Producer: Welcome, and thank you for joining today's NISPPAC meeting. To receive all pertinent information about upcoming NISPPAC meetings, please subscribe to ISOO Overview at isoo-overview.blogs.archives.gov or by going to the Federal Register. All available meeting materials, including today's agenda, slides, and biographies for NISPPAC members and speakers have been posted to the ISOO website at archives.gov/isoo/oversight-groups/nisppac/committee.html and have also been e-mailed to all registrants. Please note, not all NISPPAC members and speakers have biographies or slides.

While connecting by phone is necessary to attend today's meeting, there is no requirement to log on to WebEx, however, you are welcome to join WebEx with the link provided with your registration, as all available materials will be shared during the meeting on that platform. If you have connected through WebEx, please ensure you have opened the participant and chat panels by using the associated icons located at the bottom of your screen.

If you require technical assistance, please send a private chat message to the event producer. All links will also be shared periodically through WebEx chat. Please note, all audio connections will be muted for the duration of the meeting with the exception of NISPPAC members, speakers, and ISOO.

We are expecting a fairly large audience today. Because of this, we will not be taking questions from the public. Please email your questions and comments to nisppac@nara.gov and someone will get with you offline. Only ISOO and NISPPAC members will be authorized to ask questions throughout the meeting.

At the conclusion, a survey will be sent for your 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. With that, let me turn things over to Mr. Mark Bradley, the Director of the Information Security Oversight Office, as well as the chairman of the NISPPAC.

Mark Bradley: Thank you very much, Madam Producer, I appreciate that. Thank you for your kind production. Morning everybody. Welcome to the 66th meeting for the National Industrial Security Program Policy Advisory Committee, commonly known as the NISPPAC. This is the third NISPPAC meeting that's been conducted 100% virtually, although we now understand some people are home, like we are, and some people are at work, actually in the office.

This is a public meeting. Like our previous NISPPAC meetings, this one will be recorded. The recording, along with the transcript and minutes, should be available within 90 days on the NISPPAC Reports on Committee Activities webpage mentioned earlier by our event producer. We're planning on a five minute break in middle of the meeting, so I'll flag it as we move closer to that.

I will now begin attendance with the government members. I will state the name of the agency and the agency member will reply by identifying himself or

herself. Once I've gone through the government members, I will then proceed with the industry members. After the industry members, we will easily move into our speakers. Let me start with the ODNI.

Valerie Kerben: Good morning, Mr. Chair.

Mark B.: Morning.

Valerie: I'm Valerie Kerben.

Mark B.: Hi, Valerie. Department of Defense?

Jeff Spinnanger: Good morning, Mark. This is Jeff Spinnanger.

Mark B.: Morning, Jeff. Department of Energy?

Mark Hojnacke: Good morning. This is Mark Hojnacke.

Mark B.: Morning, Mark. NRC?

Dennis Brady: Yes. Good morning everybody. This is Dennis Brady with the NRC.

Mark B.: Morning, Dennis. DHS?

Rob McRae: Morning, Mark. This is Rob McRae and Rich DeJausserand.

Mark B.: Morning, gentleman. DCSA?

Keith Minard: Good morning, Keith Minard, DCSA.

Mark B.: Morning, Keith. CIA? It still appears we're missing a rep from the agency. Department of Commerce.

Robert Tringali: They sent an email. They're not going to be able to make it.

Mark B.: Okay. Department of Justice?

Kathleen Berry: Good morning, Mark. Kathleen Berry standing in for Christine Gunning.

Mark B.: Hi. Good morning. NASA?

Kenneth Jones: Good morning. Kenneth Jones with NASA.

Mark B.: Morning, Kenneth. National Security Agency?

Brad Weatherby: Good morning. This is Brad Weatherby from the National Security Agency.

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

Kim Baugher: Good morning, this is Kim Baugher from the State Department.

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

Jennifer Aquinas: Good morning, Jennifer Aquinas here from Department of Air Force.

Mark B.: Morning. Department of the Navy?

Jennifer Obernier: Good morning. This is Jennifer Obernier with Department of Navy.

Mark B.: Good morning to you. Department of the Army?

Jim Anderson: Good morning everybody. This is Jim Anderson from Department of the Army.

Mark B.: Morning, Jim. Right, now I'm going to turn to our industry members. Heather Sims, are you present?

Heather Sims: Heather Sims is present.

Mark B.: Okay. Dan McGarvey, are you present?

Dan McGarvey: Dan McGarvey is present. Good morning, Mark.

Mark B.: All right. Morning, Dan. Dennis Arriaga?

Dennis Arriaga: Dennis Arriaga is present. Good morning.

Mark B.: Morning, Dennis. Morning to you. Rosie Borrero?

Rosie Borrero: Good morning. Rosie Borrero's present.

Mark B.: Okay. Morning, Rosie. Cheryl Stone?

Cheryl Stone: Cheryl Stone is present.

Mark B.: Okay. Aprille Abbott?

Aprille Abbott: Good morning. Present.

Mark B.: Morning, Aprille. Derek Jones?

Derek Jones: Derek Jones is present.

Mark B.: Great. Tracy Durkin?

Tracy Durkin: Good morning. Tracy Durkin's present.

Mark B.: Good morning, Tracy. Right. Now I'm going to do just a very quick roll call for our speakers. Make sure everybody's here. All right. Stacy Bostjanick?

Stacy Bostjanick: I'm here.

Mark B.: Great. Perry Russell-Hunter?

Perry Russell-Hunter: I am here.

Mark B.: Great. Roy Jusino?

Roy Jusino: Yes. I am here.

Mark B.: Great. Chris Pollock?

Chris Pollock: Good morning. I'm here too.

Mark B.: Great. Marianna Martineau?

Marianna Martineau: Good morning. I'm here as well.

Mark B.: Okay. Heather Green?

Heather Green: Good morning.

Mark B.: Morning to you. Heather Mardaga?

Heather M.: Good morning.

Mark B.: Morning. Sheldon Soltis?

Sheldon Soltis: Good morning.

Mark B.: Morning. Charles Tench? Matt Roche?

Matt Roche: Good morning.

Mark B.: Morning, Matt. Jason Theriault?

Jason Theriault: Good morning.

Mark B.: Morning to you. Booker Bland?

Booker Bland: Good morning.

Mark B.: Morning, Booker. David Scott?

David Scott: Yes. Good morning.

Mark B.: Morning to you. Selena Hutchison?

Selena Hutchinson: Good morning everyone.

Mark B.: Morning to you. Evan Coren?

Evan Coren: Morning.

Mark B.: Alright. Rich DeJausserand?

Rich DeJausserand: I'm with DHS, but yes, I'm here.

Mark B.: Great. Morning. All right, is anyone else speaking from the NISPPAC that I have not heard from or that I do not know about? If so, please speak now. All right. We request that everyone identify themselves by name and agency before speaking each time for the record. Because again, what this is, as you all know all too well, this is recorded and we have a transcript. So it's much, much easier on us transcribing if we can actually match a name with the spoken words. So with that, let me give you just a couple of updates.

We've had a few changes to the NISPPAC membership. We'd like to welcome alternate Natasha Sumpter with the Department of Energy. Tracy Kindle also remains an alternate. Additionally, we'd like to welcome Elizabeth O'Kane representing the Army, and Robin Nickel, alternate with the Navy. For two of our industry members, this is their last NISPPAC meeting as members, Dan McGarvey and Dennis Arriaga. Gentlemen, thank you for your service. I mean, you've really made some really nice contributions and we are most grateful for your service. Alright, with that, I'm going to turn it over to Greg Pannoni, who is my deputy, who will address the status of action items from the November 18th, 2020 meeting. Greg?

Greg Pannoni: Thank you, Mark. Good morning everyone. We just had a couple of items, but before that, I want to mention that the NISPPAC minutes from the last meeting were finalized on January 26th and were posted to the ISOO website on February 2nd.

As far as the two action items, they both were with the DCSA. The first one that's outstanding from the last meeting was the Industrial Security Letter. We refer to them as ISLs, and this one was on insider threat and it will replace ISL 2016-02. It's in a bit of a holding pattern due to the release of the NISPOM rule, but DCSA will continue processing the ISL for issuance and begin engagement with cleared industry through the NISPPAC to update tools, resources, and required training with respect to the insider threat ISL. The second action item

still open has to do with DCSA providing an update on their responsibility for accreditation of sensitive compartmented information facilities, otherwise known as SCIFs, and DCSA will be responsible for the accreditation of military departments SCIFs, 4th Estate SCIFs, and contractors SCIFs that fall under DCSA. So do any of the NISPPAC members have any questions about the action item status? Okay. Thank you. Back to you, Mr. Chair.

Mark B.: Sure. Thank you, Greg. Now at this time we'll go to our speakers. My first one is Ms. Heather Sims, the NISPPAC spokesperson who'll provide the industry update. Heather, all yours.

Heather: Good morning. It's a pleasure to provide industry's collective perspective today on a variety of NISP topics and priorities for 2021. Even though it's only April, it's not too early for industry members that are interested in serving as a NISPPAC industry member to start thinking about whether you want to throw your name in the hat. We have September elections coming up very fast. If any industry partners are interested, contact a current NISPPAC industry member, or an MOU member. Industry continues to increase their engagement and collaboration with a variety of government agencies in order to be more actively involved in our national security role. Industry cannot be a sometimes stakeholder partner. NISPPAC industry members, along with MOU industry association members, continue to work tirelessly, fostering relationships and trust in order to bridge the gaps between government and industry. Adapting the change has become industry's middle name. (Silence)

Mark B.: Did we lose Heather?

