NATIONAL ARCHIVES

ISOO INFORMATION SECURITY OVERSIGHT OFFICE

Transcript of the 74th Meeting of the National Industrial Security Program Policy Advisory Committee (NISPPAC) May 28, 2025

Michael Thomas, ISOO: We are here in the beautiful McGowan Theatre at the National Archives and I am Michael Thomas, the Director of the Information Security Oversight Office (ISOO). Relatively recently arrived here, but not my first stint at the National Archives. I first worked here when I was 19 years old pulling documents from the stacks. I have made a long circuitous route back as of this past November to join the Information Security Oversight Office and to join all of you.

I want to welcome you to the 74th public meeting of the National Industrial Security Program Policy Advisory Committee (NISPPAC) and we are absolutely delighted to be able to host many of you in person as well as the folks that are joining us online. I am painfully aware that the DC commute is not trivial, so I appreciate you making the time to be here with us. I want to thank our team here at ISOO as well as the wider National Archives who have worked diligently over many weeks to ensure that today's meeting is a success.

Now, speaking of meetings, over the last few months, since assuming my duties here at ISOO, I have had the opportunity to meet many of you and to listen and to learn as you have generously, sincerely, and often eloquently talked to me about the role you play in supporting our national security mission. Time and time again over the course of our history, the United States has turned to the commercial sector to help us negotiate the dangerous chasms that often emerge between our current capabilities and the conflicts that we can't avoid. Time and time again we bridge these hazards via partnership with Industry. This is a relationship that goes back quite a long way, maybe longer than some of you might think. It has its origins in our nation's founding moments.

Can I tell you a story? Do we have time? We probably don't have time, but I'm telling you a story anyways. Well this story, and stop me if you've heard this one, it starts in the balmy summer of 1776 in Philadelphia. The American colonies had declared their independence and they went to war with Great Britain. It's the National Archives. You knew a history lesson was coming right? It's actually an obligation if you do something in this theatre.

Anyways, the thing is, at the outbreak of the war, our colonial economy was hardly on a war footing. It was basically agricultural, with little to no manufacturing ability. You had small craftsmen and artisans, like the village blacksmith, or maybe our revolutionary friend Paul

Revere, who was a silversmith. But there was really no such thing as manufacturing as we [now] know it. There certainly wasn't any sort of defense apparatus. We had always relied on imports from Great Britain for our arms and armaments. There were maybe 200 people in all of the colonies that knew how to assemble a firearm if they could get the parts. There was only one gunpowder manufacturer in the entire colonies, at Franklin Mill in Pennsylvania. So, what to do when suddenly our biggest military supplier became our most heated adversary? I'll just have you know that 1776 was our first conscious decoupling with the hostile foreign power. So, what do we do?

General Washington, history tells us, sat in stunned silence for half an hour when he was told about the paltry supplies of black powder he could afford to share with his army. Benjamin Franklin was not unserious when he suggested that the Continental Army might be better armed with long bows than long rifles, given the lack of supplies. Domestic manufacturers were simply not postured to keep up with the war's demand while our independence hung by a thread on the success or failure of supplying the Continental Army.

In response to George Washington's pleading, in December 1776, Congress created the Department of the Commissary General of Military Stores. Now, the DCGMS doesn't roll off the tongue quite as well as the NISPPAC, but it was similarly responsible for coordinating the government's relationship with private companies in the development, testing, manufacturing, and acceptance of war material, including material produced outside the government's system. In this moment, I think the defense industrial base (DIB) was born.

Ultimately, through the work of the Commissary General, and with some help from our allies the French, credit where it's due, the colonies were able to provide for its military the arms that it needed to thwart the awesome might of the British crown. That includes providing weapons for a decisive victory at Saratoga, which brought those French allies fully into the fold. It includes repeatedly resupplying our troops in the south so they could keep in the fight. And, maybe most spectacularly, it includes providing the munitions that enabled the Continental Army to continue to engage in the siege at Yorktown. Now, if you know your history, you know that Yorktown is where the British surrendered, effectively ending the war, and ensuring that the American republic would endure- independent. The first republic to be run with the consent of the governed and under the rule of law in the history of the world and it endures to this day.

So, all to say, this relationship between government and the defense industry endures as well, forged in dire necessity in the desperate pursuit of our independence. It not only successfully supported the Continental Army, it not only made us ready when the British came calling again in the War of 1812, it also helped revolutionize manufacturing in our fledgling nation. Things like mass production, integrated supply lines, spreading innovative practices across an economy of emerging manufacturers. The DIB of its day, became a model for how we could produce self-sustaining goods for our own needs, forever linking a strong manufacturing economy to the security of our nation. So this is the legacy that I think we carry forward with us today.

It is with the greatest respect and sincerity that I approach the task that we have before us. ISOO is directly responsible, not just to all of you, but to the President, for maintaining and revitalizing the overall policy framework for the National Industrial Security Program (NISP), ensuring its continued effectiveness and efficiency. But as the late, great American Thomas Early Petty wrote in his classic 2006 solo album *Highway Companion*, “If you don’t run, you rust.” We have heard from all quarters over the past few months about the need to address some particularly rusty areas of NISP policy that offer us real opportunities for reform. So in the coming months, that is exactly what we plan to do. ISOO will be lacing up its running shoes, and we are asking you to join us, with the intent to report our collective recommendations to the President, as is ISOO’s formal responsibility under Executive Order 12829. So I look forward to your collaboration and to your support of ISOO as the convening point for the wide range of discussions that we already know are happening. So thank you once again, and let’s get started. I’d like to welcome Jen May to the stage.

Jennifer May, ISOO: Thank you Michael. Before we move into the roll call, I’m going to go over a few reminders for everyone’s situational awareness. Information related to the NISPPAC and its public meetings is available on the ISOO website and the Federal Register. If you’d like to connect to the Public WiFi, it is “A1 Guest”. Most of you saw the screen as you came in. Once you sign in through your device, just click accept. For those that are speaking and presenting that are in-person and that will use the stage, please use the podium for your briefings.

If you are listening through Google Meet, you may need to reset your audio settings to hear and speak. If you have Microsoft Windows 11, sometimes the audio doesn’t quite sync with Google Meet, so you may have to click a few buttons to get there. If you are connecting through the telephone or YouTube, please provide your name to nisppac@nara.gov for appropriate file retention as having attended the meeting. If you require technical assistance, please send an email to nisppac@nara.gov. Please note all audio connections should be muted when not speaking.

For questions if you are calling in on the telephone, please hit *6 to mute and unmute yourself. If you are on the computer, you can unmute yourself, ask questions through the chat, or email your questions and comments to nisppac@nara.gov. There's a theme here: nisppac@nara.gov and someone from our team will take care of you from there.

If you are in the room, please make your way to the microphone on either side of the stage for your questions. For speakers that are on the stage, if you're answering questions, please make sure you move a microphone close to you so everybody can hear you. We do have restrooms outside the theater and a cafe for a meal in case you want it. And in the event of an emergency, please follow members of the public outside. All available meeting materials, including today's agenda and slides, have been posted on the ISOO website and have also been emailed to all the registrants. As a reminder, not all speakers have slides today.

This is a public meeting. As with previous NISPPAC meetings, this meeting will be recorded. This recording along with the minutes will be available within 90 days on the NISPPAC reports on committee activities web page. We are planning on a 10-minute break in the middle of the session.

Lastly, I want to remind the government members of the committee of the requirement to file a financial disclosure report with the National Archives and Records Administration Office of the General Council. This must be completed prior to officially serving on the NISPPAC and then updated and submitted on an annual basis. The same form for financial disclosure that is used throughout the federal government, form 454, satisfies this requirement.

Now we will take attendance from the government agencies. After I say the name of your agency, please state your name so we can properly account for everyone. Once I've gone through all the government agencies, I will then move over to the industry members and then to our individual speakers.

