Mark Bradley: We are conducting this meeting virtually; we're going to do roll call differently than we have in the past several meetings. We're going to run through it twice, once before the meeting, which is what we're doing now so we know who was able to successfully call in, and once at the top of the meeting for NISPPAC members. Additionally, I'll do another roll call for speakers. I'm going to start with the government members. I'll state the name of the agency. The agency member will reply by identifying themselves and stating whether they are the primary or alternate. If the primary is present, once the meeting is live, we'll meet it 10:00, only the primary will state they're present.

Once I've gone through the government members, I would then proceed with the industry members. If we don't have industry representation, a member of my staff will attempt to track them down before the meeting, see whether or not they're having trouble calling in. Please keep your phone on mute until I have stated your agency. If you do not have a mute button on your phone, hit *6 on your phone. Thank you for your continued patience during this extraordinarily unusual time. Here we go. ODNI, are you present?

Valerie: Good morning. Present and primary.

Mark: You're Valerie Kerben, right? Remember to introduce yourself.

Valerie Kerben: Yes, Valerie Kerben, thank you.

Mark: You're welcome. DoD, are you present?

Dave: Yes, DoD is present with… from DCSA, you've got Dave Stapleton here.

Mark: Okay. DOE, are you present?

Tracy: Yes, good morning. Tracy Kindle, I'm the alternate.

Mark: Alright, thank you Tracy. NRC, are you present? Alright, don't hear anybody from NRC. DHS, are you present?

Mike: Yes, this is Mike Scott and I'm the primary.

Mark: Okay, thank you. DCSA, are you present?

Keith: Keith Minard, DCSA, primary, present.

Mark: Hi, Keith. CIA.

Heather G.: Heather Green, DCSA, present as well.

Mark: Okay, thank you, Heather. CIA? Alright, don't hear anybody. Commerce, are you present? Nobody from Commerce. DOJ, are you present? Alright, nobody from DOJ. NASA, are you present?

Kenneth: Good morning, Kenneth Jones here, primary.

Mark: Thank you. NSA, are you present? Nobody from NSA. State Department, are you present?

Kim: Yes, Kim Baugher, primary.

Mark: Thank you, Kim. Air Force, are you present? Department of Navy, are you present?

Randy: Randy Akers, alternate.

Mark: Thank you, Randy. Department of the Army, are you present? Alright, I don't hear anybody from the Army. Alright staff, we've got some people to track down, it sounds like, from the government side of this. I'm going to now move over…

Heather: **[00:03:31 inaudible]**

Mark: Okay, thanks. Now I'm going to do a roll call for the industry members. Heather Sims, are you present? Alright, we need Heather at some point. Bryan Mackey, are you present? Bob Harney, are you present? It's like we're striking out here on the industry side. Dan McGarvey, are you present? Dennis Arriaga, are you present? Heather, this is Mark. I'm not getting any industry response at all.

Heather: Yes, sir. I'll include them on the email. It is concerning, but I did get an email from Heather this morning, so I'll be sending her a text as well as the email. I've got some people still that I can text them as well.

Mark: I like your **[00:04:34 inaudible]** here as we go through this. Rosie Borrero, are you present? No. Cheryl Stone, are you present? Aprille Abbott? Alright, we just went 0 for whatever it was on the industry side, so we obviously…

Dennis: This is Dennis Arriaga. I'm here.

Mark: Hey Dennis. Okay, good. You're the lone ranger.

Dennis: Good morning.

Mark: You may be doing a lot here, man. Anyway, Heather, please see what you can do to track down our industry brothers and sisters so we can get this meeting underway. I'm going to get the roll call…

Heather: Yes, sir. I'll **[00:05:17 inaudible]** government.

Mark: Yes, sure. I'm going to do a roll call now for the speakers. I suspect we're going to have some who are there and some who aren't. Dave Stapleton.

Dave: I'm here. Present.

Mark: Good. Heather Green.

Heather G.: Present.

Mark: Okay. Devin Casey.

Devin: Present.

Mark: Perry Russell-Hunter. Alright. Roy Jusino.

Roy: Here.

Mark: Thank you, Roy. Gary Reed. Alright. Keith Minard.

Keith: Here.

Mark: Alright. Booker Bland, backup for Keith? I don’t think we're going to need Booker now that Keith is here. Alright.

Booker: Booker's here.

Mark: Great. Donna McLeod. Another backup, **[00:06:21 JJ Robertson]**. Another backup. Selena Hutchinson, another backup, and Chuck Tinch.

Selena: Here.

Mark: Okay, great, thank you. Looks like we're doing better on the speakers. If anyone is planning on speaking during the NISPPAC that we've not heard from, please speak now. Obviously, that would be the industry side which we have not heard from.

Heather S.: Hi, this is Heather Sims, can you hear me?

Mark: Yes, Heather. Good.

Heather S.: Okay, perfect.

Mark: You're **[00:06:55 inaudible]**. Good.

Will: Ladies and gentlemen, welcome and thank you for joining today's teleconference, NISPPAC meeting. Please note that all participant lines are muted. I would like to begin today's conference by introducing today's speaker, Mark Bradley, Director of the

Information Security Oversight Office as well as the Chairman of the NISPPAC. Please go ahead.

Mark: Thank you very much, appreciate that. Welcome and good morning, ladies, and gentlemen. This is the 64th meeting of the National Industrial Security Program Policy Advisory Committee, commonly known as the NISPPAC. We appreciate your patience as we navigate through these extraordinarily unusual times. This is the first NISPPAC meeting that's being conducted virtually. With that being said, we're going to be proceeding a little differently from what we've done in the past. We'll provide a survey after this is done to see how everybody thinks if this workflow did not work. We'll provide the link via the ISOO overview blog after the conclusion of this meeting if we don't give it directly.

A little housekeeping. We're going to try to go as quickly as we can, realizing again we're doing this by phone so I'm going to try to speak as clearly and as slowly as I can since this is being transcribed. I want to make sure we have an accurate transcript. This is a public meeting. It will be audio recorded. About halfway through, we're going to take a five-minute break. Unlike with the registration confirmation stage, we're not going to be using WebEx because there's too many technical challenges for that so we thought we'd rather spend time discussing the substance of the NISPPAC than worrying about who can log on and who cannot. This meeting is going to be done through phone lines only.

If you do not already have the agenda and slides, please go to NISPPAC reports on committee activities and click the first link that pops up through, three of them. This link also has a link to the ISOO overview blog. I'm going to start by asking for attendance from the government members. I'll state the name of the agency. The agency member will reply by identifying themselves by name. Once I've gone through the government members, I will then proceed with the industry members. Please keep your phone on mute until I have stated your agency. As a reminder, if you do not have a mute button, please hit *6 on your phone to mute and unmute. I'm going to start with ODNI, are you present?

Valerie: This is Valerie Kerben, I'm present.

Mark: Thank you, Valerie. DoD, are you present?

Jeff: This is Jeff Spinnanger, I'm here.

Mark: Thank you, Jeff. DOE are you present?

Tracy: This is Tracy Kindle, present.

Mark: Thank you, Tracy. NRC, are you present? Alright. DHS, are you present?

Michael: This is Michael Scott, I'm present.

Mark: Hi, Michael. DCSA, are you present?

Keith: Keith Minard, present.

Mark: Thank you, Keith. CIA, are you present? Alright. Department of Commerce, are you present? Department of Justice, are you present? NASA, are you present?

Kenneth: Kenneth Jones, present.

Mark: Thank you, Kenneth. NSA, are you present? Department of State, are you present?

Kim: Yes, Kim Baugher. Thank you.

Mark: Thank you, Kim. Department of Air Force, are you present?

Sharon: Sharon Dondlinger, present.

Mark: Thank you, Sharon. Department of the Navy, are you present?

Randy: Randy Akers is present.

Mark: Thank you, Randy. Department of the Army. Okay, no. Right now, I'm going to turn to the industry members. Heather Sims, are you present?

Heather S.: This is Heather Sims, present.

Mark: Bryan Mackey, are you present?

Bryan: Yes, Bryan Mackey, present.

Mark: Thank you, Bryan. Bob Harney. Dan McGarvey. Dennis Arriaga.

Dennis: Present, sir.

Mark: Thank you Dennis. Rosie Borrero.

Rosie: Yes, Rosie Borrero, present.

Mark: Cheryl Stone. Aprille Abbott. Alright. That's the roll call. Greg, how's the number… Yes, sure.

Kathleen: Department of Justice, Kathleen Berry.

Mark: Alright, good. DOJ is on. Greg, what's the output? The tally now for the agency and for the NISPPAC? I'm sorry, the industry members in terms of the quorum?

