[START OF TRANSCRIPT]

Mark: I'd like to welcome you all to the 63rd meeting of the NISPPAC. This is a public meeting. It's audio recorded. We're also using a WebEx and we also have people on the phone. We have different microphones in here. What's going to happen is we're going to have, most of our presenters will be up here at this podium here. We have two microphones here for the front rows, the first two where the NISPPAC members sit and then the other microphones on each end. When you come up to ask a question, again, the questions will be, there'll be a short question period after each speaker and there'll be a longer one at the end of the meeting. And we'll open it up for our, what I'd like to call the free for all, but if you would come to the mic, please identify yourself.

These meetings are recorded, and they are also turned into minutes and it makes it a lot easier for us when we do the minutes to actually be able to put the proper speaker with the question. Otherwise, we're sitting there trying to figure it out whose voice was that. I think that was X, no it was actually Y. Anyway, just in terms of clarity, it would be most helpful, again, please identify yourselves. Some other administrative notes. We'll have a 10-minute break during the middle of the meeting. Restrooms are out the door here to your left, as is a small cafe. For those of you with mobility issues, to my right in front of the stage, there's a door that leads to the elevator and that will transport you to the **main level.** Regrettably archive rules are no food or beverages are allowed in here as you can see from my deputy here. Yeah, exactly. Alright. We're going to do the introductions like we always do. We'll start with the table here and then we'll go to the first two rows of the auditorium where the NISPPAC members sit and also, we have some of our distinguished guests this morning. So again, I'm Mark Bradley. I am the director of ISOO and the chair of the NISPPAC.

Jeff: I'm Jeff Spinnanger. I represent defense.

Heather Sims: Heather Sims, industry spokesperson.

Tracy: Tracy Kindle, sitting in for Marc Brooks, department of energy.

Greg: Greg Pannoni, ISOO.

Valerie: Valerie Kerben, NCSC, ODNI.

Male Speaker: **[0:02:16 inaudible].**

Charlie: Charlie Phalen, DCSA

Gary: Gary Reed, OUSDI.

Bill: Bill Lietzau, personal vetting transformation office.

Kim: Kim Baugher, state department.

Sharon: Sharon Dodlinger, Airforce.

Bob: Bob Harney, NISPPAC.

Rosie: Rosie Borrero, NISPPAC.

Steve: Steve Pete, NASA.

Aprille: Aprille Abbott, industry NISPPAC.

Shirley: Shirley Brown, NSA.

Cheryl: Cheryl Stone, NISPPAC.

Dan: Dan McGarvey**,** NISPPAC, industry.

Carl: Carl Hellman, DCSA.

Keith: Keith Minard, DCSA.

Terry: Terry Carpenter, DCSA.

Dr. Charles: Charles Barber, DCSA.

Ned: Ned Fish, DCSA.

Mark: Thank you very, very much. Okay. Just some quick administrative things, this time I'd like to welcome Ms. Heather Sims from general dynamics. She will be our new industry spokesperson. She's replacing Quinton Wilkes who did an outstanding job and again really raised some interesting issues for us. We know though that Heather would do a superb job as well. So anyway, Heather, welcome. I'd also like to welcome another industry member, Ms. Aprille Abbott from the Mitre Corporation. She's been attending the NISPPAC meetings as well as from working group meetings for many years. We're happy to have her as the industry NISPPAC member officially. We have several changes for the government membership as well. We'd like to welcome Mr. Keith here as a new representative from DCSA and Mr. Carl Hellman beside him who will be working or be serving as the alternate for DSCA. Both of them have been involved with the NISPPAC and the working group for years and we're excited to have them here. So, thanks guys. In addition, Mr. Brad Weatherby will be the new NISPPAC representative for the NSA but he's not attending today, we'd like to welcome him as a new

member. Ms. Shirley Brown has been serving very ably as his alternate or as the NSA alternate. Interestingly enough, there is no current member from the CIA on the NISPPAC. We hope that will be solved soon.

Last week, Ms. Zudayyah Taylor Dunn is no longer serving as a representative from NASA. She's been great, and will be missed. At this time a new representative has not been officially appointed from NASA. However, Steve Peyton is continuing to serve as NASA's NISPPAC. One interesting point I'd like to make here, as a chairman, its part of my job just to solicit and accept nominations from the agency head. Interestingly enough, no member can nominate him or herself. I shouldn't be surprised, but we do get that from time to time. I like self-confidence, but nevertheless we do have a procedure we have to go through. Anyway, the bylaws stipulate that the nomination should come from the agency head. We are in the process of modifying those bylaws, which will allow not only the agency head to do it, but also the agency does need a senior official. And again, I have full confidence in the senior officials being able to do it as well. We intend to have that new language out in the next two weeks, again, with the holidays being what they are. Don't be surprised when you see that. Again, the idea is to speed up this process a bit and that's what we're...

Secondly, we do have a requirement when you do sit on the NISPPAC, you'd have to file an annual financial disclosure form with the national archives officer general counsel. It was great to point out, this is only for the government members only because we're the ones who have to file these ethics statements. They're not new forms. You can file the ones you filed with your agency with us. We're not requiring you to go out and redo what you've already done. Not that onus of a burden, frankly, it's just a matter of copying it and sending it to our general counsel. That said, you can't sit in this thing unless you do that. So... Right, I think I've beaten you enough with that. I'm going to turn it over to Greg to deal with business of the last meeting...

Greg: Okay. Thank you. Good morning everyone. Just a couple of admin announcements that we always go through. The presentations and handouts for the meeting were sent electronically to all the members and to those who provide an RSVP to the invitation. For those attendees who did not receive these documents, all of the materials will be included with final minutes as well as the official transcript of this meeting. And we'll put that on our ISOO NISPPAC website within, try to do it in 30 days. Also, all NISPPAC meeting announcements are posted in the federal register approximately 30 days prior to the meeting. And if you're ever wondering why I'm doing this, it's one of the FACA, federal advisory committee act requirements are that we have to, a lot of these protocols we have to follow based on that.

Now I'm going to turn to the action items from our last meeting. The status of those, there were total of nine. One was a carry-over from the last two meetings. That one concerned access to the Defense Information System for Security or DISS. I'm going to say all the acronyms for those that don't know them, at least once. Full name and then the acronym. Access to DISS by non-DOD agencies was the item and the status on that, the defense vetting directorate or DVD senior advisor consulted with the department of state to better understand State's need in terms of management of cleared industry under the security cognizance of DOD. As a result of this discussion, it was agreed that the best tool to support these needs would reside in the national background investigations system, NBIS, Low Side Repository, and LSR. The LSR will replace existing repositories being the central verification system or as we know it CVS and DISS and will be enhanced to support the exchange of critical personnel vetting information. So that's the important part. Dr. Charles Barber, who's here today, the DCSA director of enterprise business support office, EBSO is in the process of establishing a working group to help resolve these issues. This one is still open. Next item, and if you have questions, we'll do that at the end.

Next action item; industry to provide instances of delayed national interest determinations or NIDs, processing by the cognizant security agency, cognizant security office, CSA, CSO. Industry did provide instances of delayed needs and NID working group meeting was held in August while ample discussion occurred at the meeting and progress was made, another meeting will be scheduled in the near future with the primary objective to maximize the efficiency of NID processing. Next item, so that's still open. DCSA is still in process of internal and formal coordination of an industrial security letter; ISL, that will replace the current ISL 201602. Subject of that ISL is insider threat program.

The update on that is as follows. NISPPAC comments have been received and DCSA is in the process of reviewing them. DCSA in coordination with OUSDI staff will work with NISPPAC on comment adjudication and as a follow-on work with the industry on updates to related insider threat products and tools that effect a cleared industry. Next item. ISOO will convene a NISPPAC NID working group meeting in the near future with industry reps. DCSA was going to address the challenges in the NID process. As I noted, we did convene that working group on August 22nd to discuss this issue and other meeting is planned. Some of the ongoing challenges include consistency and reciprocal acceptance of foci analysis among the government parties involved in the NID process, so the controlled agencies controlling agencies, a common understanding of timelines and a responsible entity for updates on NID Case studies.

Next item. Ms. Patricia Stokes, DCSA mentioned there was going to be a stakeholder's forum on July 29th and 30th. The EBSO, enterprise business support office recently met with industry to address systems requirements and industry issues that support vetting and NBIS development activities. Additionally, the DCSA is planning an NBIS stakeholder symposium in the spring of 2020. An entire day of that symposium will be dedicated to support industry business and or personnel vetting needs. Next item, Mr. Chris Forest, DCSA stated there will be a meeting in August for industry and government to discuss ongoing issues with the national industrial security system or NISS. Due to personnel turnover and security mandated system upgrades to NISS, the NISS operational requirements committee, ORC meeting scheduled for August was not held. It was rescheduled and held this week on Monday. The objective of the ORC is to handle new system capabilities and as a reminder, please use the DCSA knowledge center for NISS issues.

Next slide. ODNI to host a meeting in the fall to discuss the state of the trusted workforce initiative to address the concerns of industry. Ms. Valerie Kerben to my left, ODNI, will address this issue later in the meeting. Next item. ISOO, they ask DOD to take the issue of cyber assurance back to confirm what level of confidentiality, integrity, and availability for the national contractor classification system NCCS is or is planned to be. The update on that, the defense logistics agency manages the systems accreditation for the procurement integrated enterprise environment, PIEE, on which NCCS resides as a module. The system accreditation includes the appropriate level of assurances for confidentiality, integrity, and availability for the 254 information and personally identifiable information PII, which resides on the system. So that's good. Last item, DOD will provide an update on critical technology protection. This will be discussed in the next few minutes during the DOD update, which is next on the agenda. Are there any questions?

Female Speaker: That works, yeah. Just a quick question on the DISS versus... there's too many acronyms anymore, but, so you said, so we're not going to get DISS access. They've decided we'll get low side repository on the NBIS which is going to replace CVS at some point. Is that what you're saying?

Greg: Yup. Let me go back to that. That's my understanding. Best tool to support these needs would reside on the NBIS Low Side Repository and the LSR, Low Side Repository will be replacing existing repositories, CVS and DISS and it will be enhanced to support the exchange of critical personnel vetting information. That's what I'm told. We have Dr. Barber here who if you wanted to say something about it, Oh, I'm sorry, over there. By all means, if you'd like to add to that, now's a good time. Thanks.

Dr Charles: Good morning. While we do realize there are capabilities being developed in NBIS, we do also recognize from operational perspective the needs that department of state needs. We are working to try to get interim access to this until those capabilities are developed into NBIS. So, we are in discussions with Kim at the state department and we are all working at in the interim.

Greg: Thank you. Any further question?

Female Speaker: When will this new CVS or when will that be done?

Dr Charles: The last update I had was we were targeted for late January. But again, we want to try to get you interim access into DISS why those things are being developed.

Greg: WebEx?

Carolina: Actually, we just heard that Dennis Arriaga is on the line.

Mark: First Report will be from Gary Reed, director of defense intelligence, counterintelligence, law enforcement and security, office of the undersecretary of defense.