Office of the Director of National Intelligence (ODNI)?

Lisa Perez, ODNI: Lisa Perez, ODNI

Jennifer May, ISOO: Department of Defense (DOD)?

Jeff Spinnanger, DOD: Jeff Spinnanger, DOD

Jennifer May, ISOO: Department of Energy (DOE)?

Jaime Gordon, DOE: Jaime Gordon, Energy.

Jennifer May, ISOO: Nuclear Regulatory Commission (NRC)?

Chris Heilig, NRC: Chris Heilig, NRC.

Jennifer May, ISOO: Department of Homeland Security (DHS)?

Rich Dejausserand, DHS: This is Rich, DHS.

Jennifer May, ISOO: Defense Counterintelligence and Security Agency (DCSA)?

Matthew Roche, DCSA: This is Matthew Roche, DCSA

Jennifer May, ISOO: Central Intelligence Agency (CIA)?

Don, CIA: Don, CIA.

Jennifer May, ISOO: Commerce?

Steve Barbieri, DOC: Steve Barbieri, Commerce.

Jennifer May, ISOO: Department of Justice (DOJ)?

Tanya Fields, DOJ: Tanya Fields, DOJ.

Jennifer May, ISOO: National Aeronautics and Space Agency (NASA)?

Vaughn Simon, NASA: Vaughn Simon, NASA

Jennifer May, ISOO: Thank you. National Security Agency (NSA)?

Blane Vucci, NSA: Blane Vucci, NSA.

Jennifer May, ISOO: Department of State?

Janice Custard, DOS: Janice Custard, Department of State

Jennifer May, ISOO: Thank you. Air Force?

Annie Backhus, Air Force: Annie Backhus

Jennifer May, ISOO: Thank you. Navy?

Andy Jones, Navy: Andy Jones.

Jennifer May, ISOO: Thank you. Army?

James McAlary, Army: James McAlary

Jennifer May, ISOO: Thank you. Next, I will move to our Industry members. Ike Rivers?

Ike Rivers, Industry: Ike Rivers, Industry

Jennifer May, ISOO: Thank you. Greg Sadler.

Greg Sadler, Industry: Present.

Jennifer May, ISOO: Dave Tender?

Dave Tender, Industry: Present.

Jennifer May, ISOO: Jane Dinkel?

Jane Dinkel, Industry: Present.

Jennifer May, ISOO: Chris Stolkey?

Chris Stolkey, Industry: Present.

Jennifer May, ISOO: Kathy Andrews?

Kathy Andrews, Industry: Present.

Jennifer May, ISOO: LaToya Coleman?

LaToya Coleman, Industry: Present.

Jennifer May, ISOO: Charlie Sowell?

Charlie Sowell, Industry: Present.

Jennifer May, ISOO: Thank you. Lastly, the roll call for the speakers. David Cattler?

David Cattler, DCSA: Here.

Jennifer May, ISOO: Tessa Dutko?

Tessa Dutko, ODNI: Here

Jennifer May, ISOO: Monica Marks?

Monica Marks, DOE: Here.

Jennifer May, ISOO: David Scott?

David Scott, DCSA: Here.

Jennifer May, ISOO: Donna McCleod?

Donna McCleod, DCSA: Here.

Jennifer May, ISOO: Perry Russell-Hunter?

Perry Russell-Hunter, DOHA: Here.

Jennifer May, ISOO: David Means?

David Means, ISOO: Here.

Jennifer May, ISOO: Stacy Bostjanick

Stacy Bostjanick, DOD: Here.

Jennifer May, ISOO: If anyone else is speaking at the NISPPAC that we have not heard from or that we don't know about, please speak now. As a reminder, we request that everyone identify themselves by name and agency, if applicable, before speaking each time for the record.

We've had a few changes in NISPPAC membership that we're going to share with you right now. Both Natasha Sumter and Tracy Kindle with the Department of Energy have departed. Jamie Gordon is now the primary member with Monica Marks and Theodore Banks as her alternates.

At the National Security Agency, Matt Armstrong's replacement, Della Morrison, retired. Blane Vucci continues as the alternate member. Jason Steinour has replaced Robin Nickel as the alternate with the Department of Navy. Jim McAlary has replaced Elizabeth O'Kane as the primary member of the Army. For those departed members, thank you for your contributions over the years and we look forward to continuing the work that you've done with the new representatives.

The NISPPAC last met on November 13, 2024. The NISPPAC minutes from that last meeting were certified true and correct and were finalized by Michael Thomas on January 24, 2025. They were posted to the ISOO website on February 4, 2025.

The following statements address the action items from that meeting.

The first item of interest is the status of the Executive Branch's Controlled Unclassified Information (CUI) study. The National Security Council (NSC) began to review the classified national security information (CNSI) and the CUI executive orders in 2022. CUI notice 2022-01 is the last formal guidance we provided regarding the status of that process and that program. We are still awaiting further guidance from the new administration's NSC regarding the plans in the information management space as they pertain to CNSI, CUI, and special access programs (SAP). In the meantime, ISOO continues to fulfill its responsibilities under the existing policy framework that governs the CNSI and CUI [programs]. We consider this item closed at this time.

Next, DoD was going to invite the project leads for Cybersecurity Maturity Model Certification (CMMC) from the DoD Chief Information Officer (CIO) to provide a program update at the next public meeting for NISPPAC, which is today. We are going to hear from them today and consider this action item closed unless otherwise notified.

Third, DoD invited Jill Baker to speak at the next public meeting of the NISPPAC on the National Background Investigation System (NBIS). While we don't have Jill Baker briefing today, Jeff Spinnager will be answering any questions about NBIS from a policy perspective.

Additionally, DOD asked ISOO to engage with small business administration regarding a military department's ability to meet small business requirements. This item is still pending with ISOO at this time.

Next, DOD was going to provide an update on the status of the National Industrial Security Program Operating Manual (NISPOM) at the next public meeting. We're going to hear from them today and consider this item closed at this time.

Regarding the Transfer of Reciprocity Information System (TORIS), ODNI will provide a TORIS update at the next public meeting. We're going to hear from them today as well and consider this action item closed unless otherwise notified.

Regarding the Standard Form (SF) 328, which is the certificate pertaining to foreign interests, DCSA agreed to work on guidance for the SF-328 along with timeframes. We're going to hear from them today about that.

DCSA will also provide an update about the SF-328 training roll out and we're going to hear from them about that today as well. We consider both those items closed at this time.

Regarding the personnel vetting questionnaire (PVQ), DCSA agreed to work with Industry to provide a demo of the questionnaire in NBIS to the industry NISPPAC members prior to the public demo in January 2025. We consider this item closed as well.

For the next matter, CIA agreed to provide industry insight into their Foreign Ownership, Control or Influence (FOCI) vetting process. We're going to hear from them today and consider that item closed.

DOE will provide an answer to the question about how often they perform business assessments. We're going to hear from them today and also consider this item closed. Do any NISPPAC members have any questions?

(No questions raised)

Jennifer May: Michael, back over to you.

Michael Thomas, ISOO: Thank you Jen. Moving on to the next item on the agenda. We've made some administrative and operational changes to the NISPPAC bylaws. These revised bylaws were shared with the members ahead of time via email from Heather Harris Pagan on Thursday, May 8th at 10:43 a.m. Today, I'm requesting that we have a formal vote on the changes in the bylaws. If you haven't had a chance to review those changes, we have hard copies here that you may promptly review in advance. Two-thirds of present government members and two-thirds of present industry members need to approve the proposed bylaws for it to be approved. As chairman, do I have a motion to proceed on a vote on the NISPAC bylaws changes?

Ike Rivers, Industry: Yes

Michael Thomas, ISOO: Motion is The motion is made. Thank you. I'll now turn it over to Jen for the voting.