Greg: Sir, we don’t have a quorum because we have four industry members present and we need five. On the government side, let me see, one, two, three, four, five, six, seven, eight, nine, ten, plus you makes eleven, so we actually do have a sufficient number on the government side. We're missing one industry… Mr. Chair, Mark, it's possible, I don’t know, but you're the person coordinating this, correct, for us?

Mark: Yes.

Greg: Is it possible that some of these people have dialed in on the participant line or the general line? I'm sorry if I'm misstating that.

Heather: We do have one that did dial in as an attendee. Do you want us and go ahead and unmute his line, sir?

Mark: Please.

Greg: Who is the attendee? Is it one of the members?

Heather: Yes, sir. It's NSA.

Mark: Oh, so NSA. Okay. It's on the government side, it doesn’t help us on the…

Brad: Hey Mark, this is Brad Weatherby from NSA.

Mark: Hey, Brad.

Heather S.: Hi, this is Heather Sims. We have two more industry members that just came on, Ms. Cheryl Stone and Mr. Bob Harney.

Bob: Hello.

Mark: Okay, good. So that takes care of the quorum issue.

Greg: We have the quorum now.

Mark: Yes, good. Okay, so let's continue. We're expecting this to be the largest audience for NISPPAC meeting in recent history. I think what the moderator said, we have 478 people on the line as of about 10 minutes ago. Because of this, we will not be taking questions from the public during the meeting. Only ISOO and NISPPAC members will be asking questions. We know this is a disappointment for some, however, please free to email nisppac, that's N-I-S-P-P-A-C, @nara.gov with your questions. We will be sure to not only answer appropriate questions, we'll include them in the record of this meeting.

Speakers, NISPPAC members and I proceeding with a question, everyone identifies themselves before speaking each time for the record. Again, this is being audio recorded and it makes it a lot easier to do the transcript if you actually have the name to match with the **[00:14:47 inaudible]**. I want to remind government membership as a requirement to annually file a financial disclosure form with the National Archives and Records Administration Office of General Counsel. Before a government member may serve on NISPPAC and annually thereafter, this must be done.

The same form for financial disclosure used for the federal government OGE form 450 satisfies the reporting requirement. Again, we're not saddling you with additional requirements. It's the same document. If there are questions, please reach out to nisppac, again, N-I-S-P-P-A-C, @nara.gov.

We have several changes to the NISPPAC membership, to draw your attention. We welcome Mark Hojnacke as the new representative from the Department of Energy. He's replacing Marc Brooks. We're also welcoming Dr. Jennifer Obernier as the new representative from the Navy. She is replacing Dr. Mark Livingston. Randy Akers who's the alternate will replace Glenn Clay. Jennifer Aquinas is serving as the new representative from the Department of Air Force. Sharon Dondlinger has been serving as an alternate but will no longer be in that position. Annie Bachhus will serve as an alternate.

Kenneth Jones is now serving as the new representative from NASA while Stephen Payton serves as the alternate. Our time with Bob Harney and Bryan Mackey with industry is coming to an end with terms ending September 30, 2020. Industry, I would like to have your nominations by September 1, 2020 for their replacements so we can keep this train on the rails. Thank you all for your contributions all over the years. We look forward to continuing the work you have done with new representatives. Greg Pannoni, my deputy from ISOO will address the status of action items from November 20, 2019 meeting, our last meeting. Greg?

Greg: Yes, thank you, Mark, Mr. Chair, Director ISOO. Good morning, everyone. What we'll do is first announce that the NISPPAC meeting minutes from the last meeting which was back in November of 2019 were finalized on February 14, 2020. They are posted on the ISOO website. From that meeting, there were 10 action items. Several of them are related so that I am going to address them in groups. Let me start.

The first one concerns NIDs. Actually, there's four of them that concerns the National Interest Determinations and that process. We'll take all four of them together. The first with industry was to provide instances of delayed NIDs processing by the CSA/CSOs. My understanding for that one is that industry is submitting a Freedom of Information Act request for listing of foreign ownership control or influence entities in the NIDs to address that point.

The next one from that last meeting was that ISOO would convene a NISPPAC NID working group meeting in the near future with industry reps, DCSA, to address the challenges of the NID processes. We will be planning to do that in the next 60 days. The next one had to do with industry requested that the NID working… this is really essentially the same thing, working group reconvene to discuss timelines and procedures. We'll do that.

The next one was that the chair requested government and industry provide metrics from the NID working group. That's also wrapped up in this hosting of a working group meeting. We will also have separately a CSA and CSO working group so that the US government can hopefully come together on some of the challenges in the NID process so that that takes care of the four groupings for the National Interest Determinations.

The next action items from the last meeting, there's two that we're grouping here. The first is the access to the defense information for security system, also known as DISS by non-DoD agencies. We had a similar item, the 10th item from the last meeting wherein the DCSA would get back the State Department about their difficulties being able to logon to JPAS. My understanding is there has been a workaround that was provided so we consider this one closed.

The next action item, the third which we're grouping again here is, this is action item three for this meeting, but it turns out it was action items three and eight from the last meeting. That was dealing with insider threat. The action item coming out of the last meeting was the DCSA was in process of internal and formal coordination of an industrial security letter, otherwise known as an ISL that would replace the current ISL 2016-02. That one is in formal review at DCSA and we expect it to be promulgated very soon.

Then the other part of this grouping, also dealing with insider threat, concern having an insider threat working group meeting. Industry requested the insider threat working group reengage to discuss maturity of the insider threat program. Due to competing priorities, we have not been able to schedule that insider threat working group meeting, but we plan to do so in the next 60 days.

The next item concerns the NISPPAC bylaws. We plan to take a vote on this item at today's meeting on the proposed changes. Assuming we get through that, which is coming up next on the agenda, this item will then be considered closed.

The next item concerns industry requesting DCSA reengage with industry on the relationship between the risk integration security oversight program also known as RISO, the defense in transition, also known as DIT, and the tailored security plan, also known as TSP, and the security rating score. This is considered closed because those programs/items are being reworked by DCSA but additional information on these items or at least some of them will be provided as part of the DCSA update.

That concludes the action items from the last meeting. Do any NISPPAC members have any questions or remarks about the action items and their status?

Heather S.: This is Heather Sims. Thank you for the update. There's no question.

Greg: Okay. Anyone else? Okay, Mr. Chair, I'm turning it over to you to move forward.

Mark: Back to me, alright. Thank you, Greg, for that summary. At the last meeting, we discussed changing the NISPPAC bylaws. Government membership with NISPPAC, ISOO listed and accepted nominations from the agency heads. I am proposing to modify the bylaws to allow nominations from either the agency head or the senior agency official for the NISP. We've also made some clarification to the administrative changes in the bylaws. We sent the revised bylaws to the members ahead of time. Before we vote, does anyone have any questions or any concerns before we actually vote? Alright, hearing none. Go ahead, excuse me. Am I hearing something or not? I can't tell.

Okay, good. I'm requesting that we have a phone vote on the change. We need 2/3 of the present government members and 2/3 present industry members need to approve the proposed bylaws in order for them to be amended. I'm going to go like this. I'll say the name of the agency and then please respond with your name and yes or no to the proposed bylaws. I'll ask industry members to vote in the same manner. I'll start with ODNI. Valerie?

Valerie: Yes, for ODNI.

Mark: Alright, that's Valerie Kerben. DoD?

Jeff: This is Jeff. Yes.

Mark: Alright, Jeff Spinnanger, yes. DOE?

Tracy: Yes. Tracy Kindle.

Mark: NRC? I don’t think we have anybody from NRC. DHS?

Mike: Mike Scott.

Mark: Is that a yes?

Mike: Yes, for DHS. This is Mike.

Mark: Alright, thank you. DCSA.

Keith: Keith Minard. Yes.

Mark: Thank you, Keith. Next, CIA? Don’t think we have anybody. Commerce? No one. DOJ?

Kathleen: Yes. Kathleen Berry.

Christine: I'm sorry, from DOJ. Christine Gunning.

Mark: Alright. That was a yes from DOJ?

Kathleen: Yes.

Mark: Alright, thank you. NASA?

Kenneth: Kenneth Jones. Yes.

Mark: Alright. NSA?

Brad: Yes, from Brad Weatherby at NSA.

Mark: Alright. Thank you, Brad. Department of State?

Kim: Kim Baugher. Yes.

Mark: Alright. Thank you, Kim. Department of Air Force?

Sharon: Sharon. Yes.

Mark: Department of Navy?

Randy: Randy Akers. Yes.

Mark: Thank you. Department of the Army?

James: James Anderson. Yes.

Mark: Alright. I as the Chair vote yes myself. Thank you. Now, I'll address the industry members. Please state whether you're voting yes or no to change the bylaws. Heather Sims.

Heather S.: Heather Sims, industry. Yes.

