics, along with metrics from DOE and NRC. We are now going to hear from Mr. Dave Scott, the NISP Authorizing Official for DCSA for the Information Systems update. Dave?

Dave S.: Thank you for that. So, I'm on page two of the metrics that were provided for the NISA Working Group. This is a national metrics. I'm not going to go through each and every one of these, but just want to kind of call out a few things. Our registered systems and eMASS stays steady, at around 5,500. Want to give kudos to Industry for continuing to work through decommissioning or when as systems are no longer contracts required or expired, continuing that step seven of the risk management framework to decommission those systems as appropriate. That really helps us keep our database clean and our accurate number of responsibilities within our portfolio. So, thank you for that. The other thing that I'll kind of call out here, these metrics are FY 23, is the authorizations process in FY 23 is around 2200.

Historically, we've been closer to 2,900, 3000. And that's in large part because the packages are much better within Industry. And we're able to get onsite at a more aggressive pace in the last year and doing more full three-year authorizations and reducing our conditional authorizations, which has been a goal of ours. So, I think that's a great effort on both Industry and DCSA, reaching the goal of those three-year authorizations, and reducing a lot of the administrative paperwork as that is as a result from the conditional ATOs. And then at the bottom there, DCSA Days for Authorization Decision. We have been averaging, as you see the 49 there, we average between 50 and 55 throughout the year, but as of the date of this report, it was 49 DCSA days. So, we're getting a really good battle rhythm moving forward with our systems and our goal of reaching a decision within 90 days. And our extensions, workflows, that's a tool in the toolbox of the regional authorization officials, in large part working with Industry, for whatever reasons the right and the ability to create an extension, when appropriate.

So next slide. Working from slide three is the triage metrics. This is where the contractor staff are following the job aids that are published, and some metrics on the first step when we get the packages in through eMASS. This is FY 23 numbers. We processed about 6,700 triaged, about 6,700 packages, and you can kind of see the breakout there for complete return, for rework, and no triage conducted. The no triage conducted is when a package is already passed that phase, and working directly with the ISSP, we don't want to waste time. That's something that's already been done. So, we pass that triage and go straight to the ISSP when we're already working on a package. And the bottom left-hand corner is the top 3 issues sent back for rework. Those have been steady, and those are typically incomplete or missing information from the implementation plan or artifacts such as a DD254, et cetera, workflows not initiated. So pretty standard there. In the bottom right-

hand quarter from the triage metrics, one thing that I'll kind of call out is the average completion time. You'll see kind of from FY 21 through FY 23 we've gotten the triage team has got a turnaround time of three days, and there's a couple of reasons for that. One, the triage team is really starting to understand the RMF process and the expectations, and they're getting very familiar with the system and what they're looking at, but two, in large part because Industry's providing a lot better products over the years, and so, I think, outstanding, timeline there, for that first step, which makes our time conducting our assessment and our risk assessments from a plan review and an onsite review much faster turnaround time, contributing to that. The other thing that I'll call out is the return for rework. You see, that's a little bit higher than normal. It says 31%, and that's due in large part to eMASS releases that we put out there. And then sometimes we change some information on what is required, so sometimes we go through those changes, there's a little bit of an increase in return to rework, but no alarm there. That's just kind of normal.

And then I'll move on to the final slide there. It's really just two topics that we've been tracking at a national level in close collaboration with the NISA Working Group, and I should have started with kudos to Mr. Sadler and the NISA working group team. The collaboration over the last couple years has just been outstanding and tremendous, in some of the accomplishments that we've made. And I'll highlight a couple of things here. I'll start with the the NISP assessment authorization process job aids and templates. This is the new name for the DAAPM. We renamed it to more closely align to what it really is, it's a job aid and a template, and, through this, we've reindexed, or we reformatted the document to make it easy to identify exactly what a stakeholder would need, if they need to a template on a hardware baseline or a software baseline, they can easily identify that and pull that out. The NISP Connection Process Guide is within as an index as well. That's a much-anticipated document that what's already been pre-coordinated with the NISA Working Group. So, the document has been sent over to the NISA Working Group and we're currently awaiting comments before we start our formal coordination through the process. So, I really want to thank Mr. Sadler and the team for taking the time. I know it's a big lift, but we really appreciate you taking the time to look at that and let us know your feedback. So, look forward to that. And then in NISP cloud capabilities, this past fiscal year, we've had some great success. We've navigated some challenges, and as you all know, we've had some success and we've authorized a system within the isolated secret region. We've documented our success through a job aid that we coordinated with DCSA, and that is now available as of about a month ago within eMASS. So, it's a high-level document, about a two-page document, that that can help point for Industry stakeholders and government stakeholders, how to request and kind of the requirements to request a cleared contractor isolated secret region environment for assessment authorization through DCSA with the cloud vendor that's authorized. So, if there's any interest there, please look and give us any feedback that you have as well. But that's all I've got pending any questions, from the group.

Heather: Alright, thank you. I appreciate that, Dave. Alright, we're now going to hear from Mr. Mike Ray, the Deputy Assistant Director of Operations of Vetting Risk Operations with DCSA for their vetting statistics. Mike?