Jennifer May, ISOO: Thank you, Michael. I will now say the name of the agency. Then please respond with your name and a "yes" or "no" to the proposed changes to bylaws. Then I will ask the industry members to vote in the same manner. ODNI?

(ODNI was not present for the vote)

Jennifer May, ISOO: DOD?

Jeff Spinnanger, DOD: Jeff Spinnanger, Yes.

Jennifer May, ISOO: Thank you. DOE?

Jaime Gordon, DOE: Jaime Gordon, Yes.

Jennifer May, ISOO: Thank you. NRC?

Chris Heilig, NRC: Chris Heilig, Yes.

Jennifer May, ISOO: Thank you. DHS?

Rich Dejausserand, DHS: Rich DeJausserand, Yes.

Jennifer May, ISOO: Thank you. DCSA?

Matthew Roche, DCSA: Matthew Roche, Yes.

Jennifer May, ISOO: Thank you. CIA?

Don, CIA: This is Don B. Yes.

Jennifer May, ISOO: Thank you. Commerce?

Steve Barbieri, DOC: This is Steve Barbieri, Yes.

Jennifer May, ISOO: Thank you. DOJ?

Tanya Fields, DOJ: Tanya Fields, Yes.

Jennifer May, ISOO: Thank you. NASA?

Vaughn Simon, NASA: Vaughn Simon, Yes.

Jennifer May, ISOO: Thank you, NSA?

Blane Vucci, NSA: Blane Vucci, Yes.

Jennifer May, ISOO: Thank you. State?

Janice Custard, DOS: Janice Custard, Yes.

Jennifer May, ISOO: Thank you. Air Force?

Annie Backhus, Air Force: Annie Backhus, Yes.

Jennifer May, ISOO: Thank you. Navy?

Andy Jones, Navy: Andy Jones, Yes.

Jennifer May, ISOO: Thank you. Army?

James McAlary, Army: James McAlary, Yes.

Jennifer May, ISOO: I will now address the Industry members. Please state whether you are voting "yes" or "no" to the changes of the bylaws. Ike Rivers?

Ike Rivers, Industry: Ike Rivers, Yes.

Jennifer May, ISOO: Greg Sadler?

Greg Sadler Industry: Yes.

Jennifer May, ISOO: Thank you. Dave Tender?

Dave Tender, Industry: Dave Tender, Yes.

Jennifer May, ISOO: Thank you. Jane Dinkle?

Jane Dinkle Industry: Yes.

Jennifer May, ISOO: Thank you. Chris Stolkey?

Chris Stolkey Industry: Yes.

Jennifer May, ISOO. Thank you. Kathy Andrews?

Kathy Andrews, Industry: Yes.

Jennifer May, ISOO: Thank you. LaToya Coleman?

LaToya Coleman, Industry: Yes.

Jennifer May, ISOO: Thank you. Charlie Sowell?

Charlie Sowell, Industry: Yes.

Jennifer May, ISOO: Thank you. The motion is carried. We will now amend our bylaws accordingly. At this time, we'll now introduce the speakers for our updates. Mr. Isaiah Rivers, the NISPPAC industry spokesperson will provide the industry update. Ike, please come up to the podium.

Ike Rivers, Industry: Good Morning. Mr. Thomas, Jen, and Heather, thank you very very much for always putting this together. Your history actually goes along with just a couple of opening remarks that I have. It was perfect actually. The power of partnership and collaboration between government and Industry solves a lot of things. Really think about it. One can't do without the other. I wrote something down here. I said the power of partnership and collaboration will get you through a lot of tough times and it will help you more than it will hurt you. And that is what the NISPPAC government and Industry is all about with the support of ISOO. So you and I must have been in each other's head, but it was really the watch thing. So you guys don't know, me and Mike, we have this thing about watches and we were both scoping each other's watches out. So I think we started that watch collaboration, but we started that collaboration a long time ago.

I wanted to thank everyone that supported Industry Day last week at the Institute for Defense Analyses (IDA). This event started from a collaboration of government leaders. CSAs like Jeff Spinnager and Mark Frownfelter and DCSA [Director] Mr. Cattler. This was a great idea to do with the Aerospace Industries Association (AIA) and National Defense Industrial Association (NDIA) not being able to host [their conferences] because of federal restrictions and stuff and the collaboration and the partnership that we have formed before that meeting resonated. You can tell because we had 287 attendees. We had 45 different industry companies and we had 22 different government agencies. So I want to give a special thanks to the leadership supporting this event, Mr. Thomas, Ms. May, Ms. Harris Pagan, Mr. Clark, and Mr. Means for actually coming out and spending the whole day supporting us. That really meant a lot to us.

But I want to, before we get to the team, I want to give a quick example about the partnership and collaboration and how it could work and how it has worked. Everybody heard about the NBIS issue that went on a couple of weeks ago and it affected not only industry but it affected government as well. Instead of everybody fussing about it, and if they did fuss, it was behind closed doors on both sides, the parties really worked together to help move some things forward. And yes, there are still some issues, but we were able to work together for many hours just to work on that and make sure that things were right. I do want to commend the leadership of Mr. Quinton Wilkes who is the industry NISPPAC chairperson for the systems working group and his working group team and the DCSA team that worked day and night trying to resolve some of those issues. And again, yes, there are still some of those issues lingering, but without that partnership and without that collaboration, we would not be where we are today. So, I just wanted to just pass that on.

So, these two beautiful individuals that are on the screen. We're having our elections coming up here in August and they have spent the last four years serving the community of industry. I could not go start this meeting without telling Dave Tinder and Greg Sadler, thank you so much. What you mean, not just to the industry NISPPAC team, not just to ISOO, but the whole community protecting the warfighter in this great country. So, I wanted to give Greg Sadler and Dave Tinder a round of applause for their service. [Applause].

Alright so these are our current members. The last meeting we did have we were minus a member. We're glad to welcome Mr. Chris Stolkey from BAE Systems. He's the Chief Security Officer (CSO) at BAE. So Chris is the new member of our team. So welcome aboard Chris.

And we wanted to welcome Christy Wilder, the CSO for Peraton, as she is now the Professional Services Council (PSC) chair.

So we're going to just get into this a little bit and just talk. A lot of these are our industry topics. I'll ask and so I'll start it off and then I will pass it around to some of my teammates. I think Jen you just mentioned CUI. CUI is still a big issue for Industry and we're just trying to figure out who's playing and who's not playing, right? We're affected by it, but nobody is talking about it. So, real simple can we get the Cognizant Security Agencies (CSAs) to the table? Is there a way to get the CSAs and everybody involved at the table to actually talk about CUI and to see what we're doing with CUI? I'm sure Mr. Spinnager will talk a little bit about it, but we'll also have some examples as well moving forward. So, one of our asks is can we get the CSAs to the table to at least have the discussion. One agency said they're not going to do it. That does no good for Industry. So, we just want to know if we can just at least sit down at the table whether we're going to keep going or whether we're not. And once we have direct guidance or something, Industry would love to be at that table after you all have that initial conversation. So that’s one of our asks.

The communication channels, everybody that’s known me for a while knows I'm huge on communication. Again, when it comes to partnership, there should be no way where industry or the government finds out things after the fact, right? It could be bad news. But if you know about the bad news upfront, it lessens the blow. So we are just trying to see if there are other communication vehicles out there that industry can grab some information before they're surprised. And so that's one of the things that we would want to ask from the different agencies and the CSAs out there: where are those communications? Where can we get some better vehicles? If industry NISPPAC can assist in having a sit down to talk about how we can collectively think about ways we can communicate better from industry to government.