Mark: Alright. Bryan Mackey.

Bryan: Bryan Mackey. Yes.

Mark: Alright. Bob Harney. Dan McGarvey.

Dan: Dan McGarvey. Yes.

Mark: Alright. Dennis Arriaga.

Dennis A.: Dennis Arriaga. Yes.

Mark: Thank you. Rosie Borrero.

Rosie: Rosie Borrero. Yes.

Mark: Alright. Cheryl Stone.

Cheryl: Cheryl Stone. Yes.

Mark: Alright. Aprille Abbott. Alright. Greg, it looks like the motion is carried. Am I correct about that?

Greg: Yes, sir. We have all yeses of everyone that's present. Absent was NRC, CIA, Commerce, and on the industry side, we had two members not present. The voting…

Dennis B.: I'd like to step in. This is Dennis Brady, NRC.

Mark: Okay, Dennis. This is the Chair; we want to ask you how you vote?

Dennis B.: I was on the wrong line. I wasn't present during the roll call. I didn't know I wasn't recognized.

Mark: Dennis, on the bylaws, do you vote yes or no?

Dennis B.: I vote yes.

Mark: Alright, thank you.

Felicia: This is Felicia. I wasn't recognized. I am on the line and I vote yes.

Mark: Alright, thank you Felicia.

Greg: Felicia, I'm sorry. Which agency are you with?

Felicia: CIA.

Greg: I'm sorry. Okay, thank you.

Mark: Okay, got it. Got it. Good.

Greg: Now we have 15 yes on the government side with one not present being Commerce. It looks like the motion is carried.

Mark: Alright, the motion is carried. We will amend our bylaws accordingly. Thank you. I appreciate your work on that and your close attention to reading it and making your closing comments. This time, we're now going to introduce our speakers for updates. Valerie, is Gary around?

Valerie Heil: Yes. I'm sorry. This just moved a little faster than we expected, so we're following up for Mr. Reed to call in in just a moment, if you can give us…

Jeff: This is Jeff. Mr. Reid is on so we're just working through the mechanics to get him live. Give us a second.

Mark: Just let us know when he's on. I'll be glad to introduce Gary.

Gary: Okay. I think I got unmuted. Can anyone hear me?

Mark: Yes. Gary, this is Mark. Let me introduce you, then I'm going to turn the mic over to you, okay?

Gary: Okay.

Mark: Alright. I'm privileged to introduce Gary Reid, Director for Defense Intelligence, Intelligence and Security, Counterintelligence Law Enforcement and Security who will give you update on behalf of DoD as the NISP executive agent. Alright, Gary. It's all yours.

Gary: Thank you very much, Mark, and good morning everybody. I'll be brief. Trying to talk to 500 people at one time. Just a couple of high-level thoughts from the Pentagon here on behalf of the Secretary of Defense and the Undersecretary. A lot of movement in the space around the security portfolio across all aspects, not just limited to the NISP, but everything we do here ultimately affects all of you in one way or another.

If you saw Secretary Esper's HASC hearing last week, he indicated his views on leaks and unauthorized disclosures and OPSEC in general. I just want to share with you briefly that you are going to soon learn more about an effort we're going to put underway in his direction to really make a dent in the defense enterprise in our views and our behaviors relative to operation, security, and protection of sensitive information and prevention of unauthorized disclosures.

A lot of the effort we're putting into this will come in protecting predecisional information, not necessarily national security information. We don't need to change the rules for national security information. We just need to enforce when there's violations, and you see a lot of that. You see that in the paper. You see federal cases coming to closure. But below that level is where the real nuisance problem is, and that is leaks of predecisional information.

We're going to move forward with putting OPSEC CUI into effect very soon for DoD. That will start a process of changing how we handle that information and that will flow across the department. That's a major undertaking. As this group knows, we've been talking about CUI for a while. This will probably be the largest effort on scale to start imposing CUI markings and controls, and it will be on the OPSEC category.

We are still obviously working with DCSA on CUI on the sensitive, I forgot the term, technology information, critical technology. We'll talk more about that in a second. But I just wanted to tease that out for you. You're going to hear and see a lot on that, and we would invite everyone's cooperation and collaboration on getting this… DoD is a lot of things, but I don’t think we're notorious for being really good at controlling information. We're such a large organization.

This is going to start here with leadership. It's going to emanate out in the Pentagon. It's going to resonate very quickly into major command headquarters, but ultimately trickle down to every member of the department. You'll see training materials on DCSA's website. You'll see personal message from the Sec Def. He's very involved in this. I just want to share that with you.

The second thing I want to lead off with is on DCSA and it was just mentioned earlier, things like SRS and tailored security plans. Here's what you already know. We have a new leadership team at DCSA and a new cadre of leaders coming onboard. With change of leaders comes refresh and reset. At a time when we are still absorbing, internalizing, and operationalizing the transition from DSS and NBIB into DCSA. That includes major changes on the technology protection, industrial security side of the ledge, not just on the background investigation.

I would ask everyone's patience as we go through this leadership reset. Director Lietzau has made some really powerful decisions on bringing on a team that can join those that are already there and accelerate efforts that affect this group the most on the tech protect side. You're going to hear from them later in the conference or on the call, so I won't go into that anymore. Only just to say that obviously we've got to do some resetting.

DCSA is doing a fantastic job of keeping missions going on both sides, again, background investigation side and industrial security side, but we have a long way to go as a department and they have as an agency to say what I would call a normalized posture as this new defense agency.

We got to do the day to day missions. We got to protect the things we have to protect. We have to support the things we have to support. But we also have a vision and a strategy for reaching a higher level of integration across the agency, and that is what they're working on and what Mr. Kernan has put in motion. A lot of movement there.

The last point I want to make just relative to the NISPOM. Again, just share with you, we are still plugging away. Jeff Spinnanger is leading to get our NISPOM change proposal out of legal and into OMB to get into the rulemaking process. We have a hard deadline, as many know, at the end of July. We're just days, hopefully, soon to be hours away from getting us out of legal. It's a quite complicated document.

A lot of changes. The most substantive change will be in the area of SEAD 3. The reporting requirements on SEAD 3 has been on the street for quite some time. We're still working across the rest of the department to get the procedures in place and getting this written into the NISPOM is an important step towards sending that out to industry. Again, the dialog is important. The collaboration that we enjoy with this group is very important to our success.

I just want to thank everybody for your patience under these crazy times that we're in and we'll keep plugging away and look forward to achieving some of these near term goals and setting these long term benchmarks for things like how does the DCSA … in the future in a more integrated way and those kind of topics. How do we get to the visions that frankly Stan Sims and Dan Payne put in motion about tailoring and focusing NISP on not so much a repetitive process but a threat-based process? How do we actually get to that?

As everyone knows, we've been doing this for a minute. We’ve thrown some spaghetti on the wall here in the last couple of years and we're still, in my own view, are looking for the right formulation of how to get the most out of the resources that we have, how to be the most effective during this time where our technologies are under continuous attack from foreign intelligence entities. Nobody's satisfied, frankly, with the level of protection we have across the board. Everyone's interested in how to do it better. It's going to come out of this group and others to come up with the best idea to do the most with the least amount of resources and cover the most ground in the most critical areas.

That work has come very far, but it'd be wrong for me to say that we're near completion. Some of this is things that are never actually complete. It's a constant state of improvement and refinement. But you can't operate like that in the dark every day. You have to have a set of rules. You have to have a set of produces that everyone understands. That's the day to day part that we move along as we work towards the longer strategic objective. Thanks for everyone pulling this together and I look forward to hearing the discussions and continued collaboration. Thank you very much.

Mark: You're welcome, Gary. Anybody have any questions for Gary? Alright. Thank you again, Gary. That was an excellent summary. I'm now pleased to introduce Dave Stapleton, Assistant Director of Critical Technology Protection for the Defense Counterintelligence and Security Agency. After Dave has spoken, we'll hear from other members of the DCSA staff. Alright, Dave, take it away.

Dave: Good morning. It's an honor to be here having joined DCSA just this past month. I would just say that as assistant director, we look forward to upcoming engagement with cleared industry and government partners. Mr. Lietzau who joined DCSA as our Director starting in March of this past year, replacing Mr. Phalen, apologizes for not being able to attend this meeting but he will be planning on attending the NISPPAC in the fall.

On his behalf, I'd like to pass on that we would like to thank our industry and government partners for working with DCSA as we continue the NISP mission while under the constraints of COVID-19. We're working on a reconstitution plan. While we do not know when we will be back to business as usual, we will keep industry informed as we make changes.

Let me conclude by stating that we are on the frontlines of economic competition against near peer and peer adversaries, and our partnership with industry comprises the tip of our economic spear. We look forward to working together with industry to protect our security of our nation and the free world. We greatly appreciate your support. Thank you all.