Gary: I brought my time, 20 minutes.

Mark: Good man.

Gary: Okay. Thanks Mark and Greg and NISPPAC members for inviting us over today to give you an update. I'm going to focus my remarks on this incredibly large and complicated topic we are calling critical technology protection. It means a lot of things to a lot of people. I want to tell you what it means to us in USDI and with the secretary of defense and undersecretary Kernan and those of us within the department that are working from our end. And we very much appreciate everything about the collaborative effort we have with our NISS partners. I've been calling on you at the end to help even more. What's mentioned in the intros seated next to me in the front row, Bill Lietzau who came on board mid-year to rescue the transfer operation to transfer NBIB over to DCSA.

He's the head of our personnel vetting transformation office. Nicolete, are you here? Nicolete Giordani is his deputy. She may be coming over later. They're sitting in on this today. It's a good time for an update on this topic. Good time for a bit of a reset. Since then, in the last six months we've got a lot of change. We have a new secretary of defense, a new acting DNI, a new PDDNI, a new OPM director. We renamed DSS, Dan Payne departed, Charlie is on board. I only point this out and we'll talk about some of those things

because I'm very comfortable that despite all of that, the day to day steady as she goes, driving towards progress, first of all, the strategic priorities have not changed for us with Secretary Esper over where they were with secretary Mattis or acting secretary Shanahan. Obviously, my boss has been the same throughout, but all of us that work this every day, myself included, Charlie Fallon and included and others, Bill **Levanin**... team here.

We've been fortunate to have a lot of stability in that area. Had it been different and frankly thanks to Charlie for his stabilizing influence to stay on board to run DCSA. That was huge. I say that as a bit of a calming the waters here. It's not total chaos. It might look like it sometimes. And again, Bill Lietzau's operation coming into full bloom here just at the right time couldn't have helped more. It looks bad, could be worse. I think we're in pretty good shape. Me personally, I'm not by background a CI or a security person. I spent the first 40 years of my career avoiding those kinds of people. I'm kind of like the opposite of Bill Levanin. I think maybe that people always make me a little nervous as cops and everything, but I sure respect them.

My army background, I was kind of trained to lie, cheat and steal for a living. We call that unconventional warfare or counterinsurgency where I come from, but I think it serves me well. And when we look at what's happening, and I never want to talk about what we're doing process-wise without taking a minute on the threat. If you look at where we are, whatever you want to call it, I don't want to call it something dramatic in a public setting about whether it's some form of warfare or whatever it is, but we're leaking out technology to people that are actively seeking it in a very systematic way. Again, where I come from, we call this going after soft targets and executing a death by a thousand cuts and its right out of any insurgent playbook you could ever look at.

That's the environment we're in, and to some degree in the commercial economic technology space with some very sophisticated adversaries. It is a systematic, calculated effort. It's multiplane, multi-vector looking at our vulnerabilities and our commercial, economic, trade, export controls, academic research, laboratories, how we control information. All of that is basically a feeding frenzy for those, that would seek to exploit seems to exploit our research development and acquisition process and really systematically target our people, our programs, our facilities, and our information. And within all of that is really where we land on our efforts to upgrade on our quick tech protect. I will again remind you that for the secretary, elevating security across the board has been the policy for the last two years plus. Undersecretary Kernan brings this into his job as the USDI. He is the undersecretary for intelligence and security among other duties, but equally important to him, he's a big believer in innovation and digital

monetization, which is good for us as we talk about how we want to strengthen our protections.

He's a big partner and ally guy, a big Five Eye integrator as his acting McGuire. I think it's probably a function of their military backgrounds, but it's also a recognition of the global environment and the global mission space we're in. And the recognition that our Five Eye partners are in this just as deep as we are in terms of maintaining our technological edge. We're obviously, I'm not going to talk about personnel vetting today. Everyone knows what's going on. Charlie's going to touch on some of the ASIS stuff, but we're very focused on this shift to continuous vetting. And obviously the continuous vetting transformation and tech protect my boss describes to me as the two no-fail missions for him. They're both under my oversight and they track them pretty closely.

What are we really talking about when we say we're protecting technology? What are we doing different? What do we owe you as an update? I'm going to talk about five pretty big things, all of which have been put in motion. I'm going to go back to August 2018. So just over a year, what's that? 15 months ago, we came out with a report that we partner with MITRE called deliver uncompromised. And this was really the brainchild of Bill Stevens and some folks at DSS working with Chris Neeson in the Mitre team to look at this topic of protecting our technology. The DEU report, its available online if you haven't seen it. I think it's still pretty good. There's a lot of big ideas in there, a lot of lines of our operation, some of which we've touched on, some which we haven't gotten to yet.

They run the range of things from legal and financial controls down to program protection, but they really identified four major vulnerabilities that the adversaries were harvesting. Supply chain, whether that's hardware services or software in the supply chain, the cyber physical, the weapon systems, industrial control systems, cyber IT, the big topic obviously we to talk about every day now about cybersecurity and human domain. Following shortly after the publishing of the DEU report, the secretary established in November of last year, just a year ago now, and the protecting critical technology task force.

Again, their mandate, general Murphy's mandate is to protect the DIB, span the spectrum of RDA. And how are we doing that? There's a lot of things. I can't go into the details of everything taskforce is doing, but I will just highlight for this group things like the new partnership that Dan Payne and Carrie Weaven crafted with Emma Lewis at DCMA. To start to connect between when we draw a big circle chart and here's the NISS and here's 10,000 and here's 300,000 in the DIB and what is in that space between, and we know where the adversaries are, where the soft targets, more so than

they are where you're obviously doubling down on your protection every day.

Increasing those partnerships, changes in contracts that A&S put out and it's still putting out to strengthen contract requirements for security. That all has been put in motion by the task force. Improving on cybersecurity, if everybody here has probably by now met or heard of a very energetic officer named Katie Arrington over in A&S, the chief information security officer for A&S. She's a champion of a program called the Cyber CMMC cyber maturities... Help me out Steve. Thank you, CMMC, well-funded now, going forward over the next year plus and many of you have worked with Katie on the minimum cybersecurity standards that they're establishing for all elements within the DIB.

Integrating security into acquisition, another focus area for the task force. This runs everything from the initial memos that came out of Navy, the so-called Hondo memo about strengthening program security for Navy programs to the ongoing work in the 5,000 series to see how far we can get. I'll tell you from our side going, we want to get as far as we can in the policy language to make security a relevant factor. If you read the deliver uncompromised report, it has the wonderful bumper sticker of security as the fourth pillar of acquisition, right up there with cost, schedule and performance. Candidly, the leadership probably never really saw it exactly like that. But on principle, I can assure you between A&S leadership and USDI leadership, there's no daylight in the necessity to make security a factor in how we operate going forward. And it's our job now to get that into policy. Jeff Spinnanger is sitting here for me and as the pin for our contributions to that and we're obviously working very closely with A&S on that.

Well, also I'll just throw in this idea, we have a thing in DOD called Intel support acquisition and it's largely Intel mission data to support our understanding of adversary capabilities. It's taking on a new meaning however, and how we use our intelligence resources to understand where the adversary is targeting and ripping us off. Every time we have a success where we say we blocked something or we prevented this from happening, typically the secretary will say, "That's great this time, but how do we just quit reacting?" Right? How do we analyze their strategy? How do we know where they're going next? And this becomes this collection requirement that we're now introducing into the IC where it's never really existed before, where we use intelligence to understand particularly how the adversary is moving around our supply chain. It happens, but it doesn't happen deliberately. So that's becoming a new thing as well.

Another mandate for the taskforce was improve security in the research domain. You see this happening. We wrote an assessment last year and provided it to the personnel in readiness and an effective a change in policy over grant funding at universities where there's a Confucius Institute and that got shut down without frankly a whole lot of fanfare. We thought there'd be more blow back on the other side of the equation. But there was just one example where we were funding language training in the same universities where the Chinese were funding language training and we said, we probably don't want to do that, too proximate. We have other ledge proposals in cycle for next year that will continue to strengthen this area and working towards a better way, whether it's done government or done by universities, have some better understanding of who is conducting this research. If you want to call that vetting or you just want to call it some sort of due diligence somewhere in between details to be figured out. But that is happening as well in that space. Thanks to the task force.

Working with interagency was the fourth line of activity defined for the task force. We won't go into a lot of details. We have some special task forces. We're working directly with commerce and justice department to bring tighter connectivity between defense centrists and those of our export control community commercial sector in our justice department. And then the last domain for the task force I really can't talk about which is what are the actions more sort of to counter the activities of the adversary in this space that could be done from a defense capability side. Those are on the plate for general Murphy. They've done a great job at the one-year point. It was a two-year starting point for them. We're planning to continue that this year.

The third initiative is the critical technology program list. People have heard of this. We put it out in March. It took a while to get it out. It was actually finalized in December. It took us another for months to the step it up. The good news is we did finally consolidate the views of the joint staff, the services, the USDI, the USD R&E and the USD A&S in a place where we did not have one single rationalized prioritized list. We had multiple versions, we had a joint staff version, we had an R&E version, we had other versions. So, this effort in March really solidified that we have one list.

The intent of this list as signed up by deputy secretary Norquist was to focus our protection measures in our security resources in this space. We looked at this to establish these domains. We looked at technologies through three lenses, through a foundational lens, say biotechnology as a foundational technology and enabling lens, say AI as an enabler to something else. And in terms of mission technologies and in thinking in terms of weapons, directed energy as an example. Using those three lens, services and components went out. We came up with 147 critical programs across the Mil depths and

agencies, seven tier one technologies. Why are they tier one? They're largely almost specifically called out in the national security strategy or national defense strategy as essential to our technology superiority. And 11 tier two technologies, which either support or enable those or are important to one or more components, but weren't maybe not called out in the NDS.

So that's the framework. The guts of that list are largely FOUO. The overall document is secret. We are working right now with a lot of people in the building to have an actual releasable version so you can have the same thing that we have. But clearly if you're within your space the updates are absolutely available to you, it's not the secret versions depending on where you are. Number four, we established DCSA, and I'll talk a little bit about DCSA. We renamed DSS by memo, one memo signed by the secretary, renamed DSS. The real work is taking DSS of old, NBIB as existed on September 30th, merging them into a single integrated organization with two very distinctive missions, with two very distinctive sets of authorities and documents and bringing some synergy and commonality where it makes sense but also respecting the importance of each of those missions. That is what we are calling DCSA transition.

Bill Lietzau sitting here in the front row is authoring, working with Charlie and Christie, a transition plan, objective and milestones, a plan for transition. It will have about a two year lifespan, give or take, no more than that, maybe less to really normalize day to day life in DCSA, but also maximize on efficiencies and economies and blend in other things such as what Kerry is already doing with NBIS and to that half of the equation and blend in things that are already underway such as CUI and authorized disclosure responsibilities that DSS was assigned previously. It's not just a name change, it's a major undertaking for both the vetting mission changes and changes to contemplate going forward in the tech to protect in the NISS space. We are posturing DCSA to become what we're referring to. The buzzword is the nation's gatekeeper. So national is a DOD agency. By the way I apologize the DCSA sounds like DSCA. National security agency was definitely taken. Kerry Weaven and I actually floated an idea that it was a federal agency and everybody that has federal in the name of their agency, not naming names, thought that was a hugely offensive.