Lastly we talk about dollars being spent, extra man hours, and things; reciprocity of training. You have Ike Rivers. He belongs to a couple of government agencies and every agency he goes to he has to do the same training. It's the same exact training. When can we actually have a conversation where we can say “okay your training that you do for DIA is also good for NRO which is also good for CIA or NSA”? That will save a lot of time and effort and it'll put money back in the taxpayers' pockets because they're charging for those hours. This is not free hours. So just wanted to put that out there on the plate too as an ask if we can actually think about that training reciprocity.

Greg, you want to talk a little bit about CUI?

Greg Sadler, Industry: Sure. Regarding CUI, even within the DoD, we're seeing differing guidance on how material should be handled and how it's protected within that process, especially in the Request for Proposal (RFP) space. That's pre-award. There's a lot of intellectual properties brought to bear, then it becomes this magical control channel or handling guidance or pick your flavor of definition there. So, while Ike had highlighted the need for the CSAs at large to get together and hammer some commonality out, within the DoD itself, we could get more tactical and hopefully address that a little faster because we're one big family. So the real ask there is, as a community, can we get together, work through this so we have that commonality and we're a long ways away. One particular group [had] CUI and said “handle as secret.” We haven't seen that in the last 12 months but that extensive or range of guidance needs to be tightened down. The consistency will help us be efficient, which then will return money back to the taxpayer, and/or allow [taxpayer dollars] to be better used writ large. Thank you Ike.

Ike Rivers, Industry: Latoya, you want to just throw out some comments about Sensitive Compartmented Information (SCI) indoctrination authority for industry? This is one that has been on the table for a little while and we want to try to see how we can get this pushed on a little bit.

LaToya Coleman, Industry: Sure. So, as many know, Industry is experiencing delays in getting personnel in program due to the inability to conduct SCI briefings for some of the service departments. The nomination process is also an issue that's kind of tied into that. But that process within itself could be updated to help improve the time and getting personnel on mission. What we have done thus far is the Undersecretary of Defense for Intelligence and Security (OUSD I&S) has included industry into a DSAG meeting and we have had the discussion with the service departments as it pertains to the SCI Indoctrination (Indoc) process and the nomination process or us being able to have more Indoc authority and the nomination process. We are asking OUSD I&S to continue to work with the service agencies to expand the SCI Indoc authority and continue to review that nomination process. In addition, we're asking for additional meetings so that we can work with OUSD I&S and the service departments to come up with a better process moving forward.

Ike Rivers, Industry: Thank you, Latoya. And I meant to say that the ask here falls under the DOD. So, I just wanted to make sure everybody knew that. Chris, you want to have a quick conversation in regards to solid state drives?

Chris Stolkey, Industry: Sure. Solid state drives are a concern for Industry primarily because there's no approved sanitization for solid state drives. This becomes an issue when solid state drives are involved in a spill. It wasn't too long ago that we only saw solid state drives in our mobile devices or laptops. They're everywhere now. They're in our network storage devices. So, a spill that occurs on a network storage device can cost millions to replace and lots of downtime. It's under DOD, but it's bigger than the DOD. Although the DOD, Mr. Spinnager in particular, has been working with us to understand what the problem is and try to find a path forward. If we don't address this, it's much like just sticking your head in the sand. As we expand in the cloud, the cloud servers are all solid state drives. Industry needs a solution that we can work forward with the government on to solve this problem. Thank you.

Ike Rivers, Industry: LaToya, Can we have a conversation with Mr. Spinnager from DOD about how the support that OUSD I&S has been regarding NBIS? You want to chat about that a little bit?

Jeff Spinnanger, DOD: Regarding what?

Ike Rivers, Industry: NBIS.

Jeff Spinnanger, DOD: Sure.

Ike Rivers, Industry: No, Latoya, you want to have that conversation with Mr. Spinnager?

LaToya Coleman, Industry: So what industry is asking as it pertains to NBIS. We all know about the critical challenge that we had maybe a week ago when it came to NBIS and the Identify, Credential, and Access Management (ICAM) deployment. What Industry is looking for is more engagement and more communication. It is Industry's understanding that OUSD I&S has a stake in this process which I'm sure that Mr. Spinnanger will talk more about in his talking points. But what industry is requesting from OUSD I&S is around a conversation that we had last fall with OUSD I&S where OUSD I&S stated that they would have an IRTG in place for industry to provide requirements and feedback. Industry is requesting that we start having those meetings in the next 30 days and recurring until successful deployment of NBIS and any other concurrent system or application going forward. Industry has working groups available and ready to support those efforts and we just need to understand when we can start to engage and start helping build those requirements so we can make future deployments of systems and applications more seamless

Ike Rivers, Industry: Thanks Latoya. Charlie, you have a couple questions regarding Executive Orders (EOs)?

Charlie Sowell, Industry: Yes sir. Thank you. This is Charlie Sowell, Industry member. Since January 20th, President Trump has issued 152 executive orders. The impact on industry from these executive orders; there's common sense understanding of what some of it means, but we're formally requesting that ISOO coordinate with the CSAs to provide industry guidance as soon as possible on the EOs that are relevant to the National Industrial Security Program (NISP). There are several, again, that are, just on their face, common sense impacts on Industry and four months into the administration, we have not received any implementing guidance direction. And we understand that the coordination process in government can take a long time. We get that. But even any interim guidance that could be given would be extremely helpful to our companies. Thanks

Ike Rivers, Industry: Thanks Charlie. We're going to move over now to DCSA. So, these asks are in regards to DCSA. But there was one thing I forgot to mention and I'm glad Director Cattler is here. During that NBIS challenge for government and Industry last week, there were two individuals specifically that were working around the clock with us: Mr. Donnie Lewis and Mr. Mike Fowler. So I wanted to make sure that I passed that along to you. So Latoya, I'm going to pass to you for investigation timeline updates.

LaToya Coleman, Industry: So, Industry NISPPAC has been closely monitoring the uptick in the investigation timelines with DCSA and we understand that DCSA has created a tiger team to mitigate what those timelines are. What Industry is asking is that DCSA address what the findings were from that tiger team. What's being done to address the findings and what should Industry expect going forward to manage the case load.

In addition to that, this is not a DCSA concern, but it's on the ODNI side, I want to address the SCI processing timelines with ODNI and explain the processing timeline. This is from the time of industry submission to the time getting the person in the seat. So what industry is asking, we would like to know what ODNI is doing to help to reduce that timeline and we are asking that ODNI form a working group that includes industry to help reduce that timeline and the numbers going forward.

Ike Rivers, Industry: [LaToya] you want to go ahead and take the PVQ updates?

LaToya Coleman, Industry: I do. One of the things that was mentioned earlier or in a previous meeting as it pertains to the PVQ was the demo. Industry did receive a demo of the PVQ. However, what industry is requesting is that just like with any other system or application or deployment of anything, we're asking that DCSA and OUSD I&S partner with industry in a working group to make sure that we are able to effectively test and pilot the PVQ for a smooth transition.

Ike Rivers, Industry: Alright. Thank you. Greg, Authorizations to Operate (ATOs)?

Greg Sadler:. Thank you. From an ATO perspective, Industry thrives on cost and schedule predictability. So if there is anything with the looming budget changes, the early out within the government structure that may come to bear on the ATO timelines, while ATO is a common piece from a systems perspective, the concern also extends to any government approvals for open storage areas or other aspects to which we may experience some latency. That could be a greener workforce that's executing the mission, that might involve some concerns from a predictability and scheduling perspective. So Industry is really seeking that. Not only from DCSA, but any CSAs across the organization that are involved in that process so that we can improve our predictability which improves our ability to execute on contract.

Ike Rivers, Industry: Jane, I know you have a couple. One is regarding Facility Security Clearance (FCL) timelines and then staff training updates.