Greg: Heather, are you there?

Producer: We may have.

Mark B.: Hello?

Producer: Yeah, I don't see her line at the moment. I think it may have.

Mark B.: It just fell, I guess.

Producer: Yeah, I think it may have dropped off.

Greg P.: Maybe go to Jeff and come back.

Mark B.: Alright. Jeff, I'm going to bring you out of the bullpen.

Jeff: Alright, Coach.

Mark B.: All right. So anyway, we're going to, as we try to resurface Heather, we're going to turn to Jeffrey Spinnanger, Director for Critical Technology Protection for the

Office of the Under Secretary of Defense for Intelligence & Security, who will give you an update on behalf of DoD as the NISP Executive Agent. Jeffrey, all yours.

Jeff: Well Mark, thank you very much for that, and should Heather come back on, I'm more than happy to go back into mute mode and let her continue, but thanks for that and thanks for the opportunity. As ever, today it's pretty remarkable how we're been able to adapt and execute in this remote environment. I'm pretty sure I said the last time and I'll continue to say, however, I look forward to the opportunity for us to get back in a room together, both for the sum and substance of the official portion of the meeting, but frankly for the candid conversations that happen in and amongst the women and men who participate in these meetings. I think they're very, very important and something I'm looking very forward to being on the receiving end in the future.

So with that, our update today. I have a number of things to go over. Some I'll hit the wave tops on, deferring much more so to some detail that'll come later in the brief in the meeting today, principally from Keith Minard and others at DSCA. But the alligator that's been nearest our boat or in our boat here for a good long while is now, or shortly to become, I don't know, mounted or at a zoo someplace or something, but the NISPOM federal rule became effective on February 24th, and as many of you know, that is a years long undertaking that our office and principally Valerie Heil and many, many others have been patiently and persistently, I think the technical term is slogging through, for what amounts to several years.

It's a big deal. I know I said in a prior meeting when we were forecasting this, I will continue to say it, much of the sum and substance of the NISPOM remains unchanged. There are a number of elements that many of you are becoming aware of now that have, but the biggest single takeaway, our single sentence that we continue to champion here within the building is that it creates more accountability on government, and we think that that's really critical. It's the key to consistency where the program itself is intended to be and that is an industry, right? So it's not a hard sentence to get through. It's going to be very, very hard and challenging in execution, but we're very excited at the prospects of actually getting to that execution layer here later in the year.

We are adjudicating a number of comments that did come through in the public period. I think in total, we received 84 comments. And just because we're metrics driven around here, just wanted to give some context to that, to our leadership. About 60% of those came in as a collective submission from our NISPPAC industry partners. And honestly, I cannot thank you enough for that, alright? So the due diligence that we undertake to be able to go through each comment is a very deliberate process. And our accountability is, frankly, to people who don't know a whole lot about the NISPOM, right? Their expertise is in policy, right, federal regulatory policy, and being able to make it through what amounts to an audit by them, requires…. It's not an easy undertaking. And so the work that was done by Heather and the other industry folks to consolidate

inputs before they ever got to us through the formal process will absolutely save us a tremendous amount of time, and it really speaks to the collaborative nature of the NISPPAC, I think, and its intent, but more than that, in its execution, and I really do thank you a lot for that. We're an army of about three and one of those is me and I just sort of nod up and down like a bobble head when we get into much of the details. And so it's kind of...it's very, very important to have that partnership and to really call it out. Bringing down those 84 comments a little bit, the key issues that we're presently adjudicating are reasonably summarized as focused on SEAD 3. Certainly going to hear more about that. I anticipate that when Heather rejoins this, that she'll have some comments, and I know that Keith will as well. Further guidance with respect to trusted workforce, and continuous, NIDs and Section 842 made a small resurgence in the discussion, and clarification with respect to safeguarding. So we're preparing a proposed amendment to the rule to address each of these comments and resulting changes. This will go through a DoD internal coordination and on to OMB review for about 90 days. And there's some fudge factor in those timelines. The OMB collects these sorts of issues and processes from across the federal government, and so while it's hard for us to imagine any more important than the Industrial Security Program, I think it's fair to say that there's more than one thing going on, and that's where inner agency review comes in. So all that in mind, we can't really give a specific timeline to how that will unfold. We probably put ourselves on a spring glide path. I think we'd have some pretty firm timelines to be able to provide were we to meet in July, but in as much as we're not going to do that, we will provide update through the working groups as they continue to happen.

So I mentioned the SEAD 3 ISL that came out. Went out for NISPPAC comments. We've gotten those back. They are extensive. We thank you for those many comments that came in from industry and government alike. There's a lot in there. There's a lot to unpack. A lot of focus on the implementation timelines that are getting a lot of attention right now. We'll keep you updated on those. I think, like I said, Keith may have a few more comments on, I'm not sure, but we're trying to continue a steady drum beat that we can all maintain the ISLs, not new. So as we start to make progress and come to common understanding with respect to implementation, that is a team sport, and one that we'll continue to follow that known forward. A word on the ISL, right.

And again, you'll hear more about ISL processes generally, but one of the changes by virtue of the issuance as a federal rule, is that OMB...so our issuance of Industrial Security Letters, although ultimately approved by and will be issued, as has been our practice by the Under Secretary, we need an OMB coordination before that happens. And so that's another step in the process. And so the first one will be a bit of an experiment, and that should inform what our recurrent processes will look like for subsequent Security Letters. There's been quite a bit of discussion with respect to federal information systems and this specific term. A lot of questions regarding the policy on information in Federal Information Systems as it's described and defined within volume two of the DoD manual. We believe the term Federal Information System itself is a

source of some confusion. In the past, federal information systems were previously referred to as guests systems, which meant a system approved by another government organization. DCSA has authorized federal systems in the hands of cleared industry for many years, however, some government customers are reading the volume two federal information systems paragraph as the only way to adhere to policy for their systems, which we think is not really the case, so we're kind of sifting through that. Folks are trying to be as deliberate as possible, but with the heavy and increasing reliance on extensions of systems of this type. We're looking to work through and come to common understanding policy clarification where necessary. At this time, however, as industry or government customers told to disconnect a previously proved system, please raise the issue with the regional authorizing officials who will engage this directly, right. So happy to take questions on that, and address concerns either here today, or of course, through the working group as it goes forward. Discussions regarding Solid state device sanitization, destruction policy, largely deferring at this point to NSA for any further guidance in future NISA working group meetings on the topic. For industry, they don't need us to speak for them, but I think it bears mentioning that DCSA follows volume two guidance, which does allow some flexibility for the government information owner to accept a risk of sanitization risk, rather than destruction. We recommend, however, if industry has specific sanitization products or questions that you would like to address or utilize, that you either submit them directly to NSA for evaluation or speak to your government customer for further guidance.

Couple more topics that are really kind of growing near and dear to us here: I mentioned last time, Section 847, and FY20 NDAA includes a requirement for assessment of beneficial ownership pertaining to foreign ownership, control, and influence for DoD prime and subcontracts that are more than $5 million in value. It will require a DFARS clause that will go through the rule-making process, however, in advance of that process, DoD right now is in the nascent stages of a draft DoD instruction. It is presently in the internal coordination phases within the DOD components under OUSDI&S. From there, it will make its way out through and into the formal issuance process. There's a lot of congressional attention on this particular issue, FOCI and Supply Chain Risk Management, which Stacy Bostjanick is going to go into quite a bit more detail on, I think, in her briefing here later. These are near-synonymous terms, right, and a source of tremendous amounts of interest. So this particular one, the expansion of FOCI pretty comprehensively is something that is garnering the interest as you would imagine. For our purposes, like I said, this begins through the issuance process to define kind of how we would get after the provisions that are within the NDAA and left, right rudder guidance, as it were, for DCSA as the executing agency. Honestly, that's where the real work begins. So as it continues to unfold, we'll certainly be looking for government and industry inputs on this very, very important topic.

Last two things I'd like to get into, one is a little bit...I don't try to do a whole lot of forecasting, but one thing I'd like to put out there, right, so our office within OUSDI&S is the sponsor of the University Affiliated Research Center called the

Applied Research Laboratory for Intelligence and Security. At some point, some of you may have some familiarity with this. I don't want to spend a lot of time, I'm just about out of time myself, but I wanted to put out there, right, kind of a nod back to the discussion on information systems earlier, but we're sponsoring a project up at ARLIS right now that I want to put out here for just public awareness, and that'll tee us up for more substantive reporting on this project when we're next together in the fall. But in short, we're exploring the use of commercial classified cloud in the NISP. ARLIS is going to conduct a pilot, working with a small number of NISP companies to independently evaluate the connections and approvals process. Project builds on observable improvements to inter-operability, cybersecurity, and core requirements for information security in insider threat. User activity monitoring for highly classified IC and DoD requirements pertaining to compartmented programs that are already in work today, and exploring how those can meet similar application and requirements are presently executed under the NISP. We think there's a lot there. There's basically cloud in the most highly compartment aspects of work done in industry, and there's certainly cloud within the unclassified space. The opportunity to explore the same options kind of in the expanse of the Industrial Security Program is something that we think there's quite a bit of potential there. We look forward to leveraging what we have up there and a pretty powerful tool in ARLIS to showcase kind of the...I'll call it the good, the bad and the ugly.