It is the defense CI and security agency. Not going to be CIFA, they're not going to be running CI investigations. The CI part recognizes the CI mission they have, but it also recognizes the integration of CI in security, which is something that's been underway in the government for quite a while, NCSC being the example, somewhat analogous to NCSC but at the DOD level. But you have to realize it is a government wide agency, 105 vetting customers, 33 NISS partners. It is a government wide agency with some unique DOD responsibilities as well. And we will situate those down there, whether it is

on our security side, not, we got per sec, they got industrial sec. They're all over that. But where are we going with physical security for example? I have an office in USDI that does phys-sec. We don't really, we shouldn't manage missions. I need a mission manager and mission owner to operationalize security. That's where DCSA is going. I guess, I lost track of my little scorecard here. Okay. Wrapping up, I've covered that.

The last one, number five. In September we kicked off for this year the research agenda for our university affiliated research center located at university of Maryland. It is the applied research lab for intelligence and security. It was formerly the center for advanced study of languages. It was an NSA activity. We took over sponsorship two years ago. We've been working in that time to retool. This is now what I described ARLIS, ARLIS. They're actually having a stakeholder event up there this week. We have a big thing tomorrow. We're underway with our research programs. Why does it matter, and some of you are already involved, but the research focus is again, social systems, human behavior, conflict security, augmentation, human system integration, AI, autonomy, information dominance, experimental technology? That's the research agenda for this and it's the only UR that exists to do that kind of research and we're very excited about some of the long-term implications of that research.

Looking ahead, so that was everything we've been doing. We're going to keep doing it. We're going to continue to press on what we can squeeze out of the DEU report as a vector for activity. We're going to work with A&S and R&E on elevating the importance of security across the board and acquisition. We're going to stay focused on CI, on CUI cybersecurity. Really again, if I could describe it one way, we're very comfortable with what you do in the NISP. We've got a lot of wide-open space in the rest of the DIB. How do we do best practices within all the authorities that are available to protect the technologies? That's the focus.

It's a busy time. We appreciate all the great work. Again, I couldn't compliment Charlie and Bill any more on the transfer. It was almost painless, believe it or not. The worst thing that happened was somebody got two paychecks out of 3000 people. Nobody got no paycheck. That was a big concern, but a great work. We appreciate your support. We appreciate that change is hard. If it's not making you uncomfortable, we're probably not pushing hard enough. Frankly, it should be a little uncomfortable, but we don't want to break anything.

We don't want to break the mission. We all want to operate with our head in the sand. So, we need your help. We can't compromise on getting things done every day. We got to all keep our eye on the next original line and where we're trying to go to be better than we have been in the past. Not

because we weren't doing a good job, because the dynamics has changed. The adversary is on the move and we're playing a little catch up, but we want to get out in front and sustain. So, thank you very much. And I'll turn over to Charlie.

Mark: Hey Gary, hold on a sec. Gary?

Gary: Yes sir. That's what I was looking at.

Mark: Does anybody have any questions for Gary?

Male Speaker: Nope.

Mark: That's why I love having this guy come. Yeah. Anybody on the phone or the WebEx, Carolina? Okay. Gary, you are excused. Thank you so much. Charlie, you're up. Charlie Fallon, acting director for DSCA will provide an update. Charlie, please.

Charlie: Okay. Thank you all. I hope you can hear my voice here. I had a historic family event over the weekend with my daughter getting married and my voice is still trying to recover from a raucous kind of a weekend. But I'm happy to be here with you all this morning. And first a couple of... I think, so I saw Quinton in the audience. There he is right there. Thank you for your time as a spokesperson and your support for all that we've been doing and whatever job I've been in for the last eight years, I think. And Heather, welcome aboard and you bring some unique insights into this. I mean you worked both sides of the house in both government and industry. I'm going to give you time for questions at the end here and look forward to the feedback you guys have. I am going to have to escape at the break. I want you to have a lot of time to hang around and take questions at that point. So please take advantage of the time. I'm going to leave at the end here for this thing. Gary has given you a good strategic view of what's happening within this organization. I'm going to really focus sort of on the really DCSA operations. There some things that are happening there. Starting with the hunt for 1, October, it's over. Transition, I think it is noteworthy that we moved several thousand people over that transom. Actually, when we woke up on 1, October, that transition had happened three days earlier over midnight on the 28th of September. As Gary pointed out, nobody missed a paycheck.

And then in full disclosure, the one person who got two paychecks is standing here at the podium just because of there's some confusion within the office of personnel management and my status there as opposed to anybody else in NBIB. But I'm in motion to pay it back just for the lawyers' purposes here and make sure it's covered here. Or was that a bonus, Gary?

Help me out with that one. We made that transfer. Again, no real issues. We end up looking at an organization as Gary points out that as you start asking yourselves, and we did this throughout the transition, moving inward, moving up to it, what do we look like? What is our focus? What is it that DCSA is? And it really boils down to two big questions that we are here to answer.

One is, do we trust the people that are coming into the government, either as staff employees, as contractors, as affiliates, whatever relationship they're having with the government? How do we vet those individuals and make sure that they can be trusted? Continue that vetting throughout their time and inside the wire here. Second thing is again, a longstanding traditional focus is cleared industry, which is providing a lot of that technology. It is giving this country that edge. How do we protect that critical technology?

And everything we do in this organization answers one of those two questions. In fact, frequently it answers both of these two questions because a lot of what we're doing here, all the moving parts that are in this organization, whether it is investigations, whether it is adjudications, whether it is a counterintelligence activity, whether it is industrial operations, whether it is building an IT system support, all of this stuff, whether it is all the training that we provide across the spectrum for a number of different people, all of that goes to answer those two questions.

Trust the people that are in here and do we trust that we can protect that critical technology that is in the classified world today? We expand as Gary suggest beyond the world of classified into some other things which we'll talk about in a minute here, but can we continue to trust that? And that's really what we're focused on here. Obviously as you guys know, all of this interacts with the national security program that all of you are part of here. National industrial security program, I'm sorry. As Gary said a big organization, 105 agencies we're supporting on the vetting side, 33 on the technology side. When you put everything together, whether it is staff or contract people we're getting somewhere between 11 and 12,000 people on board doing this work every single day. That number varies depending on some of the level of efforts that are going on here.

I would say that our goal was to have this transition with no speed bumps. We virtually have no speed bumps in this. A couple of little nitnoid things out there, but the big issue is moving the people, moving the funding happened literally overnight. And... There are folks at a certain part of the government that are looking at this thing. This is so unusual. This really becomes a case study, how to do a transition in this business area here. Again, guys in industry will understand this; we took a merger and

acquisition approach to this and followed a lot of the business processes. Again, Bill and team that Bill Lietzau that's got together, helped us sort of formulate and think about through a lot of these things. And recognizing again in a true M&A fashion, the businesses that are emerging in an M&A have to keep doing it .And that's exactly what our goal was, to keep that business going, get everybody over the transom and focus on getting those things going. We've got a lot of these transitional things still in motion, somewhere in motion before we even got started. And our goal was not to mess with that progress here.

Two big things again that we're focused on is how do we deal with protecting critical technology? And in this transition that we're in right now, we'll talk about in a few minutes. At the same time the thing that has been nagging everybody is how long investigations done, and a lot of activities were in place as we moved through the transition. They continue in place. I'm not going to do a lot of statistical conversation today, but I will drop one number on the inventory, which was sort of astronomical at one point as of two days ago. Today is Wednesday, right? I'm still recovering from the weekend. The Monday inventory number for investigations was 267,000. Which, and when you think about in investigations, working investigations inventory, our steady state based on today's method of doing business is about 200,000 to achieve the timing that we need. I think we're getting pretty close. I'm pretty happy with what folks have done on this thing.

A couple of personnel updates as we organize this activity here. I have two deputy directors for DCSA. One focused on critical technology protection, one focused on making sure cell phones are not activated in the building... That'll be reflected in incident report to Gary. It's an update, yeah. The number is now 265,000. The other is for, and so on the technology protection, Kerry Weaven had that job when we did the transition. She has moved on to a private industry and probably a shop somewhere in your doorsteps... I'm going to guess. We have an acting there; Bill Stevens, some of you know, is running our counter-intelligence activities. He's acting as a deputy director in that area. On the personal vetting side, Christie Wilder who came over from NBIB is the deputy director personal vetting side. We're continuing on in that area.

Focusing on these two areas, let me give you a quick update on vetting updates. I'm not going to talk about statistics and stuff, but I think it's been important; it continues to be important for us to continue the relationship we have with industry and with our other government partners here. An example Chuck Barbara sitting in the audience here recently enterprise business support office to engage with a few key members of the NISPPAC to address them on the system requirements we have as we're building out the new interfaces for both industry and government to be able to get into

and maybe get out some of the systems that we're working to, all those number of systems that we've referred before. We're going to need to expand that engagement in that particular issue and continue the engagement we've had with a lot of you overtime both on the vetting side and how we're rethinking on the industrial operation side here.

I had an opportunity when we're at the NDIA meetings in Arizona a year ago or I guess a month ago, to talk to the NISPPAC representatives and just get some feedback and I would say at this point that I got a lot of good feedback. One of the questions you guys asked at the time is, is the feedback loop that we have had both with NBIB and with DSS from the legacy organizations is going to continue? The answer is yes. In fact, there were some inadvertent cutoff on some of this stuff. We're going to put that... not done on purpose. It was just, we sort of lost track of a couple things. We're going to keep that going and keep working on that. A couple of real high highlights on the on the vetting side. Again, I'm going to defer this to Ned who'll talk in more detail and show you some good-looking slides. But during the fiscal 2019, you all gave us, you all industry sent to us 141,000 or so investigation requests. And that's a pretty good number here.

We put a number of folks into our CE program. Probably 1.4 million people are in our continuous evaluation program, but a quarter of those are industry. And so, we're keeping track of all that stuff. I know there's concern out there on the vetting side about how do we track that. And it's been a little bit hard to wrap our arms around, but we are going to be very shortly able to in the release 9.0 of DISS be able to, you'll be able to track where and why folks had been enrolled in CE. We worked out an arrangement with the DNI to be able to let other agencies understand why people are in our CE program, why we haven't deferred some of those to some of those periodic re-investigations and not penalize people who have been put in that deferral status who are going to be trying to be crossed over and otherwise moved across that transom here.

By the end of the year we hope, maybe January at the latest, by the end of the year we hope to be able to put all of that information about who is in a deferred PR program and the status into scattered castles and into CVS and make it available to everybody access to them. We'll see where that goes. On the adjudication side a lot of the CAF efficiency activities have been going on, some of the mirroring, some of the process engineering stuff we did the investigation side are paying dividends and I would say probably about 50% more efficient today on those than we were, if we're looking back at... So again, we're making some great progress in that standpoint, but that really sets us up for, and as we put all that together is what in this vetting world is not... it's a future goal but not a distant future goal.