Mark: Thank you, Dave. Any questions for Dave? Alright. Thank you. Next, we have Heather Sims, the NISPPAC industry spokesperson who'll provide the industry update.

Keith: Mark, this is Keith. I was gonna start the DCSA updates.

Mark: I'm sorry, Keith. You know what, I tried to read my talking points in front of me, I'd be dangerous. Sorry about that. Yes, please Keith. Go.

Keith: It's okay. I appreciate the time.

Mark: No, not at all.

Keith: Good morning. Keith Minard, DCSA. First, I would like to provide an update on our operations under COVID-19 because I think this is a key and critical update to show the work that's been going on during this very challenging time. As you all know, COVID-19 has impacted the entire NISP community. In order to address these impacts, DCSA has implemented a wide range of initiatives to ensure we continue our engagement with industry and our government partners to continue our oversight and support to the NISP.

Some of these changes include moving to continuous monitoring process for conducting assessments instead of onsite visits. We'll continue to process FCLs. We are still holding FOCI and national annual meetings in virtual formats. We have modified our processes for approval of safeguarding, and we'll continue to process new and existing ATOs that we are deferring the onsite assessments.

I do need to mention the staff from OUSD (I&S) and ISOO who are invaluable in assisting on a wide range of issues as a department in national level which included GSA overnight safe carriers and guidance that came up for underwriter's laboratories regarding monitoring station changes due to COVID-19. Great value in the team effort on this to get the right information out to industry and continue to put that information together so we can keep industry moving forward in these programs.

While we still have challenges due to COVID-19, engagement with industry and our government partners has enabled DCSA to continue support to the NISP while working to minimize impacts. Since March, we've actually had weekly calls between DCSA and the NISPPAC industry spokesperson to address key issues and impacts and rapidly work to identify resolutions. This really enabled us to address and work quickly to provide updates and enable guidance on these critical issues to keep industry moving. I will note that the slides on the website include more information on DCSA ATOs on stat and timelines. There'll be no specific briefing in this, it should be on NISPPAC, on our ATO side.

Mr. Reid mentioned Security Executive Agent Directive 3 which the reporting guidance. Just late last fall, industry had an opportunity to review the ISL which will be a companion document to the NISPOM revision as it comes out. What I'd like to note on that is we are currently planning communication guidance and resources to aid in this implementation as we did for insider threat 2016. We see that SEAD 3 requires the same level of effort as a community to make sure we're successful in those requirements.

While we're waiting on the NISPOM revision to be issued and we'll also incorporate the ISL, we do need to begin planning for these requirements. Our internal staff planning is ongoing. We'll be working to schedule engaging industry to NISPPAC to begin planning for these requirements because we see a need for tools training and resource to support implementation. We know that we're scheduled here in the near term to scheduled industry to start that engagement strategy.

The next thing I think is one of the bigger things we'll talk about today is the Defense Information System for Security ISL. We appreciate the comments and the coordination effort that OUSD (I&S) did with the NISPPAC and coordinate with this ISL which is… this is the replacement for JPAS as a system of record for personnel security.

What I would like to note today, and we've already informed the NISPPAC spokesperson that we have made administrative updates to the ISL 2011-04 adverse information. The administrative changes address the use of DISS for the submission of incident reports and adverse information. We'll be working to post the updated ISL and notice to the DCSA website by the end of the week. This effort's been in coordination with staff elements of DCSA, OUSD (I&S), DoS, and DMDC.

Some key points on this. To ensure you'll be able to submit incident reports, contractors how have not obtained their DISS accounts should do so as soon as possible. The transition to DISS for incident reporting will occur on August 15, 2020 and the ISL does include links on access information email for the DISS support team and links to training on adverse information reporting to better enable industry in this transition. Both to make sure that the staff that manages the DISS side of the house from DCSA is engaged on this and make sure that any issues or challenges are addressed along the way till we hit the August 15th mark for transition.

The next update is on FCL timelines. The entity vetting components of DCSA which includes now the former facility clearance branch and FOCI branch has seen timelines dropping since their merger as a single division that handles end-to-end process under FCL and FOCI, now called entity vetting. Based on the organization change, our focus strategy, we are seeing some reductions in timelines and we will surely keep industry updated on improvements. We also see efficiencies in processing as we bring additional staff on board in the next few months.

I know that in the action items and Mr. Reed mentioned this is that there are some changes in DCSA, and we are looking at prior efforts. An example to prior efforts that we're looking at is the standard practice and procedure process that’s been recently engaged with industry on through the NISPPAC spokesperson and there's been some discussion on this. We are taking strategic pause in some of these efforts as we move forward to ensure we keep industry members of the NISPPAC engaged on initiatives and also as we move forward to reengage on some of the strategies.

The last couple items I have are actually on systems updates. I know that NISS usually is something that comes up because of latency and other issues but I would like to say that for the National Investment Security System, NISS, this month, DCSA is assessing output in the application monitoring tool and will be planning improvements to NISS application infrastructure to improve system performance. What we'll need is feedback on how that goes along the way over the next month or so to make sure that we can validate that the change we're making actually do the things we need them to do.

The last note I really have is on NISP Contract Classification Security System is the federal acquisition rule has been issued on NISP NCCS for the government 254s, the Contracts Classification Specification. It'll have an effective date of August 3, 2020. It will address use of NCCS by DoD and non-DoD service branch signatories for industrial security services. I would ask everybody to go look at the rule and if you have any questions, please contact DCSA before changes are applied to solicitations issued on or after the effective date of change. Contracting officers may actually use the rule retroactively but as far as DCSA's view on this, it's used on the way forward for new 254s.

Now that the rule has been issued, DCSA will begin an increased engagement strategy for deployment working primarily to the NISPPAC NISS systems working group, which was just recently established, and we'll have more to follow on that. DCSA staff will provide additional tips on personal security clearance during the working part of the agenda. While not really in the office, DCSA is here to support you today as we were prior to COVID-19. Thank you.

Mark: Does anybody have any questions for Keith?

Greg: This is Greg Pannoni, ISOO. First of all, thank you very much Keith for that comprehensive update and the note of ISOO support and others. Just a little bit more on this transition to DISS on the date. I heard you say August 15th, is that a hard date that JPAS is cutoff on that date or… because I thought JPAS would not be cutoff until the end of the calendar year. We talked a little bit about it during our clearance working group. Just if you could give us a clarification on that point, please.

Keith: As I mentioned, this is for incident reporting and adverse information reporting. It's transition of a module.

Greg: I see. Okay, very good. Thank you.

Mark: Okay. Any other questions for Keith? Keith, is that the end of the DCSA update?

Keith: That's it.

Mark: Okay, great. Thank you. Next, we have Heather Sims, NISPPAC industry spokesperson who'll provide the industry update. Heather?

Heather S.: Good morning. This is Heather Sims. It's a pleasure to be able to provide the National Industrial Security Program Policy impacts from an industry perspective today. To say the least, it's been a busy and very unpredictable year thus far. What hasn't changed, industry's active involvement monitoring all the moving parts of the NISP that may have an impact on the industrial base. Today, I'll provide just a few topics being monitored, tracked, and worked by the industry NISPPAC members and many of the industry association.

Industry has encountered an enormous amount of change these past few years and we're noticing that this is increasing at a much faster pace than anticipated. Understandably, due to the increased threats towards US interest, it's more important now than ever that industry in the United States government gain fidelity on the cost of the NISP implementation before any additional reforms and policies are considered and implemented.

I will also now is the time for industry to be united in our efforts in addressing our collective concerns for the benefit of the entire cleared industrial base. Together, we are stronger. I ask that the NISPPAC industry members are utilized to the extent possible to address industry's NISP concerns with the United States government.

New legislation, development of policy, and the variances in which federal agencies interpret and then implement has cause a strain to industry that could impact our ability to provide the needed services and products to assist the United States government in maintaining its competitive edge over our adversaries.

Industry is continuously tracking new legislation and policy changes that were having overarching impact on industry's operations. Some are minor and have been anticipated while others will have a major impact on our way of doing business. On the surface, one section of the legislation may not cause concern, however when combined in a collective with all the other new policies, it may have an administrative and resource strain on the industrial base.

Industry must closely follow legislation and policy from development to implementation. As often seen a well-intended policy is as only as good as it is implemented at the lowest level. In many cases, the way an agency or department interpret a new policy sometimes has an even greater effect on industry, often adding unnecessary administrative burdens when not accompanied by a strategic vision or communication.

Through the NISPPAC, we can better shed light on industry's challenges in a collaborative environment proactively. While I don’t have time in this forum to address all of industry's interest and concerns with legislative impact, I will speak to a few key sections of the National Defense Authorization Act for fiscal year 2019 that has our interest.