Then finally the last thing, I think you'll hear a lot more about, right, operating within a COVID environment. Mark did mention that some folks, there is a slow returning to work. God help me, but I'm happy to be saying, and I'm sitting in the Pentagon on the call today. Now remind me, I said that maybe in November, but it is nice to be back to work with some regularity, right? The work didn't go away, and that's true for everyone out here. But one of the things that we continue to look at and continue to capitalize is, right, this environment has forced us to find ways to get work done. And in some ways really confront some of the kind of long-standing processes that we've undertaken, and evaluate whether or not those are the right ways to do business, I think they're certainly the way that they're defined, but are they the right and best way to manage risk as it pertains to general security, but with an eye for industrial security. I think we're looking to capitalize on what lessons we are learning, to make revisions in policy and get better at really defining what our requirements are, and executing against those requirements in the future. So that's kind of my minor soapbox moment, but I am right at my 15 minute mark, so I'm going to stop right there and turn it back to you, Mark. Thank you very much.

Mark B.: Okay, anyone have any questions for Jeff before we let him off the hook here? Okay. Hearing none. Is Heather Sims back?

Greg: Yeah, she's back, Mark. Yep.

Mark B.: Heather, would you like to pick up where you left off?

Heather: I'm back in and I think I was talking about adapting the change and I have to continue to do that as technically challenged.

Mark B.: Yeah.

Heather: So I am back in and thanks for that update, Jeff. That was great. I was wondering how DoD would take industry having so many comments on the ISL, so I was pleasantly surprised when you mentioned that you appreciated the feedback, so thank you for that. So I'm briefly going to talk about our current top three industry priorities in some of our watch list items. They're listed on the slide, but I'm not going to talk in any particular order. The long awaited new 32 CFR Part 117, the new NISPOM, is currently a major focus of industry while we move to implement and also adjust to the new changes. I would like to say thank you to DoD and DCSA for your early and meaningful industry engagements. The more industry engagements are the better, in our mind. We look forward to hearing from the other CSAs today, how they plan to implement oversight of the new NISPOM declared industry. I would also encourage my industry partners to actually read the new NISPOM yourself, and don't make assumptions what's there and what's not there. We also look for more engagement with PACPMO, ODNI, and OPM as trusted workforce continues to mature. Information sharing continues to be a challenging item for industry. While some of my industry members focus specifically at improvements within the intelligence community, it's a much wider impact on all of industry. Industry often has to manage the security programs blindly. Industry is challenged with sharing of adverse information of our cleared employees, potential insider threats identified by the government, target threats against our companies, and our products and services we provide to the government. Industry is charged with protecting against threats. So we would like to have engagements with our government partners to talk about how we can increase information sharing. The industry's also challenged with being able to share known threats between companies without fear of reprisal and lawsuits. Information sharing with industry holistically is a challenge and improvements would only strengthen our ability to provide better security mitigation strategies with the included industry.

I'll touch a little bit on supply chain. It's been a hot topic for many years, but we're seeing a lot of action in the implementation of many statutory and regulatory requirements embedded into the acquisition process. It's not necessarily NISP focused, but there's a direct impact to the NISP at large and the supply chain of the NISP. As government begins to get back to normal, industry understands there will be fundamental changes to how we operate. Many industry partners will continue to operate virtually for the foreseeable future, while others begin the process of bringing remote workers back to the offices and some variations in between. Industry does look forward to hearing from the five CSA's today on the return to work plans and how industry can be prepared as we anticipate a return to in-person oversight visits.

Now, I would be remiss if I didn't mention the recent JPAS to DISS transition. While this wasn't easy by any means, I will say we had a lot of pain points, and a lot still exists, there's still quite a few lessons learned. Thanks to Sheldon Soltis for truly listening and working on fixes for Industry's concerns, with the continued issues with functionality of the system and data integrity, with a sense of urgency. We've heard a lot of excuses of why the process went so poorly, but the bottom line is we can't allow this to happen again. One, if not the largest government system utilized to verify and validate eligibility and access level, it's still not where it should be operationally and we're already talking about its replacements. While industry has started NBIS engagements with government partners, industry will not let up when requests for a strategic rollout plan, increased communications, training, and understanding of how industry will utilize the system. Industry understands we're not alone with exerting an enormous amount of resources and validating correctly this information, but we have to do better. Industry is preparing for the implementation of a new NISPOM, managing and validating and correcting data in DISS, anticipating such a workforce 2.0, preparing for CMMC assessments, and trying to manage the role of controlled unclassified information (CUI).

While we are often reminded that CUI is not the NISP, there is no doubt an impact to clarity industry and will continue to be impacted by CUI implementation oversight. We're already experiencing a bifurcation of the programs. Each federal agency has been charged with developing a program, but when what industry is dealing with is an interpretation of implementation strategies that vary by government agencies. Each program, each base, is coming up with their own set of rules, leaving industry in the middle of managing expectations. Industry only has so much time and resources to manage their programs. We need better oversight of government agencies to ensure consistent approaches levied on Industry. With continued engagement, a shared respect between government and industry partners, we can strengthen our NISP. Protecting our economic prosperity. We can see our warfighting competitive edge of our adversaries. With industry, we can help ourselves by continuing to be united in our Industry priorities with the government partners at a strategic level. Understand we can be better together than simply our own individual company interests. Most important, we stay informed, stay connected and stay engaged.

As I conclude, I'd like to thank the Industry partners and the government partners for increasing our engagement this past year. Thanks for your time today. And I look forward to a strengthened relationship. And most importantly, I look forward to in-person meetings again, so I don't continually drop calls. Thank you.

Mark B.: Okay. Thank you. Anyone have any questions for Heather? Thank you, Heather. I'm glad we got you back. We'll now hear from Mr. Keith Minard, Senior Policy Advisor with the Critical Technology Protection of the Defense Counterintelligence and Security Agency. Keith, all yours.

Keith: So, thanks. Good morning. Keith Minard, DCSA. Today, I'll be providing an update on DCSA planning efforts for industry and our internal implementation of 32 CFR Part 117, the NISPOM rule. Then I'll provide a short update on our COVID and post-COVID NISP oversight operations planning. As Mr. Spinnaker already mentioned from DOD, 32 CFR Part 117, the NISPOM rule, is now effective. Since he already addressed some key changes, I will focus on the activities to support implementation of the NISPOM rule by cleared Industry.

What I would like to note first though, is that I believe the other CSAs maybe find some information. So I'd like to note that the planning by DCSA is for cleared contractors under DoD cognizance only. If you fall under another NISP CSA, please contact them for additional guidance. So, as Jeff mentioned, thanks to the NISPPAC members for the review of the NISP rule, implementation industrial security letters, and the SEAD 3 ISL. As noted, the SEAD 3 ISL has a wide range of comments, comments from industry help us understand Industry's implementation guidance requirements, and questions they have as we put these together and draft them, coordinate them and issue these ISL's. Really, the ISL is there to help clarify, interpret and provide guidance for industry to better implement portions of the NISPOM requirements. In addition to development coordination of the SEAD 3 ISL's and the implementation of ISL, DCSA Policy, in late January, developed and fielded NISPOM rule cross-reference tool that enables readers to select known sections of the current NISPOM and it takes the user to the portion of the rule that it aligns. You can find the tool on the CDSE website. The cross-reference tool is really a great place to start when you're viewing the rule and eases much the transition to the formatting changes of the NISPOM from a DOD manual to a federal regulation. As Heather already mentioned, I think one of the important things that we have to do is, is people need to read the rule. I think it helps bring clarity and understanding of what changes there are and what things actually conveyed from the existing DoD manual to the federal regulation. I'd just like to note that over a few weeks ago, the tools had been downloaded over 2,500 times. I wasn't able to get an accurate update for today's meeting, but I'm sure we're probably closer to 3,000. So, it's important to engage industry as we move through this process. I kind of like to think this is very similar to 2016 when NISPOM Change Two came out about insider threat. Our first event was held on March 25th and was hosted by CDSE. This was like the kickoff webinar focused on the NISPOM rule. The webinar had over 800 attendees and provided an overview of the rule for attendees and included panel members, not only from DCSA, but also from the Office of the Secretary of Defense for Intelligence and Security, Industrial Security Policy. Thanks to them for this joint participation. We are currently working with the NISPPAC Industry lead and NCMS to plan in late April, two additional webinars. The first webinar from CDSE, I would call it a firehose. Now we need to turn the flow down to begin to discuss more in details, get to be more like a sprinkler. So the next webinar will be focused on key changes in the NISPOM rule and other key elements that we are either hearing from Industry that needs clarification or where DCSA sees an opportunity to help provide guidance and clarification. A follow on webinar will be focused on safeguarding. One of the other key changes, this session is in part to better

educate on the changes of the NISPOM rule referral to national information security policy in 32 CFR Part 2001, and to provide an update on the changes for certification of intrusion detection systems. Reference you all 2015 reference, the use of other nationally recognized tech laboratories. More to follow on scheduling. And additionally, the next steps is planning for webinars to engage industry on SEAD 3 reporting requirements. As you can kind of see, we're thinking that we started off with the broad scope of talking about the NISPOM rule, we'll break it down to key changes. And as we move to its implementation period, we'll identify those key areas that we can use and help Industry leveraging and understanding through webinars and other communication capabilities.