Jane Dinkel, Industry: Yes. Good morning. I'm Jane Dinkel with Industry. I chair the entity vetting/FOCI NISPPAC working group.We work closely with the DCSA, and specifically Matthew Kitzman, regarding entity vetting. We appreciate the partnership with DCSA and their data collection of the facility clearance life cycle. We would ask DCSA to break down the facility clearance life cycle and identify timeline goals for each stage of the facility clearance life cycle. What are the goals for each stage in the life cycle? What is the recourse if DCSA does not meet those goals?

And additionally we met with the DCSA entity vetting office in January up in Quantico and we, Industry, provided facility orientation handbook updates and edits for consideration with DCSA. We've not seen any of those edits be implemented. So, we'd ask the status of the update for the facility clearance orientation handbook and when Industry might get that as a final product.

I'd also like to address the staff training update regarding inconsistencies across the field. I continue to hear that some field representatives identify recommendations and observations during security reviews as if they are requirements. What should be the implication if a recommendation or observation identified during a security review is not implemented. There should be an understanding that those are not requirements. They might be best practices or good to haves, but they're not requirements and should not have an impact on the security review process.

Additionally, when the field calls the knowledge center, in many cases, depending on who they speak to, they'll get a different answer to the questions they ask. Those answers should be consistent. So industry would ask DCSA to address the training of the knowledge center staff to ensure that they all have a clear understanding of the processes and are able to give consistent answers to industry. Thank you.

Ike Rivers, Industry: Thanks Jane. And now the last one, ODNI. LaToya will talk about a couple of policy updates that we're looking for. Over to you, LaToya.

LaToya Coleman, Industry: For ODNI, the covered insider threat information sharing policy update. We would like to know where we are with that. We know that there are quite a few policies that have been, for lack of a better word, frozen, as we work with the new administration. So we would like to understand where we are with that covered insider threat information sharing policy.

In addition, the overhead billets policy. Mark Frownfelter cited last week at the industry NISPPAC day that [the overhead billet] policy is back with legal for review before sending it back out for agency coordination. So we would like to understand what that process is going to look like and what is the timeline as it pertains to that policy moving forward into fruition. It's been quite a while.

The Transfer of Reciprocity Information System (TORIS) update. I think that was mentioned earlier that we will be getting an update on TORIS. So I will yield my time back to Ike.

Ike Rivers, Industry: I'm going to let Ms. Kathy Andrews come and have the podium. She's going to give a physical security working group update because the physical security working group was the latest working group that we added to the Industry NISPPAC team and there's been a few things that have happened since the last time we had a public meeting. So, I'm going to just turn this over to you.

Kathy Andrews, Industry: Thanks Ike. Good morning everybody. I wanted to share with you some updates we've had since our last meeting on the 22nd of January. We've had quite a few positive things. We've had multiple ODNI/NCSC working group meetings, data center working group [meetings] as well as the IC industrial security representatives meeting. Industry has been reinstated to attend the Physical and Technical Security Working Group (PTSWG) which is very important for us. We've got a very strong collaboration with the IC and we feel that most of the questions and concerns that we have are moving forward through that organization. We continue to have monthly NISPPAC working group meetings to solicit from industry those major concerns that we have so that we can collectively put those together and present those to the government. Companies are also very busy putting together the Plan of Action and Milestones (POAMs) for each of their high-risk areas. So that represents the main things that have happened since January.

Industry's key concerns or asks is that we continue to see a misalignment or separate dates and guidance from the individual agencies. So again, we feel like we're getting very clear guidance from the IC. We could really use some guidance from the services specifically about the Special Access Program Facilities (SAP-Fs). That seems to be where most of the pain points right now in Industry are coming from. And so we'd like to try and get some clear guidance from the services on expected timelines for POAMs, compliance, and other milestones. We'd like to continue to see the risk-based approach to modifications to current facilities which is the biggest challenge for industry at this time. We also are hearing that there is a lack of response to POAMs that are delivered and I know in a lot of areas they aren't due until the end of December. But as we've previously mentioned, for Industry to control costs and to be able to predict financially, which is important to our C-suite, we need to make sure that these POAMs and our recommendations for them are responded to. We have had some contractors or some industry members have visits by the government but the results of those visits have not been provided and those are very important for companies to move forward with the request from their companies for capital as well as to start the modification and build process. So responses to those are very important for us.

We have a continuing concern regarding reciprocity across the government. I know that's a very big challenge.I know all of us are trying to get to one place when it comes to compliance. But for us to understand and have a means to arbitrate reciprocity challenges will greatly make things easier for industry and government and allow us to share very costly facilities across the board.

And last but certainly not least, we ask the government to consider innovative alternatives to achieve the TEMPEST certification. There are many [innovative alternatives] that Industry is very willing to present as options.

The big one right now is the approval for self- testing by Industry due to the shortage of Certified TEMPEST Technical Authorities (CTTAs) in the government. And that those tests by the companies, done by CTTA professionals, would be accepted in lieu of a government certification test. So that is just one. So thank you very much.

Ike Rivers, Industry: Thanks Kathy. This is our portion, but I have to say, Chris, Charlie, LaToya, Greg, Jane, Kathy, and Dave, they do a tremendous job, right? This is not their real job. They're leaders in this industry at the very senior level, and then they find time to do this for Industry. It's extremely important for us because Industry, just like government, have to have that voice that's going to be out there to fight. That's going to be out there to help do whatever needs to be done to protect that warfighter in our great country. So a lot of great information. The asks that we have is that you really consider the things that we've talked about and just remember that power of partnership and collaboration. And if you need anything from us, some additional questions, we are here, day and night to answer any of those questions you may have. Mr. Thomas, thank you very much for allowing us to have this particular time to talk to NISPPAC community about our issues and our asks. Thank you.

Michael Thomas, ISOO: Any questions from the members for Ike or Industry? For those participating remotely, in the interest of time, we will reserve questions so please email nisppac@nara.gov to make sure that we enter them into the record. Any immediate questions?

(No questions from NISPPAC members)

Michael Thomas, ISOO: Ok Jen, over to you.

Jennifer May, ISOO: Thank you Ike and team. Next we have Mr. Jeffrey Spinnager, the Director of the Information Acquisition Protection Directorate for the Office of the Undersecretary of Defense for Intelligence and Security, who will give an update on behalf of DOD as the NISP Executive Agent.

Jeffrey Spinnanger, DOD: Good morning. So I realize I have 20 minutes, so I have 40 minutes of remarks. Just in keeping with expectations. But first and foremost, thank you to the ISOO team. 2019, it seems like a long time ago and sitting here for the first time since then, it reminds us just how long and much time there has been and it is really great to be here. These meetings are very very important. The opportunity, the collaboration, just the few minutes of conversations that happen before we go on the record. Those questions that come up while we are on the record. God knows what will happen when we get some coffee. But it is really great. These are things that we just cannot do when we're off camera or even on, so thanks very much. I know it's a herculean effort. I did confirm that Heather went home for at least a little while last night. So thank you very much for that.

Also, beforehand, to Greg and Dave, on behalf of the department, I think I'm allowed to say that, thank you very much. You've been fantastic partners to us. You're candid when you need to, you’re gracious always, well mostly, but you say what needs to be said. You put in the time and we are all better for it. For those who come next, and this has been kind of a continuing theme. I've been doing this for a minute now. They're very very important and so for those that come back and those are come next and those who are going to remain here the partnership is very very important and so I would like to echo what Ike said up front to that.

There's one more departing person, she was only here one time, but Jen, I know you're not going to be here much longer, but thank you very much. We've had some opportunities to meet. One of the first in-person meetings I had here back at ISOO you was with you. I was glad for that. So whatever comes next don't be a stranger. Thank you very much. With that I'll jump in.