Section 889 prohibits the federal government from procuring or obtaining or extending or renewing a contract to procure or obtain a new equipment, system or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system. This prohibition takes effect August 13, 2020.

Considering the impacts foreign COVID-19, industry associations have recommended language to extend Section 889 implementation. While we understand the need to combat the national security and intellectual property threats that face United States, there is still a lot of unknown implications to this rule. More collaborations with the United States government is required to ensure no disruption to services or products provided and to better understand how federal agencies intend to implement the processes they will put in place for cleared industry to ensure compliance.

Industry is confident that NISP supply chain topics will be the focus for the foreseeable future. Industry recommends the creation of a

NISP product supply chain working group for discussing the impacts to the proposed or approved legislation can be addressed, and as a team, we can find viable solutions to our shared concerns about the risk to the supply chain.

National Interest Determinations, NIDs, timelines and processes are still a perceived concern for companies under foreign ownership, control or influence that have a requirement for a NID. Delays on the process affects the ability of contractors to meet contractual obligations.

NDAA Section 842 eliminates the NID requirement for covered National Technology and Industrial Base companies beginning October 1, 2020. Industry will look into United States government for additional clarity and guidance to all contracting activity. It is recommended at the next schedule NIDs NISPPAC working group to discuss the current NID process, identify gaps and work to find efficiencies in the process to limit processing timelines.

Currently, NISPPAC industry does not have a full listing of companies under a NID obligation to better understand the full impact of the issue from an industry perspective. Industry is working on a Freedom of Information Act request to obtain the information so that discussions can be started with affected companies to better understand the impacts and areas of concerns. Industry continues to work with the United States government on the overall process to improve timelines on NID approvals.

While industry has expressed concerns about the United States government's ability to share threats, adverse and insider threat information for decades, there's still work to be done. Section 9403 of the NDAA federal policy on sharing of information pertaining to contractor employees in the trusted workforce is the first step to improving that gap. Although industry was treated an equal partner in the full spectrum of information sharing, we are limited on our visibility of the potential threats. Information sharing policies should take into consideration protection for cleared industry to share relevant information between cleared companies and the United States government without the fear of reprisal.

There are many other sections of the NDAA that affect industry's involvement in the NISP. These will be tracked, and the industry impacts collected to the NISPPAC policy working group for discussion with our government partners. In the future, it is beneficial for industry and the United States government alike to understand and knowledge impact to operations early in the process with a partner to find amenable solutions.

Industry has and wishes to continue to be an active partner on working groups to provide expertise early in the planning process for all aspects of the NISP. With that said, industry would like to acknowledge their appreciation to many government partners over this past year. ODNI, OPM, and PAC PMO have increased their collaboration with industry NISPPAC members on vital personnel security reform. We look forward to continue discussions as the government develops and implements this reform.

Additionally, DoD and DCSA were quick to act and increase their collaboration with industry on the onsite of COVID-19 to better understand the impact to industry. Albeit collaboration had already increased prior to COVID-19. It was appreciating the level of involvement and effort by DoD to get industry guidance on several operational impact. Industry encourage this type of collaboration on all levels on a continuous basis and not just during the crisis.

Industry is closely monitoring the impacts of new legislation and policy, but we're also still focused on many of the CSA agencies' efforts to provide oversight of the industrial base. At the November 2019 NISPPAC meeting, I spoke about the 2020 industry's key efforts we were focused on. At that time, it was the DoD which started security maturity model certification risk management, insider threat and personal security reform.

While CMMC is about to be implemented through the DoD's cleared contracted date, industry still have concerns about the level of the efforts, duplication of oversight and how the rollout will impact industry over the next few years. As noted previously, ODNI, OPM, and PAC PMO have been working with industry in personal security reform. While there is still some implementation unknown, the transparent discussions through the process are appreciated.

The NISPPAC industry threat working group met after the last NISPPAC meeting and is working on updating **[00:58:00 inaudible]** anticipation of an updated industrial security letter. Industry is still closely monitoring DoD's efforts to move the NISP from a compliance-based program to a more risk-based process. While industry understands the reasoning, there have been processes developed over the last two years and tested in certain segments of industry resulting in an administrative and financial burden for companies without an associated policy of contractual obligation.

While the process appears to be on hold for the moment, industry is still concerned about new processes for telesecurity plans being developed under the names Standard Security Processes, SPP, development of the security rating score and other oversight procedures with little industry engagement at the NISPPAC level.

A strategic vision and communication strategy of efforts would be beneficial to industry and the government customers that DCSA provides oversight and support of. As DoD has the predominance of the cleared companies in the NISP, industry would be interested in being engaged fully with all CSA as the new oversight procedures are developed. There's always a continued need to improve strategic communication of efforts, transparency of processes, consistency across the nation and understanding industry's inputs. Together, we can develop solutions to better protect the nation's critical information.

One notable area that industry has been exerting an enormous amount of resources is managing all the government systems being developed and utilized to manage the NISP. Many systems have come online and/or developed at the same time. While looking at one system might not seem to be a concern but coupled with the lack of strategic planning or communication issues, these are amplified when promulgated to industry. There's also system latency and data integrity issues affecting the industries. Without a full understanding of the impact for any new system, process or procedure, the role of the facility security officer or any NISP security professional can quickly become riddled with administrative burden that move them away from actually performing security functions and moving them to more risk-based approach.

Industry looks forward to assisting our government partners in understanding our challenges so that collectively, we can work on viable solutions that industry at large can meet the NISP regulatory requirements, ensure our company's viability in the US and global markets and maintain a viable secure supply chain so that we can get a balanced approach protecting our national security.

One administrative note before I end, industry NISPPAC has started the process on the nomination selection for two new industry NISPPAC members and will have the proposed member nominations to the Chair no later than September 1, 2020. Thank you for your time and allowing me to provide updates today. I look forward to our next meeting hopefully in person. Thank you.

Mark: Thank you, Heather. Anyone have any questions for Heather? Alright. Hearing none. I'll turn to Valerie Kerben, ODNI, who will provide the ODNI updates. Valerie, the floor is yours.

Valerie: Hi, good morning. Thank you, Mr. Chair, for the opportunity to brief at this virtual NISPPAC meeting. I wanted to begin with some updates to where we are with the response to COVID. Of course, with the stay-at-home requirement, DNI had some very limited staff in the office. However, we were closely monitoring and had key staff in the office monitoring the government-wide databases of scattered castles and continuous evaluation.

On the policy side, some important things which I'll discuss this morning have moved forward and some things have been signed. Also, we were working on legislation as well and responding to CDAs. We did have discussions, engaged discussions with our Director of the National Counterintelligence Security Center, Mr. Bill Evanina, to evaluate the process and look to streamlining for NIDs as we've all discussed prior and also with what was discussed earlier by Heather and Greg.

One important thing to note is the Director of National Counterintelligence and Security Center was confirmed by the Senate in May, and Mr. Evanina continues to be deeply committed to the NISP program and our partnership with industry and committed to the trusted workforce efforts.

To begin, one of the important policies that did come out and was signed on May 18th, the Security Executive Agent Directive 8: Temporary Eligibility was signed on May 18th by Director, Acting Director at that time, Grenell. This establishes the requirements for authorizing temporary access to classified information, temporary access to a higher level of classified information, a one-time access, and also temporary eligibility to hold a sensitive position or to hold a higher level of sensitive position when the interest are determined to be in the national security interest prior to the completion of a required background investigation.

This policy was distributed to our department and agency heads and also to the TOCs and our Security Executive Agent Policy Advisory Committee. Hopefully by now, you all have seen it. We will ask that ISOO send it out to our NISPPAC members if they have not seen it yet. However, it is posted on our ncsc.gov website. Additionally, a congressional notification was drafted for our oversight committee and as of tomorrow, there will be additional questions addressed at the background investigation stakeholder's committee hosted by DCSA.

The next policy update is Security Executive Agent Directive 2. As you know, this was signed in 2014. It's for the use of polygraphs in support of personnel security determinations for initials or continued eligibility for access. Since this was issued, there have been a lot of other policy updates. In addition, the National Center for Credibility Assessment, NACA, is going to transfer from the Defense Intelligence Agency to the Defense Counterintelligence and Security Agency.

Due to the impending transfer, it was important to update SEAD 2 to reflect the new authorities and also to explain that there will be a co-chair of an advisory board with the SecEA and OUSDI. This went through some formal agency concurrence and we just received clearance from OMB for it to come back to the DNI and it will go to our internal review and hopefully be issued very soon.