To ensure effective communication, DCSA has added an external facing webpage that is now live. It's intended to be a single source to the NISPOM rule information, key changes, events, links to tools and policy, and we're looking to add frequently asked questions for postings related to NISPOM rule to better enable its implementation. This is similar to the webpage that supported NISPOM Change Two and insider threat in 2016. We'll share with ISOO, the link to that page, so they can post on their blog, but the page can be found on the DCSA website. Go to mission centers, then CTP, and you'll find a link at the bottom of the page for the NISPOM rule. You'll also find that there's a link to the cross-reference tool on the NISPOM rule page also, as it is also on CDSE's tools under FSO toolbox. I would like to note that we're working with our public affairs to make sure that we're also using social media to communicate updates on the NISPOM rule. And one of the things we worked with, so at the bottom of the NISPOM rule page, please take the opportunity to view the video at the bottom of that page called Get Ready for the Rule. It kind of gets some key points and outlines some of the key changes in the NISPOM rule. During the implementation period, we'll be working to address input challenges identified by cleared industry, and to work to address what tools and job aids, webinars or communications or guidance in the form of additional ISLs would address those challenges. So, in addition to the implementation of SEAD 3 ISL, we completed a scrub of our existing ISLs, identified some that have to be reissued and I would say, expect to see those reissued ISL's for coordination sometime in the near term, through the NISPPAC for industry comment and coordination. Again, not all existing ISL's will remain, but we did identify those that need to be reissued, so, and this'll be a reissue of existing guidance, so there wouldn't be too much concerned about major changes. They're being revised to align with the NISPOM rule formatting, citations and other areas like that.

One of the key focus areas that Jeff already mentioned, we know we'll need to be working with industry on, I mentioned already, an extra webinar, is Security Executive Agent Directive 3 Reporting Requirements. That's very important. I'm sure there's communication guides and any tools that are needed to support that implementation. I would note that while it's now included in the NISPOM rule, everyone must keep in mind that this is a national policy requirement on the reporting. For those that personnel with access classified information hold a sensitive position.

As with industry, DCSA, CTP and CDSE are reviewing our products and tools to align with the NISPOM rule. This includes oversight procedures for changes, aligning citations for the NISPOM rule and updating our systems, as well as CDSE revising tools, training, and resources. So, what should Industry do? First download the cross-reference tool and the NISPOM rule. Begin by clicking on sections in the current NISPOM you are very familiar with, then read the corresponding rule language. Get familiar. This will help you understand that while now a federal regulation, there are some key changes for industry to implement, but much of the NISPOM remained the same or had very minor changes or revisions.

Finally, DCSA is working to ensure our field personnel are have a consistent message on the rule. DCSA field personnel will not begin overseeing the new NISPOM rule until its implementation date. So, closing on this topic, I would be remiss if I didn't mention a couple of my staff members who have been leading efforts in our office to support this implementation by DCSA, and had an impact on many of the topics that we have already discussed: the webinars, the web page, the tool and the ISLs. This includes Booker Bland, Larry Piles and Jason Theriault. So, that's my closure on the NISPOM rule information.

I'll go ahead and hit some COVID talking points here, and then I'll open up for any questions. With the onset of COVID-19 travel restrictions last March, CTP shifted from mega operations to remote only activities. Our first priority was the health and safety of our workforce and yours. Secondarily, we focus on maintaining our support to your facilities and continue to conduct oversight responsibilities. COVID limited our ability to physically conduct onsite actions. For example, ATOs were issued without the necessary onsite review. Virtual closed area approvals and administration inquiries were conducted virtually. The CMs that involved telephonic discussions with cleared contractors and their facility security officers to ascertain the overall status of the security program. And the CM is really a touchpoint, not an assessment, therefore, no security ratings resolved in the CMs. To date, DCSA has conducted over 7,000 CMs in the past year. So the first priority, when we can safely begin scheduling onsite contractor visits will be actions that have been delayed over the past year. This would include final assessments and approvals of storage that have been done without onsite validation, review of information systems that need verifications and review of corrective actions from our CMs. So that kind of gives you an update of where we are on the CMs, and I would note that additionally today, later on, during the updates for the working groups, you'll hear from Mr. David Scott, who is now serving as the DCSA CTP accrediting authority, and Ms. Marianna Martineau, who is the assistant director for the CAF who will provide an update on DCSA vetting stats during the working group updates. Subject to your questions, this is all I have for today. Thank you.

Mark B.: Anyone have any questions for Keith? Thank you, Keith. Right, next, we're going to hear from Ms. Valerie Kerben, Senior Security Advisor, Special Security Directorate, National Counterintelligence and Security Center, Office of the Director of National Intelligence. Valerie, yours.

Valerie: Hi, good morning. Thank you, Mr. Chair. And I also echo what Jeff and Heather said: it would be great when we can all get together again and work together in person vice this virtual environment. So I'm going to provide you all an update since we spoke at the last November NISPPAC public meeting. So I'm sure you've all heard the news, pleased to state that the new Director of National Intelligence was the first confirmation of the Biden administration, Ms. Avril Haines. And during her confirmation, she stated security clearance reform will be a high priority for her. And she will come up to speed to understand the progress made thus far and the extent and nature of the problems with the existing process. So we're thrilled to have her in our lane and helping us move forward on Trusted Workforce and everything else we have our hands on.

So to give you a little update on Trusted Workforce, in January, exactly January 15th, OPM and ODNI, as the Executive Agent, signed a joint Executive Correspondence. This EC really shifted from the prior phase of Trusted Workforce, where we worked to reduce the inventory. I'm sure you'll hear from DCSA where they are, their steady state of producing background investigations, but we shifted to phase two of Trusted Workforce 2.0. The phase two really focuses on policy development for the implementation of the new government wide approach, the policy levels and how we're going to get through the personnel vetting process from beginning to end. So the EC, one of the main topics in this was guidance for the executive branch departments and agencies, and explains the differences between our Trusted Workforce 1.25 and Trusted Workforce 1.5 transitional state. We're doing this process and iteratively versus one big change at once. Working on the continuous vetting, we're working to ensure agencies are capable and ready to enroll in one of these transitional states. The ultimate goal for transitioning now is that continuous vetting will satisfy the traditional PR process. So we're not going to be doing the periodic reinvestigation every five, 10 years. All employees in the national security population and those contractors, our NISP contracts will be enrolled in a CV capability where checks will be done ongoing.

So we also included some milestones, by September 30, 2021, all departments and agencies must enroll their full national security population in at least the Trusted Workforce 1.25 capability. And DCSA will talk about that, I'm sure, in their update, but it's a capability they are able to offer to their customer agencies. Then by September 30, 2022, all departments and agencies must enroll their full national security population in the 1.5 capability. There's some differences in the capabilities regarding which record checks are being done, and certain things the agencies are also responsible for doing. So we are in helping our agencies enroll and ensuring to address any of their concerns during the implementation phase. I also believe some of our NISPPAC members have seen a copy of this correspondence, and that was part of the information sharing with some of the high level policies that come out of our office to share with the NISPPAC members.

Additionally, in regards to personnel vetting, in December, prior NCSC director, Mr. Evanina, released a statement regarding COVID-19 and how mental health

impacts should not impact national security eligibility, and really stating that counseling and undergoing treatment as a result of COVID or the associated stresses should not in itself be considered a negative or disqualifying factor for rendering eligibility, or access to classified.

Also, in January, our new acting director for NCSC, Mr. Michael Orlando, signed another memo reiterating Mr. Evanina's statement that there are the COVID impacts on the cleared workforce, and with just concerns and wanting to ensure that the wellbeing and seeking counseling to address these concerns are being taken care of. It is definitely a positive step and not a disqualifier.

Let's see, one other area I want to talk about, and we've gotten some questions and I know it's been in the news, OPM issued their clarifying guidance on marijuana use and reiterating the federal drug-free workplace, but just wanted to state and remind that there was a 2014 memo that came out from DNI stating that the adherence to the federal laws of using marijuana is illegal. It's a controlled substance. So we're still following that guidance. It's still valid, however, we are considering putting together clarifying guidance and also monitoring legislation.

ISOO has asked us to give a background on the impacts of COVID. ODNI continues to operate with limited staff. Even though we're not back to business as usual, we still have lots of staff working on team type of schedules. We are operational and we're ready and able to respond to questions and concerns from our partner agencies in Industry. We just ask you to be patient. Our response times may be a little longer, however, important for you all is that the Scatter Castles program and our continuous evaluation systems, help desk personnel are still available and they are fully operational. We continue to attend and brief at Industry related conferences and panels virtually. We are available and do want to continue our partnership with our stakeholders here.

Regarding the NISPOM rule implementation, DNI and CIA are working together to implement the NISPOM rule and retract any references to the prior NISPOM manual. I know they are working on making changes internally to new acquisitions, and I'm not sure if CIA came on the line or if they're available, if they want to provide any more detail.

If not, otherwise, I am finished and thank you very much. Are there any questions?

Mark B.: Okay, well thank you, Valerie. That was very helpful.

Valerie: Thank you.

Mark B.: Okay. Sure. Up next is Mr. Rob McRae, Director of the National Security Services Division and Mr. Rich DeJausserand, Deputy Director for Industrial

Security to the Department of Homeland Security for their updates. Gentlemen?