Mike R.: Alright, so good morning, everybody. First off, just want to kick it off by saying, always appreciate the collaboration and partnership with the NISPPAC team. So, really appreciate that as we walk through different things with this and that kind of thing.

So, looking at the slide here. So, we'll start off in the end-to-end timeliness for T5 initials. This is for FY 23, Q4. 20 days for initiation, 134 days for investigation and 16 days for adjudication. So that end-to-end time is 170 days. For T3 initials FY 23, Q4, it's going to be 18 days for initiation, 62 days for investigation, 20 days for adjudication. That end-to-end timeline is 100 days. 90% of all initial investigations had an interim termination made within seven to 10 days. If you look at the chart on the top left, which shows the current adjudications inventory at 2,400, and then the chart on the right shows the total investigation inventory for T5 is at 18,500. T3 is at 18,300, and you can see the breakdown of the total adjudication inventory T5 is at 400, the T3 is at 1500. For reciprocity, I certainly appreciate the comment earlier today by Jane. The CAS continues to deliver the reciprocity decisions at an average of one calendar day. For Industry conditionals, we coordinated between VRO, the NISPPAC, and the DoD CAS, and identify the process to issue conditional national security eligibility determinations. These conditional support mission readiness by removing a case from due process and using continuous vetting to monitor compliance and support risk mitigation. DoD CAS plans on beginning to issue the conditional in Q1 FY 24. The Industry specific communication materials are currently being finalized. We did share that within NISPPAC team, received some comments, and just finalizing that, and as soon as that's completed, we'll distribute that out to Industry and across the department once available. For the DoD CAS call center, so, as part of identifying synergies between VRO and DoD CAS, the DoD CAS call center started answering inquiries from Industry on PCL VRO statuses on October 1. The DoD call center phone number is (301) 833-3850.

And then transition over to CV Alert Management. So, post CV enrollment, alerts are generated based on established thresholds which align with the federal investigative standards and adjudicated guidelines. CV is impactful as we average the 6% alert rate. Criminal and financial are the most common valid actionable alerts. Thus far, in FY 23, VRO received 28,000 Industry alerts, of which 13,500, or 48%, were not previously known. And that's from 22,000 unique Industry subjects. Just note that this information should have been self-reported, and as we know, our goal moving forward is to have individuals self-report information, as it occurs. And that's all I have for the group, and I'll pause here for questions.

Heather: Thanks, Mike. Any questions for the VRO with DCSA from NISPPAC members? Alright, we're now going to hear from Ms. Natasha Sumpter, the

Program Planning and Management lead with the Office of Security Policy, Department of Energy. Please provide your metrics.

Natasha: Thank you, Heather. Good morning NISPPAC members and participants. As always, it's a pleasure to have this opportunity to provide the Department of Energy's policy updates and updates on our personnel security investigations process, metrics, and timelines. On behalf of Mr. Mark Hojnacke and Mr. Tracy Kindle, thank you for giving the Department of Energy the floor. The Office of Insider Threat Program just broke ground on rewriting DOE Order 475 entitled Insider Threat Program. Just two weeks ago, the Insider Threat Program formed an integrated project team working group that is reviewing the current order to identify focus areas and priorities. If all goes well with this aggressive timeline, they anticipate publishing the new order before next fall. The Department continues making progress with rewriting DOE 470.4B entitled Safeguards and Security Program. The directive is being superseded by two new orders, Safeguards and Security Program Planning and Safeguards and Security Program Management Operations. The latter of the two impacts Industry most of all. That's where we have our facility clearance, FOCI, and other NISP related activities outlined, excuse me, I'm so sorry guys. I am recovering from a sinus infection, so I'm still a bit nasal. So, continuing, the two drafts are being developed via the integrated project team process as well, and both teams have developed and are reviewing their drafts and preparing to coordinate the drafts for departmental review. We will continue to provide updates via this forum as we meet milestones that impact the greater community.

Now onto the slides. So, I'm providing this update on behalf of Tracy Kindle from the Office of Departmental Personnel Security. A special thanks goes out to DCSA for providing the metrics that I will discuss. So, onto slide two. Overall, DOE continues to meet the IRTPA goals and average over the past four quarters with an average of 10 days for initiation and 17 days for adjudicating. The investigations on slide three, DOE continues to exceed the average initiation and adjudicated goals for the year. And as you can see on slide four, we met and exceeded the initiation and adjudicative goals for the past year. On slide five, over the past four quarters, DOE continues to meet average initiation and adjudication goals, but did have a few bumps in the road during the past winter. We expect the trends over the last five months of this year to continue. On slide six, overall DOE continues to meet the IRTPA goals on average over the last four quarters with an average of seven days for initiation and 10 days for adjudication. And as always, if our Industry partners have any questions, please do not hesitate to reach out and we are ready to assist. Thank you for this opportunity, and I concede the floor back to Heather.

Heather: Alright, thank you. Are there any questions for the Department of Energy? Alright, Mr. Chris Heilig, Chief, Personnel Security Branch with NRC, please provide your update.