Now, to talk about Trusted Workforce 2.0. The executive steering group, the ESG, as I've mentioned in prior meetings, made up of senior leaders from ODNI, OPM, OMB, DoD, DHS, FBI, and the IC, they were meeting monthly and also during COVID, they continued to meet virtually and continued the momentum to move things forward. The executive agent staff along with our partners at PAC PMO meet regularly to work on the policy construct for the next set of documents in the policy framework.

Also, as mentioned before, there were three top level documents to implement and give direction to the executive agents and agency head. One of the documents that did come through is the executive correspondence. It was jointly signed on February 3rd, and this was transforming the federal personnel vetting measures to expedite reform and further reduce the federal government's background investigation inventory.

This EC amounts to new approach framework for federal personnel vetting to ensure the entire federal workforce is trusted to protect people, property, information, and mission. In addition, this EC directs additional measures to continue to improve effectiveness and efficiency and reminds agencies of the continuing applicability of previous guidance. It also included the clarifications and revisions to the existing federal investigative standards and gave the investigative service providers authorization to use a broader spectrum of investigative methods which actually is very pertinent now during COVID.

One other important aspect of this EC to drive early adoption for compliance with periodic reinvestigations through a continuous vetting program. A lot of this information was also captured in fact sheets summarizing the EC contents. These fact sheets were distributed to the departments and agencies as well as a public version. Additionally, a congressional notification was sent to our oversight committees and will again ensure that our NISPPAC industry members have been informed of the information and given a copy of this EC.

Just a few other next steps and additional collaborations that have taken place. The core vetting doctrine was also pushed through for informal agency review. The executive agent's PAC PMO convened two virtual tabletops with our agency policies meets in late March. Also, in late March, the executive agents coordinated hosting of virtual meeting with ISOO and our NISPPAC members providing an overview and intent of the document, very good conversation and feedback was exchanged, and incorporated some of those edits into our final version. The core vetting doctrine was approved by the executive agents to go to OMB OIRA on June 22nd for formal interagency review. Comments were due back to us on July 2nd. I know we have received a few comments and we're going to be adjudicating those shortly.

Additionally, the EAs and the PAC PMO hosted another quarterly meeting on June 30th with our ISOO and NISPPAC members to further discuss the core vetting doctrine and also provided updates and address any other questions and concerns. We do promise to continue our dialog with our partners from industry as we move forward with more modernization of the federal workforce vetting process. Thank you very much for the opportunity to brief you here today.

Mark: Thank you Valerie for your excellent summary overview. Any questions for Valerie? Alright, hearing none. Up next is Devin Casey from my staff to provide an update on the Controlled Unclassified Information program, also knowns as CUI. Devin?

Devin: Hi, good morning. As mentioned, I'm Devin Casey and I'll be providing an update on the Controlled Unclassified Information program. Thank you for your introduction.

First, we'll start with agency implementation progress, CUI Notice 2020-1 and Agency Reporting. CUI has a section in the annual report where we reported on the progress of agencies implementing the CUI program. As mentioned during our last presentation, this is the year where we expect to see most agency's CUI policies published and finalized, which is really the first domino to fall at agencies for implementing their CUI programs. The rest of the dominos of training and physical security, marking and the other elements of the program fall rather quickly after that.

We did put out CUI notice 2020-1 which describes the deadlines for implementation in order to help agencies as they were finalizing their implementation plans and steps to implementing the CUI program. There's a bit more of a coordinated approach and preparedness to meet the deadlines and requirements of the CUI program across the executive branch as the transition period for agencies and industries and all of our other stakeholders is one of the areas that is a bit more difficult under the CUI program. The establishment of deadlines helps to bring the different agencies in line with their planning efforts to implement the CUI program.

We did request agencies report on the status of their program again this year. It's published through our CUI website and our request for the annual reporting on the status of their CUI program, and reports are due to our office on November 1. We are allowing a 60-day extension due to the COVID issues that can cause delays in gathering information at an agency.

Our office has been providing a lot of updates and information. One of the most attended updates that we've been doing is our CUI marking class led by Charlene. It's a WebEx class. Anyone can attend the class to learn more about CUI and CUI markings. It is not required and does not replace any agency-specific training, but it may be helpful for many people who would like to know more about CUI and how it can mark on the CUI program. The training is based off of the 32 CFR 2002. The next class that you can sign up for or attend through our CUI blog is on July 23rd from 11:00 am to 1:00 pm. Again, you can find out about that on our CUI blog.

We've also published some CUI notices. 2020-03 is a nondisclosure agreement template. This was in response to a lot of agency's… they're asking to update existing nondisclosure agreements that they had or to begin using non-disclosure agreements to protect or identify the responsibilities to protect CUI. We did provide a template for agencies to use. The intent after getting a little bit more data about how these templates are used and from agencies that begin using it is to work towards a standard form.

We also released CUI Notice 2020-02, marking alternative notice that specifically looks to address how alternative markings can apply and when they apply, as well as a notice on the usage of NIST 800-171-A which is the assessment criteria for NIST SP 800-171. It outlines that in NIST SP 800-171, the formal way for assessing the effectiveness of the controls implemented in 171 are documented in NIST SP 800-171A.

We also have a current ongoing effort where we're looking to address the potential for insider threat in the CUI environment. We've worked with the National Insider Threat Taskforce as well as OMB on efforts to provide CUI understanding to the insider threat environment, as well as receiving an insider threat understanding Interviewer the CUI environment. There definitely seems to be a significant amount of insider threat potential in the CUI environment. We want to make sure that we're adequately preparing agencies with the information they need to address that threat and address that risk as they implement their CUI programs.

We also have a CUI metadata standard. It's a standard, not the standard. Big note here, CUI does not have a built-in requirement for metadata tagging or marking. It is an optional practice that agencies can use to support their CUI programs, whether it's supported automated accessing controls or supporting machine marking or automated marking of information, metadata marking is allowable. We work with the National Information Exchange Model or NIEM to create a standard as well as a domain in the new NIEM architecture which will allow for either a single point of translation or a good reference for anyone who is setting up metadata marking schema to pull from one that has already been created and vetted by our office.

That is currently out for comment. You can find out more about how to comment on our CUI blog. It is out for comment, it is NIEM Revision 5.0 Beta 1. There's a blog post that points you to the NIEM website for how to provide comments to that. Again, it is not a requirement, the CUI metadata mark, but if you are going to mark it, we recommend either using that schema or adopting from that schema to ensure the best compatibility with other entities. Comments are due by July 17th. NIEM has mentioned that they will accept comments after that close date as long as you follow the commenting process outlined on their website.

We will also be having a CUI stakeholder update. We did have an ad hoc one on Monday talking about the NIEM metadata marking. We will be having our regular quarterly update on July 13th. Two more quick notes. NIST 800-172 which is additional controls, they're enhanced security requirements for protecting controlled unclassified information, a supplement to 171, formerly known as NIST 800-171B. It's out for public comment on the NIST website. You can get there by Googling the NIST website or by going to our blog where we link directly to it. Comments are due by August 21st, and there's a discussion of the purpose and intent behind this 800-172.

Finally, GSA has the unified agenda regulatory and deregulatory action has been updated for the spring 2020 estimations. The CUI FAR case is still on the unified agenda and the projected comment period, and again, this is an estimated and projected comment period, is from October 2020 to December 2020. You can find more about that on our CUI blog as well.

You probably heard me mention the CUI blog a lot of times. So far, we do put a lot of our information on the CUI blog or the CUI website. You can get to both from either. To stay updated on the CUI program, please feel free to reach out to us through either our email address on the website or through comments on the blog, and we're happy to answer questions. Again, we will have a regularly scheduled quarterly update to stakeholders that has a significant period for question and answer. Unless there are any questions on the CUI program, that's it for me.

Greg: Devin, this is Greg Pannoni, ISOO. Thank you for that comprehensive update as well. I believe you said July 13th for the CUI stakeholder update. Did you mean August 13th?

Devin: Oh, sorry. I have two dates here. July 13th, I did, correct. I did, yes.

Greg: Do we have that date for the next one?

Devin: Yes, it is on the blog.

Greg: We can always email it out if you don't have it ready or I suppose…

Devin: I have it. There's a full post on it on our blog and we can email it as well if needed. I copied over the wrong date.

Mark: Okay, we'll bump that out.

Devin: I copied over a date for the ad hoc meeting.

Mark: Not a problem. Okay. Any questions for Devin? Hearing none, we're going to take a five-minute break now. Please be ready to resume promptly so we can remain on schedule. I think we're actually ahead, which is good. Will from Events Services will then mute the bridge so that only those on the speaker line can speak and hear until we resume the call. He'll then unmute the bridge after the break. My watch is showing exactly 11:15, so we will resume promptly at 11:20. Okay, thank you.