Rob: Hey, good morning. Thank you for an opportunity to update everyone. So the department continues its important mission of protecting the homeland through counter-terrorism efforts, mitigating homeland security threats, securing cyberspace and critical infrastructure, securing the country's air, land, and sea borders and strengthening the preparedness posture. Our workforce largely posture largely remains in a telework remote work environment with the exception of law enforcement, border operations, port operations, obviously they continue to operate in various areas throughout the country. One thing of note here, is through the department's operation, vaccinate our workforce, or Operation VOW, and through a partnership with the Veteran's Administration, We have successfully vaccinated over 58,000 mission critical employees here in the department, so we are continuing with that important program here and getting the population of our law enforcement personnel vaccinated here. And so with an update regard to industrial security, I have my deputy here, Rich DeJausserand. Rich?

Rich: Thanks, Rob. Good morning everyone. I'll try to be pretty brief here. As everybody knows, I'm sure that DHS, we receive a majority of our industrial security services from DCSA through a special service agreement, however, we continue to work with DCSA, my team is continually working with them on the implementation of the new NISPOM final rule. Specifically, working with our personnel security team in regards to SEAD 3, we are developing and implementing communication plans, we're developing policy documents, and we are also developing reporting tools, or in the process of developing reporting tools for SEAD 3, and we continue working with DCSA for FOCI assessments regarding accepting NIDs. While we will still conduct our own risk assessments with those NIDs, we will make a risk management decision, get with our CSO, who's the CSA, to determine if we are going to accept those NIDs based on our risk assessments. We are still in the process of developing and working hand in hand with DCSA. That's all I have. Thank you.

Mark B.: All right. Thank you so much. Anybody have any questions for our colleagues at DHS? Okay. Thank you. So the next update we'll hear from is from Mr. Mark Hojnacke, Director of Security Policy at the Department of Energy. Mark?

Mark H.: Yes. Good morning, everyone. Thank you for giving us the opportunity to give DOE's update on the NISPOM implementation and our COVID return to work status. DOE has included a review of the NISP CFR requirements against the department's current security requirements and has noted a number of areas that will be addressed, either the page changes to the security directives or through a secretarial policy memoranda. The one that stands out, obviously, is the NIDs language from the recent NDAA update. Our DEAR clause, that's the DOE Acquisition Regulation, security clause, references DOE security directives, rather than the NISP, to account for other security assets within the department. Because it does not specifically address the NISP, there is no need

to update that security clause, although there will be other updates to the DEAR to address the NIDs and FCL processing.

Our COVID return to work status. In March of this year, DOE issued an updated COVID-19 workplace safety plan and held a department wide safety clause, which included all federal and contractor employees. The safety clause was led by senior leaders within the organization via virtual town hall style meetings. The clause introduced the updated COVID workplace safety plan. Reviewed and reinforced COVID safety protocols that the department provided in an open dialogue between employees and management about the challenge of associated with the COVID-19 protocols. We have also shared vaccine information, including vaccine availability through the department and encourage the workforce to be vaccinated. Our current operating status is that we continue maximum telework throughout the department in compliance with the OMB goal to operate at 25% of normal building occupancy, or lower, per sites experienced high community prevalence of the transmission of the virus. That 25% occupancy standard can be waived upon approval by the secretary. That's our update for today and I'll provide any answers to any questions anyone may have.

Mark B.: Thank you, Mark. We appreciate that and next we're going to hear from Mr. Chris Heilig to give the NRC update. And after that, we're going to take a five minute break. Right. Chris, you're up.

Chris Heilig: Good morning. I'll end up kicking it over to Dennis Brady for the NISPOM implementation and COVID information, but in terms of personnel security or updates, there aren't really much of an update to provide. Our volume of cases and adjudication timeliness is stable. We were fortunate that our agency was able to continue processing cases as usual, even during the COVID restrictions. Our process is primarily electronic. Things are getting a little easier that we could not do in person, for instance, drug tests and fingerprinting. As COVID restrictions are easing, we're able to take care of those steps at almost a normal pace again and as things progress in the COVID world, and we will obviously get back to normal a little quicker because we were not as impacted as some of the other agencies. That's essentially all I have in terms of personnel security updates. I would ask Dennis to take over from there.

Dennis: Okay. Thank you, Chris. Good morning, everybody. Dennis Brady. From the NRC perspective, we continued to regulate the civilian use of commercial nuclear energy in the academic and medical use of it as well. The NRC is continuing to implement the requirements of the NISPOM, although like all other agencies, we've had to come up with alternative means for conducting that, but working with our industry stakeholder partners, we've been able to achieve those goals.

As an agency in our COVID response, most of the agency is in, what we have is phase two for maximum telework, but some of our regional offices still are in

our phase one for mandatory telework, but are still able to conduct our functions as the regulator for nuclear energy. That's my report for the NRC.

Mark B.: Great. Anyone have any questions for our friends at the NRC? Alright. With that, we're going to take a five minute break. I've got 11:04 here, so by 11:09, 11:10, we'll start back up. And our first speaker, when we come back will be Ms. Stacy Bostjanick. Alright. Five minute break.

Producer: Welcome back. Let me turn things over again to Mr. Mark Bradley.

Mark B.: Alright. Thank you so much, Madam Moderator. Next we're going to hear from Ms. Stacy Bostjanick, Director of Cybersecurity Maturity Model Certification, also known as CMMC Policy. Stacy, all yours.

Stacy: Thank you very much. Can everybody hear me? Can you hear me?

Mark B.: Yes ma'am.

Stacy: Okay, good. So as of Monday, I am now the Director of Supply Chain Risk Management for OUSDI&S, and so today I'm going to give you some updates on the whole enchilada that we're working on. So with CMMC, we are continuing to work through the rule making process. We have started the adjudication of the comments in earnest, and based on those comments, we've gone back and looked at the model and are considering some possible changes in response to those questions and comments, but we're not ready to publicize exactly what those are yet.

We are moving forward with our pilot and getting the C3PAOs assessed at the CMMC level three, as we consider the information that they're pulling together with those assessments as being sensitive information. So each and every C3PAO that will be performing the assessments, will have to have a CMMC level three assessment done on themselves first. Every assessment that they accumulate and review will be housed in the DISA GovCloud, And that information will then be ported over to the SPRS system where contracting officers and program managers will have the opportunity to go in to validate that companies have the appropriate CMMC level for the contracts that they're competing on.

We have had a couple of pilots that have canceled and waved off for various and sundry reasons. Some of them had award dates in June and our C3PAOs didn't look like they were going to be ready in time and one of the main tenets of our pilot is we're not going to impact the timing of any of the award cycles for our acquisitions at this time. We're also working very closely with International Cooperation, they always confuse me because they call themselves the IC and coming from DIA, I'm like, "Wait, who?", but International Cooperation is working very closely with us to make sure that we get the agreements in place with our partners, because they're very interested in participating in CMMC.

We have had some countries indicate that they may want to wholesaley adopt the CMMC process, and then we have others that may want to be their own C3PAOs or may set up their own accreditation body. We've also had other agencies within the federal government express interest in CMMC. DHS is looking to onboard. They're planning some pilot activity and pathfinder activity here in the near future, and as well as GSA is going to run some pilots for us as well. So CMMC is rocking and rolling. There is a 30 day assessment being done internally by the new administration, just to make sure the implementation is going the way that they expect it to. There's also a GAO assessment going on for Congress. So based on those two, I'm sure we may have some tweaks to the program, but whole family we've seen a lot of support through the administration for CMMC.

On the supply chain risk management side, we're working with trusted capital in setting up avenues for companies to come in and hopefully get some investment, to try to mitigate the interest from our adversaries in investing in some of our innovative companies. We're also working very closely with many of the supply chain illumination tools. We use some of them during Project WARP SPEED to further our capabilities, and that seemed to be very successful, so we're looking at that across the board. We also have set up a supply chain working group with members of OUSD, across OUSD and the services, to come up with a lexicon and taxonomy and a standardization to look at supply chain risk and how to assess it and mitigate it and then what are the tolerance levels that we can expect. That's pretty much my update, barring any questions, I appreciate your time and the ability to speak with you.

Mark B.: Anyone have any questions for Stacy? Alright, Stacy, go back to the beach.

Stacy: I'm on my way. Thank you guys so much.

Mark B.: Okay. Enjoy yourself.

Stacy: Thank you.

Mark B.: Sure. We have Roy Jusino and Chris Pollock with the General Services Administration, here to brief us next on the GSAs black label safe removal program. Gentlemen?

Chris P.: Good morning, Mr. Chairman. This is Chris Pollock with GSA, and I appreciate the opportunity to speak to the NISPPAC today. As you mentioned, we also have Roy Jusino from the DoD Lock Program, here to address some of the issues. By way of introduction, I'm the Branch Chief of the Standardization and Engineering Branch at GSA. I'm also the Program Manager for the GSA Approved Security Equipment. I'd like to talk today about a recent policy related issue that addresses the removal of some older GSA approved containers and vault doors that are currently used for protection of classified information. Next slide please.

There we go. So this one looks like, at least on my screen, it's a little bit hard to see, but if you have a copy of the presentation, maybe you'll be able to look at it closer there. I'll run through it real quickly. Back at the end of January of this year, we issued this letter to the GSA approved security training schools and equipment manufacturers, laying out the requirement for the removal of black label containers and vault doors. I understand ISOO was also working on a similar policy that should be issued shortly. If you could read the table, you would see that the black label containers are all at least 30 years old, some of them as old as 70 years old. At the end of service, the removal date that's listed in this letter, is between 2024 and 2028. This gives everyone at least three years and in most cases, seven years, to identify the older equipment and get it replaced. Next slide please. That's just a signature page, so again, next slide.