And that is to become really ready for continuous vetting as soon as Valerie and her team tell us it's okay to do that and make that more formal through the... but this I think is one of the biggest CE changes in how we think about trusting people in easily the last 70 years. We do a really good job up front in the initial vetting. We will continue to do that and then put people into a continuous vetting program where we were able to identify problems much sooner. And as people... this happens as you guys know, people deteriorate in how they think about protecting classified and sensitive information, whether it's because I'm evil or more likely because I'm just dumb. They devolve. We need to be able to see that happening sooner rather than later and take measures to stop that problem from occurring here.

Moving on to-- so we would be prepared. Moving on to the critical technology. Gary gave you a lot of the precursors of why we're doing this, a little bit on some of the practical aspects. Understanding that DCSA is really where the rubber hits the road in terms of working with industry and working with our government partners and putting the reality around that. Our focus in the past and continues to be in this fiscal year is a strong relationship with industry, with our government partners and as it relates to the NISP operations. I know there are a number of ISLs out there, industrial security letters that you all are looking at and providing feedback on. I will tell you that I personally and as an organization, we collectively appreciate the candid feedback that we are getting.

We will continue to process that feedback. Some of the things I know are worrying not just industry but worry us in government as well is so exactly what does a security plan look like, intelligence security plan looks like? What exactly are we looking for? Appreciate your feedback. This will be a continuing dialogue. What does it mean to put CUI in enforcement out there? Kind of a new thing. I know it's been around for a while as a concept actually enforcing it with the complexities that are involved is going to be a challenge for all of us. And we are sensitive to both those two things I just mentioned. We're not going to force things down people's throat. We're going to continue the dialogue with everybody involved and make sure that we get this right.

We'll again continue working with USDI and with NISPPAC on the convent adjudication to make sure that that we've got this... We did get some feedback the way-- I was not part of this, but the way that this team managed the conforming change too in the insider threat requirements and in the NISP about three years or so ago is a good role model for how to do this. We can go back and look at the lessons from that and see how that feedback evolved and do work from there here. I know we've got a lot of data systems out there. I'm going to read them and make sure I've got them

right. This, this and this. NCCS, e-APP, E-agency e-MASS. Some of them I can actually tell you the whole name for all of these things.

A lot of stuff, a lot of opportunities for us to do talk about those things. I'm not going to go into excruciating detail of that right now, but we do want to make sure you guys are included. That's everybody included in developing the requirements and the implementation strategies and getting feedback on how these things are actually working. It's going to be really... you'll get some more out of some of the other speakers on this today. Gary Reed has talked a lot about the high-level stuff here. To me this is an exciting time to be in this business here. A lot stuff going on here, whether it is business process reengineering, whether it is trusted workforce 2.0, you'll hear more about that. Whether it is rethinking critical technology protection, what does it mean to deliver a product uncompromised?

We're taking a page from continuous evaluation, continuous vetting, and for us this is really going to be a continuous transformation and should be a continuous transformation. We've got to continue to look at everything that we do, get feedback, move it back into the process so that we are not static as we had been maybe for a long time in all of these parts of the industry here. You guys are a key to our success. We want to continue the partnership. And we're staying focused on this as our missions. With that I'm going to shut up and leave time for some questions.

Mark: Charlie?

Charlie: You guys all want to get out of here early today. Don't you?

Mark: Is anybody on the phone or WebEx?

Moderator: Ladies and gentlemen, if you'd like to submit a question, you have two ways of doing this, either through the WebEx by selecting all panelists from the dropdown menu or through your telephones by pressing pound two on your telephone keypad. You'll hear a notification when your line is unmuted. At that time, please state your question.

Mark: What was that?

Charlie: Agents are over the wing. Please place your tray tables in the upright position.

Mark: That was almost Chinese. Okay, Charlie, thank you so much.

Charlie: Thank you all.

Mark: Now hear from Heather Sims.

Heather Sims: Thank you. I'm sure I'm going to have lots of questions. Good morning. I am Heather Sims. I'm the newest member along with Aprille of the NISPPAC. October 1st, I was also selected to be industry spokesperson. Long 50 days already. It's both an honor and privilege to be able to provide you industry updates today. Briefly I'm going to cover the current NISPPAC membership, the MOU membership, the current working groups as well as some policy changes that are affecting industries, 2020 industry key focus areas. Charlie already covered quite a bit of the systems. I actually had a slide that would have helped you out that lists most of the systems out there. The supply chain and some small business concerns that we're worried about. This slide is the current listing of the industry and NISPPAC members. And again, myself and Aprille, we have terms to 2023. Our terms are four years each. This is a current representation of the industry memorandum of understanding; MOU members, and our newest member is Kathy Kaohi, the NCMS president.

Alright. Industry has wishes and continues to partner with our government partners on working groups to provide expertise early in the planning process. Here you have the ISOO and the DCSA working groups listed individually. While many to include the clearance working group has been very impactful this past year, industry respectfully requests that the NID working group could reconvene to discuss some of the timelines and some of the processes that may need to be reviewed. Due to the various changes in terminology and methodology with a risk-based industrial security oversight, RISO, industry formally requests that DCSA engage industry to address current and potential issues as well as formulate implementable plans to get to the intent of risk-based process. Lastly, industry requests the insider threat group reengage to discuss the maturity of the insider threat programs as well as the next steps in the oversight process.

This could also start the conversation and process of updating subsequent CDSC products in anticipation for the insider threat Industrial security letter released. The previous insider threat working group has been designated as the best today collaboration. Industry wishes to continue with the positive impact during the next phase of evaluation. I'm not just saying that because I was on that working group on the government side... Due to the enormous amount of new policy affecting the NISP, in draft policy working group under ISOO was requested to better centralize and engage industry during the review process to convey the potential impacts to industry and develop solutions for implemental policy throughout all cleared industry. While industry understands the government does not have to request our permission to implement a new policy or procedure, we realize for a smoother and quicker rollout, industry input throughout the process will get the government quicker results on their intended outcome.

We don't anticipate it slowing down. With the introduction of delivering uncompromised, risk-based industrial security oversight, controlled and classified information and now cybersecurity maturity model, CMCC, CMMC. There is a concern that focus will be taken away from the NISP and the protection of classified information if not properly coordinated and funded. Continued early engagement, communication and collaboration with industry is the key to reducing some of the challenges when implementing new or updated security policy and or practices. Industry comments were provided with many draft documents and many others are under review as indicated on this slide. Industry does request that we get an update on the usage of the evaluated products list and cross-cut shredders in the investment of marijuana, ISL.

The 2020 industry key efforts, while not all inclusive, focuses on addressing concerns on the following. Little industry engagement was with risk-based industrial security oversight since early 2019 has led to much concerns throughout industry. Specifically, what is the status of the security rating score; SRS? What is DCSA doing to remove the subjectivity of SRS and how we'll be using the acquisition process? With a discussion that the security rating score could affect the company's ability to win contracts, it's understandably a major concern for industry going into 2020. Inconsistencies with DCSA activities and field offices is causing industry to divert attention and resources to processes that have not yet been formalized, which could lead to even greater risks within cleared industry. Creating, convening industrial security oversight working group would be beneficial to both government and industry. CUI and CMMC. The existence guidance is conflicting, and industry has already been engaging with multiple government agencies and military component customers on reviewing of unclassified systems for control defense information. That's leading to inefficiencies for both government and industry notwithstanding the countless hours and resources that industry have used to prepare for these visits. Industry is awaiting information on what steps are being taken to ensure a consistent approach to oversight of cleared contractors in the NISP and our uncleared supply chain. Overall, some of the concerns are who owns the process, how will government communicate to ensure a systematic approach to industry and how can industry become more involved?

Insider threat. While the initial insider threat working group has been noted as the benchmark for ISL creation and implementation, the program would benefit from reconvening to discuss the next steps. Trusted workforce 2.0 and personal vetting. And I'm proud to say in the past few weeks, industry has been working with government officials and have become active, is actively involved in the trusted workforce 2.0. Currently there is now NISPPAC representation in meetings and engagement has been very much

appreciated. Noticeably missing from these slides is personal security investigations. NBIB, now DCSA has made great strides in hearing industry's concerns and offering transparency into the efforts to bring down the inventory as well as create efficiencies in the investigation adjudication process. And we do appreciate those efforts.

Well, I couldn't cover each of these systems in here. It would take up my full 10 minutes. You can see from the slide there's numerous systems that are coming online at the same time, or have been put online at the same time that impacts the industry. While on the surface, industry's concerns on system rollout are being addressed individually, there are still many systematic issues impacting industry's ability to perform on contracts. When all systems don't reflect the same information, there has been risk to customers removing contractors from work sites. A sense of urgency needs to be placed on providing system wide resolutions versus fixing one-on-one issues.

Again, my list of systems was not all inclusive. It's just the ones that are majorly impacting industry at the moment. We hear multiple times from multiple government personnel that the threat is increasing on theft of our intellectual property and industry must act to protect while the principles behind delivering uncompromised, risk-based oversight and supply chain risk management are understood by industry, industry must balance meeting the NISP intent, surviving in a global economy and keeping a viable supply chain. Overregulating without set policy and not understanding industry's concerns in advance could impact the entire supply chain supporting United States government. That concludes my formal briefing. Are there any questions?

Mark: Any questions for Heather? Let me say, Heather, we will reconvene the NID working group. The thing I ask in order to make it meaningful; we need reliable statistics. I get hit with anecdotes all the time. It's funny, I can sit in a meeting with the government and be told it's not a problem. I can sit in a meeting with industry and you think the sky is falling. There's got to be some type of middle ground on this and the only way we can resolve this is to have actual meaningful data. I need statistics. Alright? I'm tasking you both with delivering those to this working group. Otherwise it's just an exercise. It's a debate and it remains unresolved. Alright. We now hear from Devin Casey from my staff on the CUI program where he stands and...

Devin: Good morning. I'm Devin Casey on the CUI staff. I'm all that stands between you and your first five-minute break in this two-hour meeting. I'll be quick. I do also only have five minutes, so I should be able to cover everything. I'll go over a quick update on CUI. I want to hit some points that were mentioned previously. This slide is more of a takeaway for you. It has ways to find out

more about the program, ways to stay engaged. We'll talk about other ways to ask more questions or understand what's happening in the program as we go through the presentation.

Our first update is agency implementation. We're currently still receiving the last stragglers of our annual report this year. Based off the information that's come in and a quick review which we'll be doing analysis on over the next few months, most agencies will have their head high level policy published within the next 12 to 18 months. And that's probably the most important milestone in the development of the CUI programs throughout the executive branch. There's the development of that policy. Many of the other milestones only take three to six months, after that the development of training and when they begin marking other information. Again, we'll have more information as we go through a deep dive of the annual reports that come in this year on agency's implementation status.