Okay. Welcome back everybody to the last bit of our NISPPAC meeting here. One quick announcement. Devin was kind enough to track down the CUI stakeholder's meeting. It'll be on August 19th. Again, that is August 19th. I'm going to now turn to Greg Pannoni, my deputy, who'll provide us with an update on the NISPPAC clearance working group. Greg?

Greg: Okay. Thank you, Mr. Chair. We've heard all of you already. We've heard from two of the CSAs on a number of the higher-level points that we discussed during our clearance working group meeting which was held on July 2, 2020. We are going to meet on a number of things moving forward that have come out of that meeting. I'll just cover some of the things that we didn't discuss already that occurred at the working group meeting.

One item is cost collection data. You may be aware, if you reviewed the ISOO annual report that recently came out to the President, that we ISOO are undertaking a holistic view of the data, the various data that we collect, why we collect it, how we use it, we report to the President, of course. The data is, we believe, should be tethered to requirements in the executive order and the… well, more than one executive order, the one for the classified program, the NISP and the directives that emerged from those executive orders.

We've been looking at this at least for over a year now. We're trying to streamline it. We're trying to make it more efficient, easier to collect, methodologies for collecting. I'm sorry, did someone say something? Okay. The part I wanted to mention is the data that deals with cost collection specifically for the NISP. It bridges both executive orders, the one for the classified program and the one for the NISP, and there's sort of two buckets of information dealing with cost. There is the bucket that all the agencies that have NISP programs are to report for their management and administration of the NISP. That's at least the 16-member agencies of the NISP and others, of course. Then there's the bucket that deals with the cost that industry extends to implement and monitor their responsibilities under the NISP.

We haven't looked at these things in quite some time. We had a meeting specifically on cost collection, I can't recall the date now, I want to say it was early May, where we invited the government members to discuss cost collection. Out of that, we are planning for another meeting. We want to start with the bucket that deals with the industry cost first. As far as… and what we're planning is mid-August, I think, or early August to have that next meeting.

The idea is to first get the government members on the same wavelength, so to speak, in terms of the particularly significant elements that comprise expanding resources for implementing and monitoring the NISP by industry. Then we would bring industry in to obtain your feedback on this as well. We don't have a specific timeline for all this, but ideally I think we'd like to aim for by the end of the calendar year to have something set up so that for FY 21, at least for a good part of FY 2021, we'll have a mechanism in place for providing more appropriate, more pertinent cost data relative to industry's expenses in implementing the NISP.

We recognize we need to do this on the government side as well, not just for the NISP but for other aspects of implementing and monitoring classified National Security Information Program. That's something on the horizon.

NISP systems, that was already mentioned, forming a working group. Our plan is to have that initial meeting in mid-August. We obviously talked a lot about trusted workforce and we're going to have Heather Green come up next here after me to give more detailed information on that. Of course, Valerie Kerben provided discussion points on that.

I would think one important point just to emphasize, first, it's been a tremendous… two points. It's been a tremendous I think success that has emanated from this undertaking of trusted workforce. We're doing this now in phases as most of you probably know. Instead of going right to 2.0, because there's challenges to get there quickly, it's been segmented into 1.25, as I understand it, and 1.50.

The key point I just want to drill home here is deferred PRs and transfer of trust. If an agency is enrolled in 1.25 and have at least minimal core evaluation to databases, maybe not all the way to the 2.0 level, then that means that individuals that are enrolled in that evaluation who've already been vetted and cleared, their PRs are deferred, and therefore, all things considered, not being anything significant in terms of something that would indicate a concern with that individual, there should be seamless transfer of trust. That’s an important point.

The industry members had made a recommendation when we met during the PAC PMO that Valerie Kerben referred to that a communication plan be put forth from a high level by the PAC PMO perhaps that addresses this issue about transfer of trust, what we used to call reciprocity, and also about training as we move forward, Trusted Workforce 2.0. I think that’s a good recommendation. Could help. I think it would help with minimizing issues with transfer of trust among various components and agencies as you drill down from the department level.

Let's see here. NISPOM rule update, I think we've already heard a little bit from DoD on that. We heard about FAR update on the use of NCCS. We heard about ISLs on SEAD 3. I'm just running through some of the things we discussed at the working group. Valerie touch on the SEADs, SEAD 8, SEAD 2. The CVCE process, Heather Green will expand a little bit on that and CE alerts and how they're processed and when actionable and valid and things of that nature.

Let's see. Insider threat, we've talked about that. We do expect to reengage in the next 30 to 45 days with a working group meeting there. CUI, we heard from that. NIDs, we did touch already on that in this meeting and at the workgroup meeting. I believe with that, those were the main points that we had discussions on, of course reviewing the data for access eligibility determinations which Heather will further discuss, Heather Green. With that, are there any questions that anyone has for me on the clearance working group? Okay, I guess not.

Mark: Okay. Thank you, Greg, for giving that. Now, we'll hear from Heather Green who's been given quite a warmup here. Heather is speaking about personal vetting metrics. Heather, please.

Heather G.: Yes, absolutely. Good morning. Thank you. DCSA has a good new story in regards to our progress made with our interim determinations, our investigations and our adjudications inventory and timeliness. There are two slides on the website for your reference that I'll be referring to during my segment here.

Looking at the inventory metrics. During quarter three, investigations inventories reached a stable state of under 200,000. This occurred in the mid-April timeframe and was two years after the inventory pay cut 725,000 in 2018. A lot of progress and a lot of hard work there. The inventory remained under 200,000 for the entire quarter. However, as of July 6th, it does stand at approximately 205,000 of which 34,900 are industry cases. The inventory has slightly increased over the past few weeks, mostly due to the COVID related impacts. We have seen a steady state of submissions for industry, but we do have an increase of cases on hold due to inability to collect some of the records for the investigations to close.

We do ask for your help in industry by responding to the employment verification request and any inquiries you get from the investigators. The adjudication inventory has also continued to decrease and is working off of a steady state inventory. Currently, there's approximately 17,200 industry cases that are pending adjudication. So again, a lot of progress with that inventory reduction in all areas.

Looking at the timeliness metrics, the significant decrease in inventory has greatly aided the reduction in timelines. As shown in the chart, the investigation and adjudication timelines has consistently decreased over the past year. The data shown reflects that the case was adjudicated during quarter three. However, based on investigations DCSA completed and provided to adjudication facility in T3, the fact is 90% of the T5 investigations were actually completed in 79 days, meeting the 80-day goal for the first time since 2014. Again, a lot of good progress.

With respect to T3, the fastest 90% were completed in 55 days during quarter three, which is 15 days over the 40-day goal. However, under today's standards **[01:33:00 inaudible]** which wasn't in place in the 40-day goal was established. But again, progress in both T5 and T3 timeliness reduction. All very good news. We certainly are heading in the right direction. Our goal is to thoroughly vet individuals in a timely manner and provide that direct support submission readiness.

The next slide provides some additional metrics from the VROC portfolio. We have processed over 130,000 investigation requests. That's an industry investigation request for fiscal year. We are currently processing interim determinations within approximately five days of receipt. We have a growing population enrolled in the DoD CE program. As we are up to over 2.2 million enrolled in the DoD CE program. Of which, approximately 455,000 are industry subjects. As of July 7th, as Mr. Pannoni referred to, we have deferred 87,803 industry PRs into the DoD CE program, and those industry PRs are enrolled in a fully compliant CE data sources to support that reciprocity.

We currently see an average of about 6% alert rate, which a majority of those alerts coming from our criminal and financial data sources. As Mr. Pannoni mentioned, one item that's done when we receive an alert, obviously checking, doing identity **[01:34:28 inaudible]** looking to see if it's previously known. Those that are previously known, that's a success. Those that are not previously known, we'll begin the action for the appropriate follow-up mitigation efforts.

There are CE industry FAQs available on the DCSA website and we do update those regularly. It also includes the clearances do not expire memo, so I highly recommend if you have any questions, please do refer to the DCSA website as we are continuing to provide updates on these FAQs. Additionally, regarding reciprocity processing, just want to make a note that the CAF and VROC are collaborating regularly to streamline the process. We've been working very hard over the last eight months or so.

We have specialized teams working all reciprocity requests. Timelines to grant reciprocity request have decreased. We have seen a decrease in our system. Although COVID-19 has presented some challenges due to the need to access the classified systems, reciprocity requests are still being completed with the dedicated resources, accessing those systems, and making that a priority. That's all I have sir. Thank you for your time and allowing me to provide DCSA personnel vetting updates.

Mark: You're most welcome. Any questions for Heather before we move on? Okay, hearing none. Thank you again, Heather. Now we'll turn to performance metrics, Perry Russell-Hunter from the Defense Office of Hearings and Appeals, also known as DOHA. Perry, yours.