So here are some examples of containers that had the different labels. The containers that will need to be replaced are the samples on the right side, where you can see there's a black label, black lettering on a silver label. If you have the containers with that label, they will need to be replaced, again, sometime in the next three to seven years. Containers that have the red label, red lettering on silver background, as on the left hand sample, do not need to be replaced. Okay, next slide please.

So why is this equipment being removed from service for protecting classified information? Again, as I mentioned a couple of times, the containers are getting very old. This leads to problems that can be attributed to safety issues, security issues, and repair issues. Under safety issues, a lot of the moving parts on containers that are over 30 years old, tend to wear out. You get worn slides, you get out stops that break off, and you also can get rusty interiors, which can affect the operation and security of the containers. Over the years, there've been a lot of different improvements to the containers, which were not incorporated in some of these older containers. Things like changes in the lockbox and also changes in the locks, from mechanical to electrical mechanical locks. There's also repair issues, many of the manufacturers who originally produced the equipment are no longer in business, so repair parts are no longer available. So all of these factors add up to a situation where it's time to start removing the older equipment from service. I will now throw it over to Roy Jusino to go over some of the industry requirements. Roy?

Roy: Thank you, Chris. My name is Roy Jusino. I am the chair of the active SEALS subcommittee that oversees these specifications for all the different GSA security equipment. I'm also Director of the DoD Lock Program, for the Department of Defense. So basically we put out this letter to all the GSA manufacturers and the training. We will be working with all the agencies to get the letter out to all the agencies, so they can plan, and what we're asking right now is everybody to start surveying your facilities for GSA-approved containers, determine number of black label containers that you have and vault doors that are in use and that'll be on the list for replacement. Determine your requirements, facility accreditation reviews, possible classified holding reductions, work with the accrediting authorities and contracting officers to

formulate a company plan for replacement. Again, this is government wide, through all federal government. Again, we put up these timeframes, we feel that will be plenty of time for everybody to start addressing this and looking at it and surveying and making plans. Again, we put the date out there and of course it'll be flexible, but we have to start somewhere to replace these older containers. Next slide please. And that's really all we have. Please submit any questions that you have, and we'll be more than happy to answer. Thank you.

Mark B.: Thank you. Any questions for our friends from a GSA? All right. Now moving into the portion of the meeting where we get reports from the NISPPAC working groups, however, we're not going to be discussing all of them, but we have provided slides with highlights of all of them. We'll be discussing today, the clearance, cost, and NISP Information Systems Authorization, also known as NISA, working groups at this time. Greg, you want to take back over? Greg?

Producer: It looks like his line may have been disconnected.

Mark B.: All right. Do you think you can raise him or do you want me to…Greg?

David: This is David Scott. I'm available to present, if you guys are ready.

Heather Harris Pagán: Mark, do you want me to speak for Greg's piece?

Mark B.: Yeah, yeah, yeah, yeah. I'll take over for Greg here and then we'll get right to it. Alright, let's see. You've heard from some of the CSAs on the high level points of what was discussed during the clearance working group on March 3rd, 2021. Since the last NISPPAC, we also discussed the Small Business Administration, the SBA, regulation combining their mentor protégé programs issued this past fall. The SBA rule appears to eliminate the requirement for a joint venture to have an entity eligibility determination, or EED, if the entities making up the joint venture already have EEDs themselves, however, this interpretation of the regulation's language is not actually what the regulation intends and it would contradict this requirement. Therefore, we will be issuing an ISOO notice soon in coordination with-

Greg: I'm back on. I'm sorry.

Mark B.: All right Greg, let me just finish this paragraph and it's yours. With SBA, Small Business Administration, to clarify the joint venture EED requirements. All right, Greg, you can pick it up at, we have continued.

Greg: Okay. Yeah, I apologize everyone, in my case it was simply a matter of my chin hitting the phone and I accidentally disconnected. So anyway, these things happen. Alright. So you already covered some of the points.

The working group did meet and a lot of things that were discussed today, we discussed during the working group, obviously the Trusted Workforce ongoing

transition to 2.0 was discussed, the JPAS, the DISS transition, the NISPOM changing over to a rule and the implications of some of the changes, particularly SEAD 3, but also a little bit on TS accountability, limited facility security clearances, and the intrusion detection recognition that not just UL 2050, but other entities that meet nationally recognized testing laboratory standards, which EnterTech, I believe is one such other entity that does qualify as certified under those NRTL standards. There was a little bit of discussion about security vulnerability assessments, the ratings, how that's evolving ratings for SBAs. And of course, discussion about oversight in general, in the post COVID environment.

Now, did you cover the other issues that I was going to mention? I think you did cover joint ventures and small business administration, is that right?

Mark B.: Yes, yes, yes.

Greg: And the cost, did you discuss the NISP entity cost?

Mark B.: No. We were just getting there when you cut back on, so please.

Greg: Okay. This is a continuation of, let me just say, this is a broader sub element to an initiative that ISOO under has undertaken, beginning about two or so years ago, to refine and simplify, to support agencies in their efforts to provide overall data with respect to their classified national security information programs, as required by executive order and directive to ISOO on an annual basis. One probably that would always get the most attention was reporting on the estimated numbers of derivative and original classification activities, which in and of itself was a highly suspect number. It was an estimate, but even with that, it was an extrapolation. In any event, ISOO, the director, suspended the collection of data while we worked on refining our collection efforts, consolidating them and taking advantage of technology in doing these things. And so cost is one of those elements within the raw collection of data that is required. In this case in particular, we're talking about cost incurred by contractors under CSA cognizance, under Cognizant Security Agency cognizance. So that's what we've been focused on in this area. We, the government, have met several times discussing this and what we're trying to do, before we bring Industry in to see what we've come up with, is for each CSA to bring their proposal for how they intend to gather costs that their contractors, under the NISP, under their cognizance, incur. That said, it could be that each CSA comes up with something that they all agree on and we just have one mechanism. One of the keys, of course, is we do not want to have duplication of cost collection. Keeping with the overall intent of the reform effort for data collection, we want to keep it as simple as possible, so once we get to that point where we have the CSAs' way ahead, and some degree of consensus, we would then bring NISPPAC Industry into take a look at what we have and to get their input. So that's what we have on that.

Turning to the, let's see, the NISA working group, the Information Systems Authorization working group, we also met and as has also been stated during

the updates that were given, one of the topics was sanitizing solid state devices/drives also known as SSDs and appreciate the update that DoD gave.

The one thing I would add to that is ISOO do intend to reach out, actually, we started already, to the Committee on National Security Systems, CNSS, as they set the policy, national policy, for utilizing National Security Information Systems to process classified. So in this case, as it relates to remediation methods for drives involved in classified spillages, we want to at least ask them to examine the existing policy, to see if there's any need to make some adjustments. So with that, what I want to do before we collectively take questions in this part of the agenda, is we want to hear from first, David Scott from DCSA, to give an update on DCSAs information systems. David?

David: Yes. Thank you, sir. I appreciate that. So I started off this position as the NISP AO last week, so I appreciate the invite and I look forward to working with the NISPPAC members and the audience as a whole. Previous to this, I was no stranger to the NISP. The last four years, I served as a regional authorization official in the capital region and served as acting southern region AO for the past year, as well as very extensive work in cleared industry myself. Couple of quick updates with the leadership changes in the capital region, there is an acting, Jamie Davis, she's acting while we look to back fill my position in the capital region and in the southern region, we've selected and have onboard a permanent southern region AO. His name is William Bond. He just started a few weeks ago and we're looking forward to his contribution to the team. Next slide please.

Okay. So from a metrics standpoint, these are pretty self-explanatory, I'm not going to run through all of them. What I want to do is just kind of highlight a couple of points. The system registrations in eMASS, are the systems that are authorized, are staying at a steady state, little increase, but not too significant. But what I want to inform everyone is we've implemented over the past, since about January, past few months, a triage process. What we identified within our agency as we move to RMF, and we had some backlog in certain areas, we were getting to the point where we had some ISSPs, their queues were getting big, and we had Industry waiting for some sort of communication on whether or not what they submitted was actually in the process of being authorized, and we were having some timelines where they wouldn't receive a comment back up to 80 days. Then the unfortunate case where Industry would submit something in this somewhat new process, we've been at a few years now, where simple mistakes were made that we just could not move forward. So what we did was we implemented, over the past few months, a triage process where within the first 10 to 14 days, we'll take a look at what's submitted by Industry, we'll make sure that it's meeting the mark and then we'll put it into our queue. If we find some simple mistakes throughout the initial triage, we'll return that so that Industry can immediately address those concerns, so industry's not waiting 60, 90 days before they hear something from us. So we've already seen some very good return on investment with that process, and we'll continue to do that. The other piece that I wanted to hit is the AOs.

There's a part of COVID, initially when we first started the pandemic, we were deferring the on-sites and doing roughly around six months authorization. This is going back a year ago. And then once we realized that the pandemic was going to be a lot longer term than what everyone expected, the AOs got together last fall and we said, "We need to do better." So we came up with a framework to where if the industry package, it's efficient, it's solid, the controls are addressed, the risk is clear and understood and acceptable, we would issue a three-year authorization deferring the on-site until we can get to a post-pandemic or a regular business model. We're just now starting to see some benefits of that. We still have the tool of a conditional authorization if in fact we're still missing a few pieces that we could do a six month authorization. However, we are moving more towards a model of the three year authorization, deferring the on-site, and that is actually starting to reap benefits. Next slide please.