CUI FAR. Another topic that isn't a joke. I am done predicting when the FAR will come out. But I will promise that when it does, we'll know, and you'll know at the same time we'll post to our blog. We do have a format on the blog where we invite people to quarterly stakeholder updates. We do have one scheduled. There will be an ad hoc stakeholder updates specifically to address questions of FAR. I do have a note here that says we won't be adjudicating comments during the question period. It'll just be the answer about the intent and content of the FAR so that we can get better comments back. It's very hard to use a comment that says, what did you, what were you even... when we got those back from industry.

We want to answer those questions so that you can provide guidance on how to best get those goals accomplished throughout that type of policy. There will be an ad hoc specifically addressed to assist with those comment periods on the FAR. I can say it's not delayed for any particular reason. It's not hung up on a particular policy issue. It's not hung up on a particular office. It's not stuck in legal review. It is working through the GSA policy procedure for comment. It's just taking a little bit longer than expected. Chances are you'll end up seeing the privacy case when our case come out pretty close together.

The next thing that was talked about we've been listening to industry. Industry has been talking. We did put up one notice on CUI talking not just to DOD, but the entire executive branch about our plans for how agencies should conduct oversight on non-federal entities. We've already had a CUI notice that talks about the content of agreements of CUI. We're having a requirement in 32 CFR 2002, which requires the reflection of particular controls for the CUI program into contracts and agreements. And this notice starts to get the executive branch ready for what we're looking for out of

our oversight programs and their oversight programs more importantly through their contracts and agreements. It is the senior agency officials for the CUI program to establish and plan and execute their oversight, not just internal to the agency, but also through their contracts and agreements.

And one of the key notes on that and that notice that we put out is the reciprocity or ability to create reciprocity between these oversight entities. As we're already aware that there's redundant oversight just within DOD, we're prepared for that oversight to become or possibly become more redundant as the rest of the executive branch implements the CUI program. What we're doing is encouraging training, educating and facilitating a better reciprocity and understanding of how best to take advantage of the work that's already being done in that by other agencies that conduct oversight/ We're very involved in DOD's current efforts that they're doing as an interim for their CUI program as they come up with their new policy that actually implements the full CUI program and of course steps and measures that they take in things like CMMC and others.

We want to take those lessons learned from inside DOD and share them with the rest of the community. This notice is the first step towards that. There will be a lot more to come once our FAR comes out. But the key tenants here are, we all have limited budgets in the government. We have an even more limited budget when we talk about the oversight of security that's not very mission focused. We want to make sure that that budget gets spent appropriately. And one of the best ways to do that is by making good risk-based decisions and you make the best risk-based decisions with good intelligence. That intelligence is something that you can get from other executive branch agencies. When they come out and they do these visits, we're looking at ways to standardize what the results of an inspection of the CUI and systems would look like and how to easily communicate those results to other agencies as well as to industry or back to industry so that we can cut down on executive visits. And so, one of the things that we're encouraging training and attempting to require is that that due diligence be done prior to the visit. We don't have the authority to limit an agency's ability to conduct a visit and assess the risk in their contract environment, but we do kind of have the ability to say you have to do so intelligently and well and then the best decisions get made with that available information.

We get a lot of questions about CUI and DOD and we're not the CUI program office for DOD. They have a current program. As mentioned very early in the COI process, we always said there will be a transition period as a government and as agencies implements CUI and we're smack dab in the middle of it. So that's why you have a little bit of confusion. We're working with DOD on communication strategies. We put out this notice, DOD is put out a lot of information on it and you can find most of it here. CDCS has a

toolkit out for CUI. There are two quick boxes you check on, what we're doing now and what we're going to be doing soon. There's the DOD procurement toolbox, which has actual and frequently asked questions and a way to ask questions directly to DCMA and their CIO about compliance with CUI requirements and the DFAR 7012. There's the DCSA CUI tab. A little bit of information now, more to come I'm sure.

And of course, if you want information about CMMC, that's on the acquisition, OSD MIL CMMC site. I believe they just had an open meeting yesterday discussing the accreditation body. But it's a great way to get that. They do have a version 0.6 out currently and you can see what that version is and how to comment on it on that website as well. Some upcoming events. We do have an industry day coming for CUI. The main kind of target audience for this is agencies and the agency personnel who are implementing CUI to understand what type of technical solutions are available or other solutions available through industry that they can provide to help agencies implement their CUI program. There'll be an invite for our people to have boots and or possibly presentations. Stay tuned to our information on that. And then the next CUI stakeholder meeting, which is an open WebEx to any stakeholders including industry, academia or nonfederal partners and as well as agencies. That will be on February 12th. It's an online WebEx. The only thing you have to do to find out how to get there is visit our blog and read the blog.

A couple of notes on some of the slides earlier before me. We are obviously encouraging industry engagement in the development of the CUI programs. There's the built-in engagement that occurs to the FAR through the public comment process. I do think when you see the FAR, a lot of your concerns, not all, but a lot of your concerns had been built into the text of the FAR, the draft FAR clause. Things like mandatory marking from the government that they must mark or identify any information they expect to receive, top of the list for industry prior to the CUI program. That information that requires differing levels of protection to be marked accordingly and that those levels of protections are communicated prior to the receipt of that information. These are all things that we've heard from industry that we built in and obviously you'll get your comment period during that. Now, you'll also notice we did share a CUI notice to NISPPAC for comment. That's one of their policy elements that they're commenting on. So, we do try to stay actively in...

We do have our stakeholder meetings, which isn't just for us to talk to you, it's for you to talk to us. So please do let us know how things are going. And as well as in this notice and the one I was previously talking about, we do encourage that you talk with your agencies respective CUI offices if they're standing up and if you are having issues between yourself and those offices

or those offices are having issues inside the executive branch, it's actually in our 32 CFR 2002 phase two, our office for adjudication. To learn more about CUI because five minutes isn't quite enough, archives.gov/cui. That's where all of our notices are. That's where all of our policy and guidance, we have training on there as well. The blog is the best way to stay up to date and you can search for the CUI blog. I think we're one of the only ones. And our email cui@NARA.gov goes to our whole CUI staff.

Mark: Questions for Mr. Casey?

Devin: I guess I answered them all of the stakeholder meetings.

Mark: Yeah.

Devin: Thank you all.

Mark: Devin mentioned one of the notices. You can see the industry comments. This is on assessing CUI systems and non-federal systems. And some great comments. We appreciate industry's comments on that. We will be adjudicating those; we're still waiting on a couple of government agencies to provide their input. Some requested additional time. So got that on...

Devin: Thank you for those.

Mark: Alright, we're up just on the verge of a break, but before we're going to hear from Valerie Kerben the security executive agent for DNI.

Valerie: Thank you Mr. Chairman. I just wanted to give you a little update on SEC EA's policies and where we are in the process. As I mentioned before, we are working with security executive agent eight, which is on temporary eligibility, which establishes the policy and requirements for authorizing temporary access to classified, but it also includes one-time access and for those eligible to whole sentences. I think as we all know policy takes a little while. It's been out a few times of review informally with the security executive agent advisory committee, but back to OMB as they submit out our formal policy in the formal process. And we're right now finishing up third rounds of review. Thank you, government agencies, for giving us those comments. They're really good comments that we're considering. We're hoping that this will get clear from OMB this month and then it would have to go to the acting DNI for signature.

Keeping our fingers crossed, this will be issued this year, Seed eight. Seed two for the polygraph and support of personnel security for initial and continuous eligibility in the vetting space. That went out from OMB for comments to departments... collecting those comments right now. For trusted workforce, you've all heard some things from Gary and Charlie and

as you know, we're working very hard to get all this policy information out. The documentation, the top three documents are all basically ready. We're just waiting for signature. But as I've mentioned before, we work this through in two phases and phase one was reducing inventory and as you heard the inventory is at a great state and that's really a great success story. The phase two of revamping the whole fundamental approach to doing clearance verification and clearance processing has been re looked at and we're going to have this new framework and it's really going to overhaul the process, improve timeliness, quality and really help out in the mobility of contracts moving from positions and in and out of the government.

It's also going to be based on a whole continuous vetting model. A lot to come, a lot more that we'll be updating you on. I also want to say it's just a lot of synergy together with our other PAC principal partners working through this whole process. And as Heather mentioned too, we've had a few engagements with the NISPPAC giving update to the process and we'll continue to do that and keep the dialogue going. I know we will plan something for early New Year to have our next meeting even though there was an informal meeting at NDIA with Greg and some of the other members. We'll have something coming up. Okay. And also, just there was a great article in today's paper. Brian Dunbar, my boss also spoke about trusted workforce. If you want, some more update is in today's federal news.

Mark: It's in seed nine?

Valerie: I didn't.

Valerie: Yes, it's still in process.

Mark: SEAD nine, whistleblower seed is still in process.

Valerie: Yeah.

Mark: Okay, thank you.

Valerie: Thank you.

Mark: Any questions for Valerie before we break?

Female Speaker: Valerie, thank you for sending me that memo from yesterday. I just wanted to clarify one thing just for my own perspective. On the whole reciprocity with regard to people in continuous vetting or continuous evaluation, whatever it is, when this was put out, when it says reciprocity, was the focus when someone leaves one government agency goes to another or is that also applicable if a contractor was coming to the state department who

needs a CI access, are we obligated then to accept the fact that they're in continuous evaluation, no matter how old their background investigation is and grant them a CI access. Was that the intent of this or was it a different intent?

Valerie: That's the intent, but if you would need to confirm that they're in either ODNI's system or DOD's process to confirm that things have been checked and looked at and that it was a favorable risk-based decision. If the eligibility is still there and continues, then we are asking agencies to accept reciprocity.

Female Speaker: But that's just a phone call to verify through non-DOD agencies just to verify if someone's in there.

Valerie: Right. If it's not, it is a phone call if it's not reflected in the system or if you can confirm it by looking into the database.

Female Speaker: It doesn't matter how old the background investigation is?

Valerie: Correct.

Female Speaker: A 16-year background, old background investigation would be okay.

Valerie: Well, I would hope something in NTSS CI has not been not looked at in 16 years.

Greg: I think the attempt is continuous evaluation, continuous vetting is essentially a continuous investigation, if you will. If you think of it in terms of really PRs is an antiquated term as we've transitioned into continuous evaluation, continuous vetting. It's like an ongoing investigation.

Female Speaker: I know, but I think it's a cultural thing, we've all been beaten into us for years. What's the date of your last background investigation, is it current, how many years and stuff? It does a total culture shock to some people; I think to say your background investigation is never going to be reflected to be other than the date it was done however long ago it was.

Valerie: Correct, it is a culture change. We all have to understand it now as the continuous vetting in the automated record searches, they'll be looked at on an ongoing basis and if things are raised or going through whatever issues or something that has come up and agencies can always extend or do some investigative product and follow up on those issues. We're not saying you'll never do a re-investigation, but for those clearances they could go into the **[1:20:42 inaudible]** and just move on to those that might be a higher risk.