Building on what I talked about. It was great that we were able to meet last week at the NISPPAC Industry Day and again testament to the folks at this table and a handful of others for stepping up and filling what is an absolutely essential void and a pathway to that partnership that Ike spoke so well about. My boss, John Dixon, was one of the speakers last week and you heard him say how we will support and advance the secretary's directive to revive the industrial base and to rapidly field emerging technologies. Today I'm just going to continue to basically echo his message. That feels like a really safe career move. But more than that because it's fundamental. Communication is paramount to that partnership. Being able to say what needs to be said and when it needs to be said. And so, although I'm gonna bat out of order, I just think it's appropriate. With NBIS, there's lots of examination of the challenge areas, the technical challenges that all are experiencing right now. I'm not the guy to talk about that. I'm happy to write down any of those questions, but I do want to spend maybe just a brief moment to talk about what did work. And what worked was some leadership and some outreach.

So when the problem was first teed up and contemplated, the first thing that a couple of folks in this room did, Ike and Quinn, is they picked up the phone and they started making phone calls. They could tell you how many phone calls they made. I can tell you that they did call me. They called Jill Baker, and the telephone tree that ensued from that. And so while the opportunity to examine the pitfalls and the challenges of a very complex series of software that has to work in an incredibly complex and dynamic threat environment is no small thing. The fact of the matter is that when there's a contingency, and I suspect there will be again, the ability to know that you have people who are going to pick up the phone and make those phone calls right that's foundational.

Certainly, we want to be in front of the information curve as best as we possibly can and I think everybody in this room and those who are out there, I think we all agree on that. But the fact that we can see it in practice is no small thing and I don't want to lose that in the examinations. I did something I generally don't do. I went and looked online for some of the feedback on this yesterday. I won't do that again. That's noise, right? That's not communication, right? This forum, others like it, the phone calls that happen, that's what real communications are. And again, there's names have been mentioned a few times, but to Quinton and Ike for picking up the phone and alerting us to an issue so we could be productive, not just reactive, I think we're all on a better footing as we address this present issue and all the issues that are to come. Thank you for that.

But one of the things that John said, we've got a lot of policy work to do. We talk about that a lot. I put a few of them up on this slide because Heather bet me that I wouldn't have a slide. But the priorities for us right now, we're very proud, and I think those of you who've been here for a while, we should be. The fact that we have a reg for the NISPOM. I've said to predominantly Industry facing audiences before and I will continue to say again the importance of that regulation is less about industry and much more about trying to corral the complex organism that is the federal government around a common set of requirements; That consistency. We've heard it from many other speakers already this morning. That is absolutely essential. It's also another pathway to that communication so that we have a common thread and theme to build from. But one thing that John said is framed around a powerful concept and he gave me some credit for it and that's kind of funny because I was just writing down what I heard him say and that is that threat informs standards, standards inform posture, posture informs compliance, and compliance informs risk management. I'm not afraid of the word compliance. Too much of one thing creates friction on the other. But it is a bit of a cycle that we cannot avoid. But it's not just a cycle. It is a mindset. It's about translating intelligence on our adversaries into enforceable, measurable, and mission aligned security practices. So again, with sincere thanks to our ISOO host, I want to highlight today a bit how we're operationalizing that concept through upcoming updates and initiatives.

Secretary Hegseth has emphasized that speed and competition are now essential elements of military strength. And to keep pace, the defense industrial base and the defense acquisition system must adopt a truly threat informed security posture, one that's interoperable, cyber resilient, and acquisition aware. To that end, we are preparing targeted policy updates. We've been in the policy update business for more than a minute now. Mostly internal here, right? It's the internals that we're really focusing on; the DOD manual. I was pleased to be invited to DCSA to speak at their recent signatories engagement where we remind all the signatories that they do follow DOD policy as part of the price of admission. And those policies that we can point to, they're out of date, and that's sand in the gears. That's everybody's gears. We understand that.

So we are focused around a lot of information security policy updates. We don't want to get out of phase. We anticipate at some point that the administration will pick up some of the great work that was being done in this space that dates back to the first time this administration was here. It's a long and arduous federal process. We've been guided by that. We don't want to be stuck in a place where we're waiting for it because policy processes are slow. If we're going to try to align them up, then whoever the youngest person in here is, when you're sitting up here, then you'll maybe get it done. And that's not going to get what any of us need from a policy work perspective.

But more importantly, we are facing great power competition in ways that I don't think any of us thought we would. Even in the recent past. So that's kind of where we are. That's about improving consistency, reducing redundant or stove pipe requirements that slow execution and accomplishment in accordance with what the secretary has laid out so directly. Let me just say upfront, and all of his immediate predecessors dating back probably 10 or more years have said words to the same basic effect, but let's be honest, the framework of the National Industrial Security Program hasn't fundamentally changed in over 30 years. But almost everything else has. Our adversaries, our technologies, and the demands of our industrial partners. But while it took more than 26 years, the NISPOM as a federal rule shows that the baseline requirements are foundational. They don't tend to change very much. What changes is the implementation of that, which again is a clarion call for the policy reforms that we in the department are undertaking with full recognition of the outsized effect that has on the broader program. We need security at the speed and scale of mission. Some important context; words that you will not find in any NISP policy: cybersecurity, cloud, solid state drive, SAP-F, SCIF, network, supply chain. I was going to add reciprocity, but I think it might be in there.

So, those words aren't here. They don't need to be here, right? The limitations and challenges that we experience in every one of these things is created within the framework of the existing policy requirements. Said differently, I hope that we undertake those broader executive level reforms. We put a lot of time into it. I really do hope that the CUI EO comes out, the work that we did on the CNSI executive order and when it becomes appropriate that we pick up and do the same thing for the NISP EO.

But I don't think that the words will change a whole lot, because they're macro. They're designed to fit evolving circumstances and allow federal agencies to do what they do. The problem that we have is a little bit closer to home. And that is where we're going to continue to spend our effort, and our energy. because I think it's where we can make a measurable impact. We cannot do that without Industry. So I'm going to highlight four key areas and then briefly address a fifth. That would be NBIS. That might be on your mind.

So enhanced systems and data interoperability. We need to ensure that classified and sensitive information can move securely and efficiently across the industrial base, across all those complex acquisition chains, and end up bidirectionally both on the weapon systems and then be able to continue to feed a never-ending cycle. Because everything is in a constant state of upgrade.

Standardized security protocols; that means we need standardized security protocols and data formats. We need interoperability across networks, including secure cloud environments. Reciprocity that is real and is not just rhetorical. I almost didn't say that. Disconnected or bespoke systems don't make us more secure. They make it harder to see and stop threats and to be able to deliver that lethality that is expected of us. We are prioritizing our policies that encourage scalable, standards-based solutions that drive that interoperability and actual risk management.

This includes continuous emphasis on secure cloud. We've made some progress, but we have not nearly won victory over that issue at this time period yet. We have more work to do here. We're stuck in some regulatory areas below the threshold of the NISP. Your continued attention on this and our continued partnership with our acquisition friends in particular will help get us over that line.

In addition, DOD is piloting use of commercial providers to deliver classified spaces and networks. Some of you may have seen draft legislation related to anything as a service. This is designed to do two things: make us faster and create some efficiencies. Theoretically drive some of those costs down. Now I need to be cost aware right so we want to be able to do that, but mostly we want to be able to meet the mission requirements. We've got to be able to move with a great deal more alacrity than we do today. Let me say the concept isn't prohibited today. There's nothing in this policy that prohibits any of these things. Not one word. Find me those words. They do not exist. But the execution and the requirements are out of balance. That might be the most polite way that I can think to say it, but I am on the record.

This congressionally-directed pilot is about creating a repeatable, auditable, and secure model that expands access, lowers costs, and brings more players into the classified arena, where all that lethality resides, and will likely for the foreseeable future. Let me say that's an integrated, secure environment right. That's not just collateral that is all the pieces and parts across all of those five CSAs. Particularly between the department and IC. The objective is simple. Contracting companies and authorized personnel must have timely, secure access to classified infrastructure wherever and whenever mission-needs dictate. Those are government-derived mission needs. That's very important. These are validated government requirements. I think we lose that sometimes in the morass and the challenge of doing things that we haven't really done before.