Okay. This is a slide that we just started recently putting together. It's our top 10 NISP non-compliant controls within eMASS. This is new. We're still digesting this information as an agency, but hopefully you'd use this tool internally and externally to help address some consistency concerns. I won't go into too much detail, but you'll see the top one right there, RA-5 vulnerability scanning. I can tell you coming from this field over the past few years, there is a misinterpretation of that control. For example, vulnerability scanning, we have a lot of industry team members where our ISSMs would state that they're using a certain tool like a scout compliance checklist. That is not the intent of that control. It is a scanning tool, but the control itself is vulnerability scanning. What is the process for finding weaknesses in the application of the system, for example, your Microsoft patches? So it is just a misunderstanding of the actual control. So what we're going to do is take this metric and start identifying some trends and then start education internally and externally for consistency across the country. Next slide please.

So DAAPM, we are in the early process of planning for a DAAPM upgrade. What I want to call to your attention is we are well aware of the NIST Rev 5 800-53 controls. We are well aware. We will have to do an update for that. We also have been working since last August, internally, on a NIST connection process guide. It's the first of our kind for an agency. Over the past many years, other agencies, DISA, et cetera, they actually have a connection process guide on how to do business with them for interconnected networks And we saw there was great benefits with those types of documents, So we actually are starting to draft our own and expand upon the requirements, processes, and guidance on how to have an interconnection with the NIST. So some of the highlights are a process flow map. If you're going to interconnect with a government network, here's what you would do. it would follow process flows, we'll provide templates and easy to read guidance, so it'll be available. It should be easy to read for any government or industry stakeholders, so we're looking forward to that. We're in the early stages of developing. We understand we've got some coordination aspects to do. We'll definitely share it with the NISPPAC as well,

but we're very excited about that document. We look forward to sharing that with you guys. And next slide.

NISP common eMASS issues, no changes here. One thing I do want to kind of call out too, is if we could make for everybody's awareness, especially Industry ISSMs is ensuring that we're checking the security classification guidance before we input stuff into eMASS, just making sure that we're double checking any classification guidance at all. We have a process if we have an SCG that states certain controls are at a classification level. We have a process for handling that in our job aids. But just want to make sure that that word is spread and that we're adhering to that. But other than that, eMASS common issues are pretty much straightforward. We're getting the questions into our group mailbox and we're addressing them on that on the regular. And next slide is just questions and some available resources. And that's all I have unless there's questions from the group. Thank you.

Greg: Thank you. Does anyone have any before week turn back to vetting statistics for that process? Anyone have any questions on information systems authorization?

Rosie: Hi, this is Rosie Borrero. Industry, NISPPAC. I just wanted to ask a quick question, and thank you, Dave, for that. Just wanted to ask for the top non-compliant controls, would you be willing to post examples of compliance in the frequently asked questions online for Industry?

David: That is the goal. I've got to work through the coordination of publication process, but that is the main goal of this tool. Now that we have enough data in eMASS collected over the last year, year and a half, we're able to provide some trends, but the goal is absolutely to share some of this information with Industry for common understanding and consistency across the board, but yes, that is the goal. No promises on timelines. I'm still a little new to this position and understanding the coordination aspect of it, but we'll definitely do as much as we can get that out to you guys.

Rosie: Great. Thank you. I appreciate that.

Greg: Okay. Thank you. Unless there's no other questions for that. And we'll now look at some vetting statistics and I'll ask Marianna Martineau please, to start that, looking at the background investigations, adjudications embedding data. Please, Marianna.

Marianna: Yes, thank you. Good morning, everyone. I'll be covering background investigations, continuous vetting and adjudication, mission updates for DCSA today. Regarding background investigations, our total inventory is currently just slightly over 205,000 cases of which 34,000 are Industry investigations, which is consistent with inventory from about a year ago and less than half of the inventory from two years ago.

Timeliness statistics for end-to-end processing for Industry cases, including initiation, investigation, and adjudication in FY21, in the second quarter: improved significantly as compared to one to two years ago, specifically our Tier 5s were running end-to-end about 159 days and Tier 3s, 127 days. Timeliness and inventory continue to fluctuate due to seasonal onboarding and hiring, however, of course, in the past year, as we've all talked about here, we've had a few unpredictable impacts related to COVID-19 and specifically surges and occasional IT hiccups, but we are seeing a gradual increase in timeliness as a result of some of these challenges that we've experienced over the past year.

For the background investigation group, as COVID continues, we are maximizing telework as most staff are already working remotely, and we are continuing to use the executive agent approved alternative processes, including telephone interviews. While roughly about 5% of the background investigations in our inventory have been delayed or placed on hold due to COVID challenges, our team is constantly revisiting each case to continue to work and close these cases as quickly as possible. DCSA has remained postured to and committed to mitigating COVID related impacts with timeliness and our overall inventory without degrading quality.

I'll talk a little bit further and in a bit on the adjudications timeline. So let's go ahead and switch over to the next slide and talk about the Vetting Risk Operations Center. The VROC is staying laser focused on all Industry functions, and as you know, that includes investigations, submissions, interims, periodic re-investigations and continuous vetting deferments, processing incident reports and other DISS, or the Defense Information System for Security customer service requests, and balancing timeliness to support mission readiness, and identifying and mitigating insider threat concerns.

To date in FY21, the VROC has submitted roughly 62,000 background investigation requests. 90% of those have had an interim determination made on average within five to seven business days. Effective April the first, as I'm sure everybody here knows, investigation requests can no longer be submitted in JPAS. Industry must use the Defense Information System for Security for all security management functions to include investigations submissions. So as a reminder, please submit your fingerprints for initial clearances prior to submitting an investigation request. The VROC cannot open a background investigation or enter or issue an interim determination without first the required fingerprint results, when applicable.

Regarding continuous setting, DCSA is responsible for implementing the DoD continuous vetting program and has begun offering the Trusted Workforce 1.25 service to non-federal agencies. Our goal is to have the entire DoD cleared population enrolled in the Trusted Workforce continuous vetting compliant program by the end of 2021. You'll see a significant increase in enrollment since FY as we are working to achieve this goal.

A few items to note here is enrollments do include the eMASS contractor population, currently about 675,000 Industry subjects are enrolled in continuous vetting, and all industry periodic reinvestigations deferred subjects or about 121,000, are also enrolled in Trusted Workforce 1.5 automated records checks. An additional 350,000 industry subjects are pending enrollment. The VROC is currently enrolling all subjects post adjudication, and is also working to extract SF-86s on file within the Defense Information System for Security and other systems of record. What we need from industry is to be responsive for any overdue periodic investigations or if an out of cycle SF-86 is requested for submission. Continuous vetting enrollment does require adding minimum the 2010 version of the SF-86 of which we have most of them, but not all, since the 2010 version wasn't deployed until the 2012 timeframe. If needed, the VROC will be sending specific instructions to individual companies in DISS this spring, so please be on the lookout.

For continuous vetting alert management, post enrollment alerts are generated based on established thresholds which align to the federal investigative standards and adjudicative guidelines. We're currently seeing an average of a 6% alert rate, although we are baselining a large volume of population. Criminal and financial indicators are still the most common, valid, actionable alerts. So far in FY21, we received 19,000 Industry alerts on 14,000 unique Industry subjects of which 8,000, while this is a lot of numbers, or 48% were not previously known. So what does that mean? It means that these alerts represent information that should have been self-reported. Our goal moving forward is to encourage self-reporting of information as early as it is known as it will avoid future continuous vetting alerts. Moving on to the next slide about the CAF.

So today the CAF continues to apply portfolio management techniques to deliver national security, suitability, and credentialing adjudications. Our readiness portfolio represents those adjudicative actions designed to get people to work, where the risk management portfolio manages risk within the Trusted Workforce. So far in FY21 through the second quarter, the CAF adjudicated Tiered background investigation products in an average of 16 days for initials or 92 days for periodic reinvestigations. For the Industry population, we did the same work and adjudicated initials at an average of 17 days or 119 days for periodic reinvestigations.

We expect that adjudicative timeliness performance for PRs will continue to be higher than historical averages due in large part because of the changing derogatory nature of the periodic reinvestigations we’re receiving for adjudication, coupled with delays related to COVID-19 and obtaining additional information from subjects. Our current total industry inventory is about 30,000 cases, 59% of which are within our readiness portfolio and the remaining 41% in risk management.

The CAF is continuing to focus on improving processes, timeliness, implementing Lean Six Sigma improvements and increasing efficiencies as we

continue to work with our colleagues in the background investigation and the vetting risk operation group to implement the trust and workforce strategy. We will also continue to focus on preparing our workforce for these challenges while also striving to continuously improve our services and support to your mission operations and needs.

Some of our focus areas for the remainder of this fiscal year include reciprocity. As an update, because I know this is a sensitive subject for those on this call, last year the CAF and the VROC executed a joint Lean Six Sigma project focusing on improving the end-to-end reciprocity process.