Male Speaker: Alright. As an investigator, it's PR every day. And I know that sounds really nice, but there's also, when you see it there-- I'm sorry, there will be established thresholds for certain types of checks and activities. It's not just what comes in the door, right? There's push and pull. There will be minimum thresholds periodicities for certain checks and then there is the daily credit pop that could occur. There's spectrum of data checking that occurs under this. And this is the problem we had in DOD is people are used to thinking that CE is some sort of courtesy thing that happens on the side and until the policy changes, we're in the center. But with the new trusted workforce framework and the NSPM, we've established there's a PR every day. There is a mindset change that will happen 16 years after it gets signed. Someone could have a 16-year-old one today. No one should have one that hasn't been initiated within the established window already.

Female Speaker: As an agency, if we see that a contractor has that older investigation, we're trying to process them for a CI, do we have the ability to ask someone through DCSA to do a PR and even if they're in continuous evaluation because their investigation is so old. I'm just wondering if there's any kind of wiggle room in that regard.

Valerie: Well, I would say there would be, there's probably some wiggle room. We'd have to know what anything you might be aware of something or, but I think there should be contact with the owning agency.

Female Speaker: So DCSA then?

Valerie: Yeah.

Male Speaker: Under the old premise of reciprocity, if somebody was within scope or I'm sorry, somebody was out of access and going for a year or so, the requirement was or the expectation was you would bring them back in with whatever level of access they had except that reciprocity and then launch your periodic re-investigation you wanted to. I would imagine that possibility could still exist here. The key to this thing is trying not to-- just trying to avoid a break-in service. If somebody comes to your door, whether staff or contractor with an Up-to-date, now in this continuous vetting world, involvement in continuous vetting, any issues that have popped up had been looked at, adjudicated, whatever it may be 16 years from now that we're still doing this, nervous about it, fine. Bring him in, cross him over, get them in the door. And then if you want to potentially launch a periodic reinvestigation, that product is still going to be out there depending on the need for something. But the goal here is to avoid having to stop everything until you want do periodic reinvestigation.

Female Speaker: So, we'd have to ask. I mean, we wouldn't do the periodic reinvestigation, we have to ask--

Male Speaker: If somebody asks you to do it, right, exactly. Yeah.

Female Speaker: That's why I wonder if there's a mechanism to do that, ask for that.

Male Speaker: I believe there will be, and Valerie will make sure of that.

Mark: Anything else? Alright. We'll take a 10-minute break. Please be back in 10 minutes.

Female Speaker: Thank you.

Moderator: Ladies and gentlemen, your conference will restart shortly. As a reminder, during the Q&A sections, if you would like to ask a question, pressing pound two on your telephone keypad or you can enter your question into the message area in the WebEx. Select all panelists... we may hold music until the conference is ready to begin. Ladies and gentlemen, your conference is about to begin. Please stand by. That'd be a moment while I connect the call.

Greg: Alright. As you can see, Mark Bradley had to leave for some senior executive training. So, I'm here for him. We gave you a little bit more time because we're ahead of schedule during the break to do some networking. Started now on the working group reports. And first up on that we'll hear from the NISPPAC NISA, that's the information systems authorization working group. I think we got a tag team on that. Alegra Woodard from ISOO, our staff and then Carl Hellman from DCSA will add to that discussion. Alegra, it's all yours.

Alegra: Good morning and welcome back. I'm Alegra Woodard, ISOO staff member and representative to the information system authorization working group. The key takeaways for the work from the working group are as follows. The first items have to do with the cybersecurity model certification CMMC, say that three times really fast and have a tongue twister. We've been dealing with CMMC all morning and we have that discussion today. Within our working group we heard during the industry update that there's been a request for clarity on the status of the CMMC process. Based on this request, ISOO hosted a CMMC presentation by Ms. Arrington who we heard is the chief information security officer for acquisition.

This presentation took place on Tuesday, October 29th here at the national archives. The second item pertains to media sanitation and disposition guidance. Industry express concerns because there seems to be inconsistent guidance among regional approving authority on how to sanitize and

dispose of solid-state media. The working group agreed that although the immediate concern our focus on regional AOs, the topic may have larger implications and may require further discussions at the CSA level. For these two items, the next step is for industry to document the specific concerns to include examples and submit them to the working group for review.

The third item was also part of the industry update. In a memo to ISOO, industry expressed concerns that the current DCSA methodology for assessing implementation of cyber security protections of a classified system is inconsistent with all USD guidance. In response to this memo on September 6th, ISOO a control on classified information notice that we heard about during the CUI update. The notice addressed the oversight of the CUI program within the private sector entity. ISOO communicated industry's concerns to DCSA in a memo and September 16th and ISOO responded to industry memo on September 17th.

The details of the memo pretty much covered teeing up the conversation about the concerns and then some of the recommendations from ISOO as to next steps for DCSA. DCSA provided an interim response on October 25th and during our working group meeting on October 30th, a representative from OUSDI informed the group that DOD is working on a final response. So, all our takeaways and updates. Our next meeting is scheduled for Wednesday, February 26, 2020. We anticipate a full and active participation from all members, particularly all governments CSA representatives. This is all I have. Any questions?

Greg: Any questions for Ms. Woodard? Caroline, on the phone? WebEx?

Alegra: Thank you.

Greg: Thank you, Alegra.

Carl: Good afternoon, Carl Hellman from DCSA. Just a couple of additional items from the the NISS working group specific to DCSA. We are currently working with the NISA working group on an update to the DCSA assessment and authorization process manual. Our last update to that was in April of 2019 and it implemented a bunch of new procedures and processes for our transition to e-MASS as our system of record for authorizations and assessments. This update that I think the working group still has till December 6th to provide us input.

We will spend the month of December adjudicating those comments, providing adjudicated comment feedback to the working group. And then in January we will have the process manual version 2.1 published. Along with that a change log of all changes between 2.0.1 and we have no specific high-

level action or activity that's engaging this change. It's just to initial review of what the procedures that we may have in the manual since we transitioned to e-MASS that aren't working for industry and aren't working for the DCSA internal folks. So, it's an opportunity for us to just address those. We appreciate the NISA's working group being that focal point to get all industry comments and feedback to us so that we can have a better product.

Another item I want to talk about is the windows extended service updates. For the folks who may not be familiar, Microsoft plans on ending doing an end of life for windows seven and windows server 2012 in January of 2020, which means there are no more vulnerability patches or vulnerability updates for those systems. We published a memo earlier this year, a couple of months ago regarding Microsoft makes available and extended services update, which can be purchased to be able to purchase for individual licenses, vulnerability patching and update for those two systems. We provided a guidance out to our field internally and to industry externally, which we provided to the NISA working group. We provided it to NCMS, AIA, NDIA and we posted it on our external website on the availability of purchasing that and the process that you would need to do to engage with us if you are not upgrading from one of those end of life legacy systems to a current system like server 2016 or windows 10.

One of our pieces of feedback that we got from working group members had to do with specifically a transition for already authorized systems from windows seven to windows 10. We are currently working-- I'm working with the regional authorizing officials. We're currently working on some additional guidance to publish on that so that everyone has an understanding of what that process will look like, both from an industry perspective and from a DCSA review perspective for that transition and what we expect with that. We'll be coordinating that with the providing some initial what that initial guidance looks like to the NISS working group members feedback on what they see as potentially impacts.

As a Alegra talked about the solid state media sanitization, we are engaging with the folks at NSA who do the evaluated products list to talk about what they see as an industry standard for clearing and sanitization procedures so that whatever we define from a consistency level at DCSA, we're also engaged with the experts at that for those processes. So that's still to be ongoing. And then two last items, obviously we've talked many times about our transition to e-MASS and we are engaged for those that don't know DCSA, our e-MASS program manager has a seat on the configuration control board of DISA for that e-MASS application. And we continue to actively solicit through the working group for industry comments that we can take to the configuration control board to make e-MASS a better application for our instance. And finally, we've been working both with the NISA working group

and some other industry working groups on taking some actions to improve authorization timelines and consistency. So, we've been engaged with a group of folks to include some NISPPAC NISA working group members and some other industry members on addressing some concerns we have with that. And pending any questions, sir?

Greg: Thank you Carl. That last point then I noticed one of the industry concerns on their slide had timelines and the delays and then we wanted to know what could be done to address extensions of approval to operate. Is that what you're referring to?

Carl: That's specifically right, that's a specific group that we have together, which includes NISA working group members is two trends that specifically.

Greg: Very good. Anyone have any questions for Carl? Phone? Carolina, WebEx? No? Quiet group relatively today. Okay.

Carl: Thank you, sir.

Greg: Thank you very much. Alright, next up is the clearance working group. I'm going to just give a brief run down. As usual, a lot of things we've already spoken about today were part of what we discussed in the clearance working group. Obviously, the clearance data and we'll have Ned Fish do some metrics after I do this as well as Perry Russell-Hunter from DOHA, but the metric data on clearances is moving in a really favorable way on the positive and you've heard that. We're pleased, kudos to DCSA and whomever else has been helping with that. As a clearance working group, we're looking beyond just personnel security clearances. Some of the things we discussed are there's ISLs that are in the works and there's five of them from some of what you heard already, the tailored security plan, insider threat, the seed on foreign travel, ISL and a couple of others.

We also got a little bit of an update on the NISP intrusion detection system standards for qualifying an entity to certify alarm installers. Just as you may know, UL has been sort of the one and only entity that could do that. There's at least one other company that asserts that they are certified to do that under the national recognized testing laboratory standards, I think is what it is. NRTL is the acronym. We met with both in a small group, DOD and ISOO and a few others with the two, the other company is called Intertek. And we met with UL. We met with each of those folks separately to get a better understanding of how they can assert that they meet the UL 2020, 50 standards.

We're not there yet, but I think we're on a path to where we'll come up with a solution to where it's not just UL that is the only entity that is qualified to

certify alarm installers and to me that makes sense. We also discussed the several security executive agent directives that are under works. I do want to state publicly the seed nine whistleblower, I am not the whistleblower. Anyway, and as I said, the personnel vetting data, we discussed that as well. With that I'll take any questions and then I'll ask Ned, or we can wait until after Ned's presentation. Does anyone have any questions right now on anything I said? On the phone and WebEx? No questions. Okay. Mr. Fish, you're up.

Ned: Well, good day everyone. Some of you might know me formally, my former position was as the DOD CAF director and with the transition in the transfer and all of the things that have happened. I am now the deputy director of the defense vetting director. Ms. Mariana Martineau was the CAF director. She's in the room here, accompanied by Heather Green who's the director of the VROC. And they along with Dr. Chuck Barber are the key entities within the defense vetting directorate. The slides I'm also going to speak to today or the slides I will speak to also include the investigative side of the efforts. And that is of course a separate within DCSA not part of the... really, I think these slides, a neat thing is they're indicative and perhaps emblematic of us coming together as one organization just to have investigations... vetting of continuous evaluation.

We as a new organization are coming together with some clearer and blended metrics that hopefully you'll find useful. As both Mr. Reed and Mr. Fallon alluded to earlier, the transfer and now we're not-- we've been actually transitioning all along went well and that's really due to the professionals that are focused on that mission set. And I think the statistics you'll see today are also indicative of that good work that performed throughout the whole process while everybody else was doing the heavy lifting of transfer. First on the investigation side of the house, you can see the numbers are impressive. About a year ago there was 590,000 cases in the investigative inventory. Well, today Mr. Fallon stole my thunder because my numbers are dated as of last week was 273,000, it's actually 267,000. So those trend lines are going very, very well with DOD industry affiliated personnel being about 41,000 of that.