Second, bolstering cyber security. The cyber threat environment is real, resourced, and rapidly evolving. Espionage, unauthorized disclosures, and insider threats are increasing. And while our adversaries continue to target classified networks, they're more aggressively targeting those internet connected commercial platforms that are the source of everything that informs our lethality, including those classified systems and networks. And of course, that's where we bring in my favorite three letters in the alphabet. C, U, and I.

CUI often lacks the protections and visibility we need elsewhere. I appreciate the ask for the CSAs to get together on this. I completely agree. The department has taken an active and leadership role on the implementation of CUI, in order to achieve much of what industry has laid out here as those pain points. The reality is we have to go further to fully implement the program.

But to do so, we will continue to pull and put tension on other parts of the government that need time to be able to kind of level set. The importance of the program will tend to vary depending on where you sit and what you do. We acknowledge that. What we have to be able to do to complete this and I think really address what is right here for us right now is to get us in a room, get together, and we invite the chair to do that. We will be there and we'll be brief.

The risk is compounded in this arena by the growing use of AI powered tools that can and do aggregate seemingly harmless data into powerful threat vectors. Our data repositories and tools must be built on a foundation of information security, not bolted on as an afterthought or built into a POAM that never ends. A recent example underscores this urgency. The indictment of 12 Chinese nationals for cyber espionage targeting US government systems and defense contractors. The scale and sophistication and the length of time of this operation serve as a wake-up call. Our cyber security, especially with our supply chains, is not anywhere near what it needs to be.

We are acting on this on several fronts in proud partnership with our CIO friends and I'm super happy that Stacy Bostjanick is here today. So please save all the hard questions for her. But promoting zero trust architecture, strengthening vulnerability management, adoption of the cyber maturity model certification and increasing cyber threat intelligence sharing across the industrial base. We need to stop building systems that assume trust and instead build detection, resilience, and recovery.

Information security reform. We are continuing our information security reform effort to modernize how the department handles classified and sensitive information. The goal is to move from a checklist-based approach to mission-aligned and intelligence informed posture. This includes digitizing class guides, improving the usability of marking and dissemination tools, enabling faster, more consistent decisions about how and when information can be accessed and shared. A great example of this, we've been pleased to partner with the Department of the Air Force on a recent initiative to digitize hundreds of classification guides. The result, improved capability for interoperability of highly complex classified systems, uniform answers.

Everyone's seen a class guide. It can be a choose your own adventure process. Again there's some method in that madness. But it's pure madness when you're trying to figure out how to interoperate weapon systems at mission speed. But a really sophisticated large language model. The hard part wasn't really the language model. The hard part was that the guides are kept in all kinds of strange and interesting ways. And being able to normalize that and to bring the data into a common way was nothing short of miraculous, and it continues. We have reviewed hundreds of guides.. It's great. Sadly however, we have thousands to go. But we'll take the progress for where it is and I really am pleased to be partnering with the Air Force on this game-changing initiative.

Finally, that's the kind of change we need. Security that doesn't hinder execution; it enables it. So those guides are now tools the way in which they've always been envisioned.

Acquisition security integration. Security must be embedded into the life cycle, not tacked on at the end or at various milestone decisions. We are issuing policies to improve this consistency, flexibility and risk management across Research and Development (R&D) contracting and sustainment. One critical area that has been mentioned already today is FOCI. FOCI Reviews must inform acquisition decisions, not just react to them. We cannot afford to award sensitive contracts or rely on a critical supplier only to discover after the fact that the entity is subject to foreign control. We cannot continue to do this. This creates a Stretch Armstrong kind of effect to awarded contracts. This adds risk to our acquisition cycle. It does not give us the ability to mitigate that. We are conducting a DOD wide study on the current impact of security policy on cost schedule and performance. The results will guide improvements. This is about aligning security with speed, competition and mission execution.

Finally a note on the NBIS and how it fits into the broader modernization integration efforts that I've discussed a bit today. And this is not just a system upgrade. It's a strategic enabler, critical to building a trusted, threat-informed, and interoperable personal vetting enterprise. It directly supports our ability to ensure that access to sensitive information is granted to the right people with the right access at the right time, aligned with mission requirements and grounded to inform risk based decision making. Recent milestones in the NBIS transition reflect important progress toward replacing outdated legacy systems with modernized end-to-end vetting infrastructure. These changes support the same principles we've emphasized across today's updates which you have heard my boss and leaders across the Department of Defense and elsewhere continue to echo and champion for years now. These changes support those principles: standardization, interoperability, and speed to mission.

At the same time, however, we recognize this transition has introduced challenges particularly for Industry. Issues around onboarding, data accuracy, and process synchronization are real. We appreciate your patience and professionalism and we are actively working to advocate and support DCSA and our interagency partners to identify, prioritize, and resolve these friction points. Just kind of a long-winded way of saying please use the phone. I know that there are those in the audience who will, but as new people and faces come in and new challenges present, that's the best that I think we can offer right now and I think that's pretty powerful stuff. We work pretty hard to be responsive, and the we in that is as broad as I can use the term. But I want to be clear. NBIS represents the kind of institutional reform we must embrace. It's not easy, but it reflects a shift from fragmented, reactive processes to a coherent, modern, and resilient vetting architecture. One that better reflects the complexity of today's threat environment and the need for trusted access at mission speed. But let's not lose sight of the fact that the threat environment is more dynamic and more agile than we could ever be. We're always going to be that way. Everybody in here have a cell phone? How often are you getting updates? Right? You probably don't check them anymore. So, how often is the software on those phones getting updates? You don't even check them anymore. Same basic idea.

Just as modernizing acquisition security, cyber security, and information protection, we must also transform the way we manage the most fundamental security decision we make: who we trust. And that leads back to a core theme I hope you heard clearly today. This is not a government-only effort. Industry is not a stakeholder. It is a partner. NBIS will only succeed through continued collaboration, candid feedback, and shared commitment to building trusted workforce capable of meeting modern demands. And I can say that my bosses and my partners, Jill Baker, Chris Gibson, and many others, they stand ready to do that. So, within the and I definitely want to be mostly responsive to LaToya, I said that beforehand, but the 30-day timeline is more than doable. And you have my pledge that we'll get that done.

These initiatives across interoperability, cyber security, information reform, acquisition integration, and personnel vetting are all part of the same imperative to build a resilient, secure, and agile DIB capable of meeting the challenges of the 21st century. Security is not separate from lethality. As Secretary Hegseth has said, we cannot afford to separate lethality from security. Protecting information and technology is central to our competitive edge. This is why our role through NISPPAC and beyond is so critical. We need collective insights to ensure policies are practical, operationally sound, and align with the realities of Industry execution. This is not a one-way conversation. This is a partnership building on shared trust and shared responsibility. So as we move forward and again, echoing my boss because again feels like a safe career move, security and counterintelligence are mission enablers. Compliance is not the goal. Mission assurance is. Collaboration between government and Industry is not optional. It's mission critical.

Greg said it best in one of [his] remarks. Execution on contract. For everything at stake, if that's not our focus, then I'm not really sure what we're doing here.

So thank you. I look forward to your questions and to our continuing work together.

Michael Thomas, ISOO: Thanks very much. Questions from our members?

(No questions raised)

Michael Thomas, ISOO: In the interest of time, we're going to move forward and remind everyone participating in the chat or online that you can send your questions to nisppac@nara.gov to ensure they're preserved in the record.

Jennifer May, ISOO: Thank you, Jeff. Next up, we have Mr. David Cattler, the director for DCSA.