Perry: Thank you. I will make this very brief. One of the advantages of us all doing this remotely is we appear to be able to do things faster and that is also true of the review of statements of reasons and the issuance of statement of reasons. This is a real success story of collaboration between DOHA and the DoD CAF. Thanks to the CAF's leadership and hard work by folks at DOHA like Jim Norman and Julie Mendez. We have a record-breaking number of legal reviews conducted and statements of reasons issued. We're using a technology called DoD SAFE which allows us to send the SOR PII protected and with the acknowledgement. That’s working well.

There've been a number of innovations that allowed us to keep the industrial due process workflow continuing. In fact, in the month of April, we broke a record of 475 statements of reasons legal reviewed. With the fact that the CAF and DOHA have been able to work together while doing a 100% telework is really a testament to everybody's efforts and the ability to adapt and transform to unusual circumstances.

The challenge has really been in resuming hearings, which we are now doing. If you look at the DOHA website, you will see that we have a COVID-19 safety protocol message up there. It does not specify what the safety protocols are because those will change over time. But instead, and the exact safety protocols are going to be provided to the parties at the time that a notice of hearing is issued. But what we are able to do is ensure that we are keeping people safe while beginning to hold hearings again while also keeping all of the other non-hearing work going at a as good or better pace than before. With that said, I will take any questions or just give you all back some time. Over.

Mark: Any questions for Perry? Thank you, Perry. You're a man of your word. We're now going to turn to another presentation. This will be on GSA containers by Roy Jusino. Roy? Roy, are you there?

Roy: Yes, I'm here. Sorry about that.

Mark: It's okay. Loud and clear.

Roy: Okay. Good. My presentation is going to be relatively short. It's not going to be that long. My name is Roy Jusino. I'm representing GSA today. I Chair the SEAL committee for GSA. It's an interagency committee that oversees the GSA security equipment product line, and I was requested to give a quick brief on the ordering process of GSA approved containers by US government contracting workforce, which I understand has become somewhat of a topic of concern.

Official regulation for purchasing GSA approved containers is found in the Code of Federal Regulations 32 CFR. This regulation requires new containers meet the required GSA standards and whenever possible, be available through the federal supply system. In 2014, GSA changed the procurement system for the security containers to address concerns raised by the interagency committee. Specifically, to better control who could purchase the containers and to increase the funding to create a more robust testing program for the GSA security equipment product line.

ISOO issued a procurement clarification in ISOO Notice 2014-02 and this notice requires that all containers be purchased through the GSA global supply system. When we first started that process, we realized that in the early stages of the effort that there would be some issues with US government contractors purchasing through GSA global supply system. We established an exemption process that would allow the US government contractors to contact GSA and GSA will review their request, determine if they represented a legitimate need for the containers to protect classified information and approve the exemption that would allow the requester to purchase directly from a GSA approved manufacturer.

The exemption process was a temporary solution to basically fill a gap while … I'm sorry. The exemption process was a temporary solution to fill the gap while contracting officers and US government contractors made the necessary arrangements to order through GSA global supply system. The exemption process went on for about five years and we actually discontinued the exemption process in September of last year. Through the exemption process, we found that a number of purchases were being purchased through third party businesses. Sometimes a number of third-party businesses which basically added to the supply chain costly issues and potential risks for accountability of containers and locking systems on those containers and also added significant cost to the end users.

The primary reason for us to increase the security of the supply chain, government agency ask that we include limited use requirements which basically limits the procurement on GSA approved security containers and locking systems to US government and US government contractors only, for the equipment. The interagency committee established this process and it wasn't made in a vacuum. We understood that there were significant problems with the control of our security equipment, and this was one of our big efforts to reel that in.

The second reason we did this was also to… GSA was losing funding with the exemption process. Every time you purchase to GSA, they give a small percentage of that sale and that percentage is used to actually fund the testing and approval process of the equipment and the quality assurance to ensure that manufacturers are staying up to the federal specifications of that equipment. That is solely funded through the sales and that is it. GSA was absolutely losing millions of dollars a year with the third-party sales outside the global supply system.

My presentation went through step by step ordering procedures but that's really not going to work today so what I want to do is I want to make sure that everybody has the website information because there is an eight-page document on GSA that actually goes through the step by step process and all the different ordering procedures established in AACs, established in DoDAACs, how to pay GSA through pay.gov with the vendor customer self-service portal.

If everybody's ready, please write this down. This is the GSA website where you can find the ordering information. It is www.gsa.gov/securitycontainers. I'll repeat that again, www.gsa.gov/securitycontainers. In the left side bar, you'll see ordering procedures. Then when you click on ordering procedures, there'll be several PDFs. The one PDF that you want is the non-government ordering process. You'll pull that document up. It's an eight-page document that goes through all the various ordering processes through GSA. There's also a 1-800 number, the GSA helpdesk if you need help ordering the containers or locking systems through GSA. That number is 1-800-488-3111. Again, that's 1-800-488-3111. That's really all I have. Thank you very much for your time.

Mark: Thank you, Roy. Does anybody have any questions for Roy? Hearing none. I want to note just for the record, the statistics for the Department of Energy and the NRC, Nuclear Regulatory Commission, background investigation located at the NISPPAC reports on committee activities page. We're now at the point of the meeting where we ask the NISPPAC members to present new business. Is there any new business to present? I take that that is a no. Greg, am I missing anything there?

Greg: Sorry Mark. I didn’t unmute the phone. No. We have the open forum where I believe you want to ask the other CSAs?

Mark: Yes, I do. I'll do that now. Since we have no new business, we're going to move into the general open forum and discussion time. As a suggestion, I thought I would like for the CSAs to tell us about their COVID-19 operating status and how they’ve managed the NISP program during the pandemic. We've already heard from DoD and ODNI. Does the DHS have anything they'd like to tell us about their operating during this very unusual time?

Mike: No, sir. We don’t have anything to report this time. We've been teaming and following with the DCSA's input and ODNI's input on things such as getting fingerprints and getting package submissions, so we don’t have anything else significant to report.

Mark: Okay, good. Glad to hear that. How about the NRC?

Dennis B.: Dennis Brady, NRC. We've been utilizing all the authorities that’s been granted to federal agencies to develop processes to continue operating. Without those, we would not have been able to continue the program. Thankful for that, we're up and running. No new news on the program at this point.

Mark: Okay, good. How about the Department of Energy?

Tracy: Good morning. This is Tracy Kindle. I'll provide a couple of points.

Mark: Sure.

Tracy: Thank you for the opportunity for providing the update on the Department of Energy has and is doing as a result of the COVID-19 pandemic. Early on, the Secretary had authorized maximum telework flexibility for employees to accommodate state and local responses to the COVID-19 operations. DOE established a COVID-19 response team hotline for reporting potential or confirmed COVID-19 cases across the complex. The Secretary also issued guidance temporarily suspending some security and state prior requirements across the department to help minimize exposure to COVID-19 for federal employees and industry partners.

From a per sec perspective, we adjusted some of our reporting timelines. We also adjusted some of our due process action timelines, just to name a couple. The Department of Energy is taking advantage of some of the exceptions offered by the Office of Personnel Management and the Defense Counterintelligence and Security Agency regarding background investigations to help ensure our industry partners' clearances are not delayed because of COVID-19.

Finally, the Department of Energy continues to stand ready now and anytime in the future to assist our industry partners however we can in support of the nation. Thank you again for the opportunity to present the Department of Energy's update on COVID-19.

Mark: Thank you for doing it in such a way. Do any other committee members have any questions or remarks before we close out this meeting this morning? Alright, hearing none. We normally provide the date for the next meeting but due to the uncertainties caused by the pandemic, there's simply too many unknowns at this time. We're trying to shoot for some time most likely in mid-November. But again, that’s all subject to what's coming down the pipe. All NISPPAC meeting announcements are posted in the federal registry approximately 30 days before the meetings take place, so anyway, there'll be ample warning for the next one.

Thank you all for your time and patience while we operate in this new environment. I'll have my staff provide the NISPPAC members with the date of the next meeting. Again, just what I just said. Over with that and without any further comment, thank you again for your patience and your forbearance as we… this is our first virtual one and I'm pleased with the way that it went and that’s all due to you all and your very good presentations keeping this meeting moving. Thank you. With that I'm going…

Greg: Hey, Mark?

Mark: Yes, go ahead.

Greg: Could I just remind because we didn’t, this time, forward the opportunity for the non-member participants. Just want to remind them if you do have questions, as Mr. Bradley said at the beginning of the meeting, take advantage of the NISPPAC NARA mailbox and send us your questions. We will respond.

Mark: Indeed, we will. Alright, thanks for that, Greg. Okay. Without further ado, this meeting is now adjourned. Stay safe.

Greg: Thank you.

Will: That concludes our conference. Thank you for using Events Services. You may now disconnect.