On the CAF side of course, there is no eligibility without the CAF's adjudication. And I think this is a good news story because unlike historic backlogs that have been worked through in the past where they had that pig working its way sequentially through the snake, actually I think a large part of this is due to what we're doing with CE in lieu of the PRs etcetera and the good work at the CAF as well is they're actually consuming the backlog simultaneous to the... investigators are consuming their backlog. So, on the CAF side of the house, the CAF work in progress today is about 105,000. It's important to state that there's about 73,000 cases that we are listening to

that's deferred periodically investigations. What that really means is in that 105,000, we are working to get your people, those initials, get your people to work are our priority as well as the derogatory PRs, the CE hits, the incident reports, those risks, threat force protection type comments are also our second priority.

And then we are working with the department on whether you adjudicate those... because those deferred PRs are clean to then with little to no risk. The good news is if you are deferred adjudication, you are still in the inventory, but you are enrolled into CE. If those hits come back in on those personnel or the hits that come out of CE, those are adjudicated. I think to date there's been far less than 1% of the people enrolled in CE... who have had a CE hit on them. But those are coming as well as if you request a final determination, the CAF is ready to accept your CSRs and make those final determinations. I just wanted to clarify that If you really look at the CAF full inventory, they're somewhere in the neighborhood of 78,000, but they're working through them at a fast clip.

And as the investigative workload stabilizes somewhere south of 267,000 cases, there's more gains made on the adjudicative working of the backlog. I think it's also noteworthy to look at the timeliness. If you look at the T5 initials for DOD industry over the last year, you've gone from 468 days for tier 5s to 295, that's about a 37% decrease. And if you look at the tier threes for industry from 234 days to 181 that's about a 23% reduction in that timeline. So, all good new stories and all trends that are continuing to move in a positive direction. Now we're going to talk about CV, continuous vetting. As we work our way right now today as we were operating under a continuing resolution that 15 days for a rendering of the interims is actually up to about 30 days is what you're seeing today. But we expect that to go right back down to that healthy state of somewhere 15 days or less once we get out of our current CR process.

Mr. Fallon mentioned earlier if you go to that top center block, 1.4 million people in total are enrolled in continuous evaluation in the department of defense. We continue on our trajectory to get to 3.6 million people. Those cleared affiliate with the department probably by late next year. Of those that are enrolled, 380,000 are from industry. If you look back at the last time, we met at the NISPPAC, it was about 350,000 industry folks enrolled in CE. So, you can see there's about 30,000 since then. If you look at the guideline trends on the top right, you can see the big hit there is financial and about 55% of the hits are finance.

Criminal conduct is a distant second, at about 26%, and then a close third and fourth are alcohol and drug issues. Again, as mentioned earlier, industry is about 27%. That 308,000 is about 27% of the workforce. Differed PRs, the

differed PRs I'm talking now are those PRs that Ms. Green and her team has looked at the submission point and whether they looked at them and they've made that risk based assessment based upon the file on the SF 86 that this person can have a differed date, about 55,000, 54,000 in change cases, industry cases that had been deferred.

And then continuing in a clockwise motion, the hit rate coming out of continuous evaluation was about a 6% hit rate, that's in triage and worked by the VROC and then they determine what cases are really adjudicative relevant and need to go over to the DOD CAF for that adjudication. The 2% number you see there the traditional reporting incident reporting coming up from the field. Traditionally we received about 2% reporting rate. With CE we're actually seen about a 6% reporting rate coming out of CE. There is some good things going on in there as we work as the nation's gatekeeper. I'm subject to your questions now. I know we have to be respectful of your time.

Greg: For clarity, I think I'm finally understanding it now. We really have two things with deferrals, because I've heard the term delayed use in the past, but you didn't use it and that's fine. There's different PRs, the 55K where the PR itself was not done and the decision was made. That's great. And then there's deferred PR adjudications where the PR was done but the adjudication has not been...

Ned: Correct, because again, those are assessed-- when we looked at the statistics and we saw that those case types in past years, none of those were revoked. Those are low to no risk. Most of those, if we had been deferring PRs to the submission point actually probably it would have been deferred by Ms. Green and her team and never investigated. But these are the ones that were in process and floated into the CAF. So, as we look at that risk managed approach, we're focusing on getting people to work by prioritized initial adjudications and also be working those cases that actually do have risk in them. CE hits incident reports and the derogatory PRs. So, if a person is a deferred adjudication, know that that person is CE, they retain eligibility and there's little to no risk in that case.

Greg: One other finer point of granularity if you couldn't add or if someone else... so the seven criteria that we have on the second slide, that are a part of the CE process ECV; terrorism, foreign travel, suspicious financial activity, criminal activity, credit, public records and eligibility. Just for a point of clarification so that everyone knows, I think I understand it now. Heather, I think you briefed it at our working group. I could be getting this wrong, but in the intelligence community for scattered castles folks that are enrolled, there's a couple of other databases that they look at that comprise seven or

how they validate those seven, is that correct? Can someone give Heather a--

Ned: Let me take first block and if you want to migrate towards a microphone. There're two programs, there's the DOD program and there's the DNI program and we are collaborating with DNI to work with against the solution. If someone is enrolled in and as Mr. Fallon pointed out earlier today with the release of DISS 9.0, I think it was actually a couple of weeks ago, anybody that's deferred SEAD at the submission point Marianne and her team, it is recorded in DISS that they were deferred and they're in CE, why they were deferred and the date. By January, we would expect to have that same recommendation to be reflected both in scattered castles and into CVS. As we enroll people, if any of our folks were rolled up into the DNI CES program, they were already reflected in scatter castles. Heather, anything to add?

Heather Green: No, I think you covered it. Basically, all the deferred periodic reinvestigations at this point in time for industry are enrolled in all seven DNI data category, CE data categories. Therefore, the reciprocity was in compliance with the seed and the reciprocity memo that was recently released.

Greg: Okay, good up. Kathy, I hope you had a question.

Katherine: Hi, Katherine Kaohi, industry. I actually have two questions for you. On your slide that's flowing right now, you show a 15-day timeline for the interim security clearance determination, when does that 15-day start?

Ned: That 15 days starts at the receipt of the case at the VROC. Is that correct Heather?

Heather Green: Yeah. There're the initiation days and then the interim determination days. We have to remember that the initiation days are shared with the FSO out there from an entry perspective. When you saw the previous numbers, you saw those initiation days. And again, when the FSO has it and they're reviewing it for accuracy and completeness, that initiation days counts both, but the 15 days is the date that we receive it. And then as we wait for the fingerprint result and then as we're able to review for an interim and we're releasing it for an investigation. The last fiscal year and fiscal year 19 we were averaging 15 days. At the end of the fiscal year, it was definitely a very good news story because we were able to execute.

We were fully funded from a PSI perspective and were able to execute down to the dollar and we were pretty much, as initials were coming in, we were pushing them out and you saw those interims happening very quickly, as quickly as we had the fingerprint results to do the analysis. At this point we

are at about 30 days on average. Once the continuing resolution has hopefully worked its way through the process then we will have our full allocation of funding and we'll be able to get back on track to that average of 15-day interim termination from the date that we receive it. We can't control which we can talk about it offline, but we can't necessarily control how long the FSO is holding that case to be released out.

Katherine: The second question is on the risk management portion of your slide. The slide says that one to two days for adverse information triage. I'm assuming that means when we submit the incident report for you guys to take a look at them and get back with this. How long does it take to get the red out? What's the current statistic on that?

Heather Green: That crosses both lanes here. Obviously when we receive the incident reports, we triage it within one to two days. If we are triaging at a medium or high level that's where an additional investigation might be needed and therefore an additional adjudication. So, some of those timelines are pending based on how long it takes for the investigation and adjudication to be completed.

Female Speaker: Absolutely, I mean it's widely varying, and it depends situationally on each individual's situation in terms of what history they have, what the incident is, how severe it is, whether we can collect that information from the subject, or we need to go out to for another targeted investigation. I'd love to give you a specific timeframe, but it's widely variant.

Katherine: Is there a cutoff point? Say if they've been red for 180 days, should we be reaching out to see, is something wrong or is it just it's just totally subjective and we just sit and wait?

Female Speaker: No, I mean certainly if it's been a lengthy time, let's just say 90 to 120 days or more, reach out to us and let us know that you're asking for a status and we'll check into the case and see what's going on with that and we'll give you the information we can.

Katherine: Perfect. Thank you.

Greg: Any other questions?

Female Speaker: We have on the chat from Lindy Kaiser. What is being credited for the dramatic reduction in processing time?

Greg: I'm sorry, could you speak to that?

Female Speaker: What is being credited for the dramatic reduction in processing time?

Greg: What's being credited for the dramatic decrease in processing time? What is the reason for that?

Ned: That's a multifaceted response. Clearly on the investigative side, and Donna, if I missed something, let me know, is mission focus, working some efficiencies trying to leverage IT and capabilities as well as an increase in the investigative workforce out there in the field. When you look at the CAF side of the house, I would say it's firstly they laid it on a single system DISS. They worked through and improved so many initial problems with DISS. There's been an additional bump up in e-adjudication all the time and Marianne and the team have done a great job in identifying additional efficiencies... work through the cases more efficiently once they've landed on that single system. Heather and the team are just kicking it out of the park here when it comes to CV and enrolling people. We're increasing the size of the VROC in order to match that requirements. And so, but I also think it's really the leadership of the teams there, whether it was NBIB and now the DCSA investigators, VROC and the CAF have all had a great impact on...

Female Speaker: Hi, I have a quick question. You said by January you're hoping that there'll be the CE will be in CVS, right? That's what you said. Which tab will that be in in CVS? Is there a tab that's going into or...?

Greg: I'm going to have to look at Heather. Do you know, Heather? Which Tab of CVS?

Heather Sims: I don't know the tab...

Female Speaker: Because the main reason I asked that question is to just ask one question. Right now, because we're a non-DOD agency, we have to go through CVS, if there's a whatever connection to JPAS, its stinks lately. Like five of the past seven days, it has been down. We can't get in there. Companies can get into JPAS, but we can't get into our little feed to be able to verify a clearance from CVS. It's just a... I'm just wondering why? Does anyone realize that and is anybody working on that to try and help us in that regard. Because it's caused a lot of problems for a lot of switchovers of contracts and stuff. We're trying to verify clearances and we can't do it because of the problems with that.

Ned: I can't speak to that last part. We can get the answer back to the, which tab is going to go into CVS, and I'll ask Dr. Barbara to take that. In reference to problems you've been having lately, I can't speak to that. Anybody?

Female Speaker: Is that yours though? Under you guys now or?

Female Speaker: Yes, the feed we get through CVS, which is the only way we can verify a clearance at this point in time.