Last month, DCSA deployed a change in the defense information security that allows industry reciprocity, customer service requests to go directly to the CAF. This update of process is functioning without any technical issues and is already improving the end-to-end timeliness. Over the next month, the CAF anticipates further process improvement as we implement the remaining Lean Six Sigma efficiencies, and we will be bringing DCSA to full compliance with the DNI five day end-to-end processing requirements.

We are also looking to deploy an adjudicative assistance tool, which is designed to implement machine learning focused on enhancing adjudicated quality assessments and training programs. As you heard Valerie talk about earlier today, we are continuing to focus on mental health care and destigmatizing seeking mental health care treatment for cleared personnel with losing a security clearance. We started that process in FY20, and we'll continue to do so through FY21. We're expanding our messaging through the DCSA web portals and social media outlets, frequently asked questions, and other information located in the DCSA CAF resources webpage. Our mental health campaign efforts also include external outreach engagements with clinicians, psychologists, security managers, and defense organizations. Again, we're trying to get our message out that simply speaking mental healthcare treatment is not in and of itself a reason why people lose security clearances.

I would like to call to your attention some amended COVID-19 extension processing at the CAF. Last year, at the beginning of COVID-19, we evaluated our processes and implemented basically a hold, if you would, where we were not receiving responses to our requests for additional information or other actions related to COVID-19. We recently re-evaluated our current operating procedures and are reinstating our pre-COVID business processes and procedures regarding correspondence requirements for responses. We will no longer be issuing indefinite automatic extensions related to the COVID-19 pandemic. Subjects, through their security managers and facility security officers, will have 30 days from the date of our request, for an action in the Defense Information System for Security, to comply with that official request for information. If you have any questions, please send those to us through the portal. We'll be happy to answer any questions that you may have, although you can find some additional information on the DCSA website regarding this announcement.

Lastly, I'd just like to call your attention to the bottom of the slide where I'm proud share with you the DoDCAF first annual report covering FY20. It highlights many of our accomplishments and continuous efforts to improve the DoD assigned adjudications and related personnel security eligibility determinations, our adoption of streamlined business processes for security clearance processing timelines, and a return to healthy and stable inventory. We are committed to working with you, our customers, and continuing to build strong partnerships to increase information sharing, and to support your operations and information readiness. So if you can, take a moment to share and read our annual report in the link at the bottom of the slide. Pending your questions, that's all I have for this morning.

Greg: Well, thank you Marianna for that excellent and comprehensive overview. Does anyone have any questions? Okay. Next we're going to hear from Tracy Kindle to provide some DOE update metric data. Tracy?

Tracy: Good afternoon, Greg and everyone. I'm Tracy Kindle and thanks for the opportunity to provide the DOE personnel security update. I know Mark spoke earlier, but just for those who didn't know that we have a new secretary and her name is Secretary Jennifer Granholm. The next thing I'll talk about is the DOE personnel security statistics. Currently we're meeting the IRTPA timeliness goal for all investigative tiers based on their February 2021 statistic. For our T5 initial, we met our IRTPA goals 11 out of the last 12 months and we expect that trend to continue. For the T3 initials, we've met our goals over the last six months, and we expect that can also continue. For T5Rs, we met those goals over the last nine months, and again, we expect that to continue. For T3, we had one hiccup in June of 2020 with our initiation process, but since that time we've been meeting upper goals, and again, we expect that trend to continue. That's really all I have right now, Greg, for the personnel security statistics pending anyone's questions. This will conclude my briefing. Pretty short.

Greg: Okay. Thank you, Tracy. Anyone have any questions? Okay. Next we have NRC. Now, I believe Dennis Brady already gave some data on the personnel security metrics, but we have Chris Heilig if you have anything additional to add.

Chris: Well, I spoke earlier. I don't have anything additional to add. I would clarify, we are meeting our IRTPA guidelines for adjudications. And as I mentioned earlier, we didn't experience any slowdowns during COVID. So we would assume everything goes back to normal sooner than later as the COVID restrictions are lifted. That's really all I have.

Greg: Thank you, Chris. So unless there's questions for Chris or any questions overall, with respect to the working groups, from what you've heard this morning, I'll turn it back over to the chair.

Mark B.: Thanks Greg. Alright. Now we're going to hear from Mr. Perry Russell-Hunter from the Defense Office of Hearings and Appeals known as DOHA. Perry?

Perry: Thank you, Mr. Chairman. Thank you NISPPAC members. DOHA is continuing to make maximum use of telework except for the personnel who are conducting and supporting the in-person administrative hearings, the DOHA administrative judges, department council and support personnel. Obviously the hearings are a core part of the DOHA mission so by having everybody else telework, we're maximizing the safety to everyone who's involved in those in-person hearings, but leveraging telework has not affected DOHA's productivity and that's in large part, thanks to the great partnership between DOHA and the Consolidated Adjudications Facility, the leadership of Marianna Martineau, who you just heard from and the excellence and expertise of her staff and the adjudicators of the CAF. Calendar year 2020 was actually the highest average year for total numbers of Statements of Reasons reviewed and issued since 2016. Statements of Reasons are still going out in typical numbers and are timely. We currently have 330 SOR reviews pending, which is a typical number. At the end of January, we had 390 pending. Considering that DOHA reviewed and the CAF issued over 3,100 draft Statements of Reasons during the period between March of 2020 and March of 2021, we're in great shape and we're current. The first four months of fiscal year 2021, we reviewed and the CAF issued 1,200 Statements of Reasons. So there's going to be a shift later this year where DOHA will begin providing the SORs directly to Industry employees and also tracking them, so that's something that we've mentioned before, but that's going to be happening over the course of the next year.

While the pandemic was impacting the hearing process because DOHA was having challenges with conventional video teleconferencing due to the simple fact that there would often be no operators available at the other end of the line where were DOHA needed to reach, DOHA has now tested and is making good and effective use of something called the Defense Communications System, or DCS, to conduct remote online virtual hearings for clearance holders and clearance applicants in locations where travel would still be unsafe or where we could not reach the individual using conventional video teleconference technology. That is all I have pending any questions from the group. Thank you.

Mark B.: Any questions for Perry? Thank you, Perry. Up next is Mr. Evan Coren from my staff of ISOO, who will provide an update on the Controlled Unclassified Information program, known as CUI. Evan?

Evan: Thanks Mark. As Mark said, I'm Evan Coren. I'm the team lead for CUI ISOO, and I support the Director of ISOO who is the CUI Executive Agent. First, I wanted to start with an update for the CUI Annual Report to the President with some data we want to share with you for the initial analysis. We have 90% agencies that are appointed. They will have their CUI policy done by the end of 2021, and this includes 65% of agencies who report that they had their policy done, or would have it done by December of 2020. In addition, 80% of agencies have already begun disseminating awareness products or training their workforce on the upcoming CUI implementation. In addition, 90% of agencies are reporting that they will meet the physical and cybersecurity safeguarding

requirements by the December 31st, 2021 deadline. In addition, and other good news, the National Information Exchange Model or NIEM has released NIEM 5.0, which for the first time includes a CUI metadata standard. For those not familiar, NIEM is one of the common metadata standards, so this will significantly improve the metadata consistency that occurs as metadata is used in association with CUI, okay? The CUI Registry Committee and ISOO will serve as the mechanism to update and review changes to the CUI domain within.

In other good news, NIST SP 800-172 has been published. This was formerly known as the draft NIST SP 800-171B. So 172 establishes recommended security protections for non-federal information systems that process or transmit CUI. It was released in final form in February 2nd of this year. It mainly evolves changes in narrative and boundaries and does not change the controls that are in place. The controls within the 172 are often used in the CMMC Level 4 and Level 5 determining that contractors have the necessary controls in place.

Okay. A lot of people have been following the issuance of the CUI FAR case. Right now it was projected to go out to public comment from March to May of this year, but since we're already in mid-April, we are currently expecting to see a pushback for comment later. Once it is out for comment, we will hold an ad hoc stakeholders meeting that we'll schedule at the beginning of the public comment period to address concerns and discuss the draft version that will be up for comment.

Also want to encourage everyone to take a CUI markings training that we are offering at ISOO. My colleague Charlene Wallace, who is CUI training lead, does a superb training about every month or two. We announce it on our blog and I'd recommend following the blog for updates on when those are going to be. ISOO issues a training certificate. And today, she's getting about 500 to 600 government industry personnel attending each training. And she's been doing that for now over a year. In addition, on training resources that ISOO CUI website on this training page has a lot of training videos that we upload easily in MP4 format, right into learning management tools. And we highly encourage both agencies and industry to take advantage of that resource. That concludes the CUI portion of the update.

Mark B.: Thank you, Evan. Does anyone have any questions for Evan on CUI? Alright. We're now at the point of the meeting where we asked for NISPPAC members to present any new business they may have. Anyone have any new business to discuss? Alright. Hearing none. Do any other committee members have any questions or remarks before we close out this meeting today? Alright. Hearing none. Now our next NISPPAC is scheduled for October 27th, 2021. I'm hoping to have the next NISPPAC in person, but we'll also plan to have it 100% virtual, if needed. As a reminder, NISPPAC meeting announcements are posted in the Federal Register approximately 30 days before the meeting, along with being posted to the ISOO blog. Alright, with that, I'm going to wish you all a good day. Please stay healthy, and this meeting is now adjourned. Thank you so much. Goodbye.

Producer: That concludes our conference. Once again, if you have any questions, please forward them to the NISPPAC email address. And thank you so much for using Event Services. You may now disconnect.