Chris: Good morning, everybody. This is Chris Heilig from the NRC. The NRC doesn't really have any updates this time around. I wasn't going to go slide by slide, but if you take a look overall, we're meeting our adjudication timeliness numbers, and I'm happy to report that our personnel security office is now fully backfilled with FTEs, so we fully anticipate to continue hitting those targets, if not improving on those numbers. We are fully compliant with the Trusted Workforce Initiative and ramping up enrollment of the Nonsensitive population. That's really all I have for you this time around, but I'm happy to entertain any questions.

Heather: Thanks, Chris. Any questions from the NRC? We will now hear from Mr. Perry Russell-Hunter, the Director of the Defense Office of Hearings and Appeals, also known as DOHA.

Perry Russell-Hunter: Thank you Heather. This is Perry Russell-Hunter, and I can promise that my update will be brief because it is all good news. The established administrative process for Industry clearance eligibility continues to perform as designed, and, this is for not just DoD Industry contractors, but for the Industry contractors for 32 other federal departments and agencies. Currently in legal review, we have 322 Statements of Reasons. That is a normal workload, and so what that means is that we are current in terms of the legal reviews of the Statement of Reasons, which is the notice document. It is how the DoD CAS and DOHA inform the individual of the security concerns, and so it's very important that those get out timely and we are timely on all of those. We completed 2,164 legal reviews of Statements of Reasons in fiscal year 2023. Again, that is a normal amount. What this tells us is that while CE/CV is allowing us in the government to get to the adverse cases faster, in the past I've used the analogy of finding the needles in the haystack faster, we may have made the haystack slightly bigger with CE/CV, but we're also finding the needles faster, and that at least based on the numbers we're seeing, that isn't creating a significantly larger number of denials or revocations, we're just getting to them faster. As Mike noted on behalf of the CAS, the commencing the use of conditionals, conditional grants of eligibility by the CAS is something that we at DOHA fully support. And we've spoken about this at past NISPPACs, because this will not only reduce risk and improve and enhance national security, it will also enhance readiness by enabling people to get to work or stay at work, where the issue bears monitoring and CE/CV allows for that, but we can let the person continue to work, so the move to conditional eligibility for Industry is a great improvement by the CAS, and we applaud the CAS for stepping into that realm. It's one of the reasons why I continue to predict that the number of denials or revocations we see should remain fairly constant.

But speaking of getting to adverse cases faster, DOHA is leveraging MS Teams to conduct more hearings by remote video. In fact, for the first time ever, DOHA is now holding more hearings over Teams than in person, but DOHA's independent administrative judges are still able to convene in person hearings, whenever and wherever we need to, in fairness to the individual, or where the case calls for it. Generally, that is with multiple or more complex witness testimony or more

complex issues or where credibility is a central issue. To the extent that DOHA's independent AJs are in the spotlight, probably the biggest news for them is that all DOHA's administrative judges and appeal board members have now been appointed as constitutional officers by Secretary of Defense Lloyd Austin. This is the result of a series of Supreme Court cases in which the Supreme Court determined that making these kinds of independent decisions, particularly after fact finding hearings, require constitutional appointment, and so DOHA has done that. Secretary Austin has appointed each of our administrative judges and appeal board members, and again, this is to enhance their independence and accountability. With that said, I now yield the rest of my time back for any questions.

Heather: Alright, thanks Perry. It sounds like we don't have any questions. We are now at the point of the meeting where we ask for NISPPAC members to present any new business they have. Anybody?

Greg S.: Hi there, this is Greg Sadler. It's not new business. I just wanted to look back to the NISA Working Group content from Dave Scott. I was fighting the mute button and failed. All the points that Dave mentioned regarding the cloud capability and the engagement with Industry are spot on and we appreciate that some of the bumps that the team experienced during the pilot are being worked through, and to smooth out that process and take the continued feedback on how to make the replication of the cloud solutions easier for both Industry and the government. The DAAPM replacement, we expect to have content or comments back to Dave and his team, by the end of the month. That's our goal to provide that feedback. One item that's already on the surface is come up with a better name. The DAAPM flowed very easily. This one is a bit of a full mouth to get out. And then the one item that Dave's team is already working on, and we hope that the DAAPM replacement and updates will further contribute to is consistency across the field, both at the AO level is greatly improving, but down at the individual ISSP level, David and his team have taken an initiative to try to drive more consistency there. It's definitely needed as the field deals with multiple locations within a single company and conflicted guidance. But again, Dave's team has demonstrated ownership in that and they're working with us and we're providing that feedback where possible.

Heather: Thanks, Greg. Do any other NISPPAC members have any questions or remarks before we close out the meeting? Alright, in the interest of time, we're not going to take any more participant questions, but please ensure that questions and comments were sent via Webex's chat feature or emailed to NISPPAC@NARA.gov so that they can be answered. As a reminder, all NISPPAC meeting announcements are posted in the federal register approximately 30 days before the meeting, along with it being posted to the ISOO Overview Blog. Our next NISPPAC is scheduled for May 1st, 2024. Meeting adjourned. Thank you everybody for your time. Bye-Bye.