Heather Green: Right, so we're certainly aware of the issues in JPAS and some recent outages that are occurring. I know that DCSA is working very closely with DNDC to ensure that we can resolve that.

Female Speaker: While that's out, you can always call the DOD CAF calls in order for us to process the verification.

Female Speaker: Well, this isn't really for us to process. This is, we verify clearances for the VARs that we get from companies and stuff. It's thousands in a month. You don't want that many phone calls.

Male Speaker: Yeah, just a curious question. So, metrics, the alert rate is 6%, so you have 6% of those enrolled in CE where there are alerts in the various categories. Are there any metrics in terms of those alerts, how many ends up requiring field investigations? In other words, the human being talking to another human being to solve an issue and also how many of those cases result in access?

Ned: Yeah. Your curiosity is clearly getting down into some further detail there. I can say, and I'm going to look to Heather, is that 6% there, that's what's going to the V-ROC and they're processing. They have the capability to triage them and say, this is not, this is already in the record. It doesn't need any further treatment. Or they can go out and do an RFI to resolve the issues or it might require an RSI to the investigative side of the house to **[2:16:42 inaudible]**. And then the minority of that 6% are then transferred over to the CAF after being identified as adjudicatively relevant and CAF will take that RSI and RFI and make the determinations. Heather, can you speak to any further details on that?

Heather Green: No, I mean I think you covered it. The key thing in that 6% that you just mentioned is that some of those are previously known, and that that's the key. We were looking at that comparison that of the about 840,000 of the cleared industry population we receive, about 2% of that population we receive an incident report on. And then that's actually a positive thing, right? Because when we get the CE alert, we can look back and see it's previously known. No additional action needs to be taken because it's already gone through the process.

Ned: Yeah. And then not really answering your specific questions, but if you look at ballpark numbers, historically, maybe 3% of the investigations and issues resolved result in SOR and less than 1% actually get to the final denial or revocation. So, you're playing in that level of the ballpark in that part of the ballpark. It's a...

Greg: Any other questions? Okay, Caroline, good.

Ned: Thank you very much.

Greg: Thank you. Mr. Perry Russell-Hunter, you're up and I'm sure you'll have something to say about revocations and suspensions perhaps from the DOHA perspective.

Perry: I want to start out by saying that I have very good news from DOHA, which is that our workload is very much within normal limits. Right now, the number of statements of reasons that are with us for legal review is 224. And our norm is at or around 250 a month. So, there is no processing delay in our legal review, the statement of reasons we're getting from the CAF. But I have other good news in that area, which is that thanks to Mariana Martineau and her team, we've been able to work out a memorandum of agreement that we'll be signing shortly that will allow for Doha to directly issue the statements of reasons. We'll actually be going back to something that was true for industry prior to October of 2012. And so we will have in the last now eight years since the CAF consolidation was first being actively worked they captured the efficiencies of CAF consolidation, but then also come back to an efficiency because while there is no delay with the legal reviews, by moving the issuance to Doha, it enables the calf to move those issue cases directly to us and for us to be able to directly issue the SOR. Look for that to be happening in 2020. That is another good news story.

DOHA is not a part of DCSA. We are a part of the office of general counsel because we provide independent review of the investigative and adjudicative work. And so, we are understandably in a different organization, but our cooperation has enabled us to make the most of opportunities like this. I want to thank the CAF for their work toward that process improvement. I also want to just briefly say that we have less than 400 cases in the remainder of due process which means that there's no backlog at any stage in DOHA. Now I have said at previous NISPPAC meetings that I don't necessarily expect that to continue because of the looming investigative and adjudicative backlog. Because those are coming down and because they're coming down into deferral, that's also good news for us because it means that we'll really only be getting cases the cases we're supposed to be getting which are the cases that have to be denials and revocations.

I'm glad that you've left Ned's second slide up here because this has some other very good news in it. In addition to the excellent work that DBD and DCSA and the CAF has been doing to reduce these backlogs, we're also seeing some CE numbers which are I'll say very reassuring. You've heard me say before that the advantage of CE is that we're all looking for the same needles in the haystack, but CE helps us get to those needles sooner. But the only way that CE really is a success is if it doesn't also make the haystack

bigger. The value here is in seeing that we've got a CE alert rate of 6% and so to the question that was just asked about what's within that, I think Heather's answer is very reassuring which is that there's going to be some duplication with information we have and also some of the alerts are either false positives or things that are not adjudicatively significant. When we get down to that, that percent that Ned was talking about, so far, we have not seen CE leading to an inordinate number of cases coming to due process. So that's very good news as well. We're keeping everybody safe by having a quicker opportunity to get to the information, but it's not necessarily creating more cases in due process; at least yet that we've seen.

I also wanted to note that there are a couple of other statistics that are important up here. One of them is that in the deferred cases, and I think this was stated early, it's about 1% that are actually CE hits within the deferred cases. That's also very reassuring because it means that those cases are as clean as we thought they were. So that's very good news. The other thing that you see up here, and it's not a surprise, is that over 50% of the CE hits are in the financial area. That's really been kind of true since 1995 because you remember it was in 1995 that we first started pulling credit reports on all clearance applicants in the wake of the revelations of the Aldrich Ames's case. And that was executive order 12968 that authorized that. We've now got an almost quarter century arc of pulling credit reports. We know that this is going to be the low hanging fruit of anything that we pull in because credit reports will show and then we have to get to the bottom of it. And so, the other thing that I want to reassure you about is that while that number may look high the real thing that matters in a financial case is the why.

It's not so much the amount of debt. It's really how did the person get there and what are they doing about it. The most common mitigating condition used in the new adjudicative guideline is a seed for the security executive agent directive four, which is the adjudicative guidelines that were implemented in June of 2017. But it continues mitigating condition that's been in use for a while. And that is that circumstances are beyond the person's control and they've acted responsibly under those circumstances. Once we've applied that analysis, either at the CAF or later in due process, there's a substantial number of those that are getting favorably resolved as they should be. Just to finally close out one of the other reforms of the seed for guidelines was that we were no longer collecting people's foreign passports because now what really matters is that if you have a foreign passport, you tell us about it.

The reason I mentioned this is because I'm still hearing a lot of urban legends or basically false premises, which is that you can't get a clearance if you have a foreign passport. That is no longer true. You just have to tell us about it and make sure you use your US passport to enter and leave the

country. Dual citizenship is not disqualifying. And by the way, here's a hint. It never was but it's still a thing that I hear a lot. And then finally, the idea that a foreign relative, including in-laws are per se disqualifying. They're not. It's really an analysis of the heightened risk caused by that relationship, which is not going to be simple. This is not something that people should be trying at home. I passed that along for what it's worth. And then finally close with my thanks to the NISPPAC and industry because you all ask great questions and keep those cards and letters and questions coming because a lot of the issues that I deal with on a regular basis are not actually issues it turns out. It's just... thinks they are. Watch this space for DOHA issuing SORs to industry in 2020 and continuing to work hand in hand with the CAF and DVD on other process reforms. Thank you very much.

Greg: Thank you. Any questions for Mr. Perry Russell-Hunter? In the room, on the phone, WebEx? Okay.

Perry: Thank you very much.

Greg: Appreciate it. We are at the near end of this. This is the open forum, general open forum session. It's the opportunity for anyone who is here, on the phone, WebEx to raise a question or comment or concern. Anyone? Carolina, phone, WebEx? No. Okay. Alright, well, now we're at the closing. Our next meeting is Thursday, March 26th, and that will be right here. I'd give you the meeting date after that, but we are unable to get that from the archives more than six months out or thereabouts. We'll have that date sometime around January because we're aiming for July, which is what we typically do for the second meeting of the New Year. Once we get that date, we will let you know. It will be here. That's the plan anyway. And as I mentioned at the beginning of the meeting, the federal register notices go out about 30 days prior to the meeting. Carolina.

Greg: Okay.

Female Speaker: Marc Brooks, are you on the line?

Greg: Mark?

Marc Brooks: Yes, I'm still here. Just very briefly. Marc Brooks, department of energy, just one, affirm. Great meeting, great status updates. Just three quick things regarding going back to a point you raised earlier, Greg, reciprocity of foci analysis. I think one of the things is going to be important to underscore that at the current national level policy and guidance, there is no minimum standards for foci analysis. I definitely want to acknowledge that and that's something that we're going to have to address in order to have reciprocity of foci like we enjoy for personal security investigations and adjudications.

Also, our good colleagues at DOD I believe it was Mr. Reed, talked about the critical technology list. I was wanting as they work through getting a FOUO releasable version, can we capture item under NISPPAC to make that shareable so we're all covering down in terms of protection and risk management on the same technologies that might be shared in terms of research and development or applied R&E efforts.

And then just the last one regarding systems, I believe Mr. Fallon noted for DCSA, he went through a litany, a myriad of systems. One of the things that's come up in terms of DOE is to make sure as we move out on facility clearance or entity eligibility determinations as a foci, that there was a national level system and I believe DCSA is going to have that repository. I'm not sure if it's in this or not to where the interagency could have access so we're sharing information and we don't duplicate work. Thank you,

Greg: Marc. All three are excellent points. I agree on all three. Certainly, the foci analysis, we got to tackle that from the policy perspective. The FOUO release, I have Jeff Spinnanger here sitting to my right. He acknowledges that something we should be able to do on that critical technology protection list at the FOUO level, get it out to the NISPPAC members. The third point more for DCSA to speak to the NID, but at national level system as far as entity eligibility, data, that makes sense to me. Is there anyone from DCSA or USDI who want to say anything about that? Is there agreement on that point that's...?

Keith: Greg, this Keith Minard. I think we have to look broader when we talk about sharing. It's not singular directional. If we need to talk sharing from a NISPPAC perspective, we should talk about sharing cross the CSAs, not independently from DCSA to others, but how do we make that work in a bigger process?

Marc Brooks: Correct, I think Greg and Keith and I won't belabor, it's lunchtime, that a central repository or way to import or share information is going to be helpful. We at DOE we get beat up quite a bit because a lot of the reciprocity requests in regards to facility clearance or entity eligibility determination is DOD issue facility clearances. So, we need to see it in order to grant reciprocity, not to duplicate efforts to include foci and other mitigation instruments. And the last part on this, just a comment, I appreciate the leadership of the ISOO director to request that and we're going to continue to NID working group. We need specific data in terms of which cognitive security agency or cognitive security office or controlling agency, where there's a continued lag in the system. I think with the revision of 32 CFR 2004 effective May 2018, I think the CSAs have made tremendous progress and it would be helpful to get that level of fidelity or detail to understand where bottlenecks continue to ensue. Thank you.

Greg: Okay. Thank you, Mark. We'll take some of this offline at our working group meeting. Anyone else? Carolina, phone, web? Okay. Robert, you give me the signal that we're toward the end here. Unless there's any other comment, statements, I want to thank everyone for attending and for your participation. The model is to continue to work together with our industry partners. We're stronger together than we are singularly. Have a great rest of the day.

Moderator: And that completes our conference. Thank you for using AT&T event conferencing enhanced. You may now disconnect.

[END OF TRANSCRIPT]