David Cattler, DCSA: Thanks a lot for the opportunity to speak. Jeff and I; I think you're going to hear us both emphasize several common points, especially the need to adapt policies and the nature of the work for now and for the future. I'd ask you to please take note, not just that we agree, which I think is really important to ensure we've got good alignment between OUSDI&S and DCSA, but for two other reasons. I think one is that it's important that Industry not just give us feedback, but also jointly advocate for the need for these changes and be very clear about what's necessary from an Industry perspective. I'll talk a little bit about that as I go through. But I'd also ask you to please take note of the elements of this speech. I gave some pieces of this last week at the NISPPAC [Industry Day] and I think some of these questions were answered quite a few times. I'll answer them again today.

As a director, I'm proud we're the lead implementer of the National Industrial Security Program, not just for DOD, but also for 35 other departments and federal agencies. DOD has received clear policy direction, both the president and our secretary, to ensure that the industrial base is rebuilt and capable of rapidly fielding emerging technologies. This will include, I think, attracting more companies, including small and innovative firms, which themselves may be new entrants into the industrial base. These will help improve the readiness and lethality of the warfighter. But since these new entrants will be largely unfamiliar with the NISP, we also expect to see an increased need for our security services and oversight, increased communications, and interactions. Our adversaries know our industrial base is key to military effectiveness and to our economic competitiveness. So you can be sure that they will redouble their efforts to steal technology and information and exploit weaknesses within our security enterprise.

DCSA is the largest purpose-built security agency in the federal government. No other agency delivers the volume, velocity, and variety of security services that DCSA does. Our workforce is co-located with industry around the country and delivers integrated security services with both economies of scale and economies of skill. We are operating with a customer provider mindset and preparing for the future of the agency. You've seen that we published a new strategic plan in March. It describes three strategic thrusts we are currently implementing.

The first is to move DCSA to full performance and integration in each mission. The second is to anticipate and prepare for the future by equipping the agency to confront an evolving threat environment in the year 2040. And third, to raise the level of understanding and awareness of DCSA as the premier provider of integrated security services for the federal government and then as an extension out to Industry. The strategic plan makes clear that DCSA is, foremost, a service provider, and we want to be the service provider of more services. The true service provider for the full suite of security and vetting services for the federal government. So what does this mean?

It means we're focused operationally across all of our missions and we will continue to drive cost efficiencies, engage customers, and act on feedback to create better customer experience and delivery and to provide quality in terms of return on investment, national security impact, reliability and consistency in all of those services. Now, let me share a few observations about the state of each of our missions that support the NISP. These missions are executed by a workforce, as I said, located across the country, who are dedicated to this mission and trained in specialized roles. Our industrial security representatives or (ISRs), our information system security professionals or (ISSPs), counter intelligence security analysis (CISAs), the foreign ownership control or influence (FOCI) analysts.

Over the past two years, our performance in personnel security did not meet the required performance standards. So last fall, we stood up a dedicated personnel vetting transformation tiger team to conduct an end-to-end review of all personnel vetting processes and to generate data-driven recommendations. We partnered with a PAC PMO to follow a phased approach that produced a wide range of recommendations; from targeted quick wins to major changes to our processes and organization. And I've directed DCSA to implement all of these recommendations and to reorganize our personnel security mission.

So to LaToya's question, frankly, we haven't seen a rise in inventory or timeliness since last year. Since standing up the Tiger team, we reduced the background investigation inventory from a peak of 290,000 in September of 2024 to 222,000 in May of 20 of 2025, which is more than a 24% reduction in less than 6 months. The timeliness metric that is most important for our customers is a lagging one to inventory reduction. But even there in April, we saw timeliness improve by about 10%. We're using this data-driven approach to make changes that will have an enduring impact on how we conduct business. We anticipate we will continue to drive improvement in our performance numbers, even as we are reducing our workforce through the various workforce shaping methods. You'll hear more about the personnel security mission metrics from Donna McCleod, who represents our adjudication vetting services.

Now on NBIS. The future of the personnel security mission, as Jeff said, is linked to our delivery of NBIS. When fully operational, NBIS will be the end-to-end IT platform to support the delivery of those personnel vetting services for the entire federal government. Two weeks ago, we did get permission to move this ACAT 1 software development program back into the execution phase of the DOD adaptive acquisition framework. This is definitely a significant milestone. We gained that approval on an accelerated timeline while making progress in other areas to prepare the program for success. We achieved this milestone by working in close partnership with many key stakeholders across the department including the offices at the Undersecretary level for Intelligence and Security, Acquisition and Sustainment, and Research and Engineering, the DOD Chief Information Officer and Chief Data and Artificial Intelligence Officer, the Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency and the DOD Comptroller. And I'd be remiss if I didn't remind again the entire PAC and the PAC PMO. Over the past year, we reimagined and rebuilt the NBIS program. We established a new governance structure with I&S as the program sponsor managing requirements and A&S as the acquisition decision authority. This governance structure is the entry point for industry and customers to provide their requirements.

Second, we developed an NBIS digital transformation roadmap and architecture that was approved by A&S. During the past six months, NBIS achieved meaningful progress towards the goals of migrating and modernizing the existing systems, making cyber security improvements, and completed the foundational work to move back to the execution phase.

Third, we translated digital transformation into the NBIS product roadmap, aligned to the trusted workforce 2.0 strategy, and did all that to guide our agile development over the next two years. The program is slated to complete by the fourth quarter of fiscal 27 and the legacy systems to be decommissioned over the course of fiscal 28. Moving to the execution phase paves the way for rapid development of operational software in accordance with this roadmap.

And fourth, and finally, we built a new team, with a technical focus to drive this new vision for the program. This included hiring me, an enterprise program manager and a chief product officer. We have the right people in the right roles and we have upskilled that workforce.

In March, we met the first milestone on the product roadmap with the release of the initial iteration of the personnel vetting questionnaire for non-DCSA investigative service providers. The next phase of PVQ implementation will be to roll it out for use for the 5-year continuous vetting (CV) update. We aim to do that roll out with a limited audience this June and the NBIS team will engage Industry to test this new capability.

Moving on to industrial security. As the lead implement of the NISP, we're reducing facility clearance timelines while increasing our outreach and efficiency. Before jumping into performance data, I'll note that last October, we launched the security rating scorecard, which as you know was developed in partnership with Industry. Those results so far indicate that we're achieving the desired effect: more fairness in scoring, and an overall improvement in security review ratings.

To answer another question from the panel, the fiscal 25 initial and upgrade FCL package inventory is less than 300 cases, which is the key performance indicator (KPI) and right now we're sitting at an average of 43 days for non-complex tier 1 cases and 284 for complex FOCI tier 3 cases. ATO timelines are also ahead of schedule. The goal is 90 days and our 12-month average is 80.4. This includes both Industry and DCSA processing time. While the timelines are down, our count is up. We are issuing more FCLs to Industry; 32% more FCL's so far this fiscal year than in the same time frame in fiscal 23. And in addition, you will have seen recently that the Office of Management and Budget (OMB) has approved an update to the SF-328, which reduces the numbers of questions and provides comprehensive instructions which aim to add clarity and specificity to the form. This should provide uniformity across industry and government stakeholders and help us to further accelerate those reviews.

On the cyber security front, we're implementing the cyber operational readiness assessment or CORA as developed by the US cyber command. In fiscal 25, we anticipate completing 45 CORAs and are on track so far with 11 to 12 CORAs completed each quarter. We are one of the first in the nation to provide this service outside of cybercom itself. Now, I've received feedback from CEOs who have gone through the process and they noted that they consider the assessment to be very intense and not always comfortable for them and for their companies. But they were confident that the overall assessment and process helped them learn and to improve their security programs. You'll hear more about our cyber security program from David Scott from our NISP cyber security office later today.

We still have a lot of opportunities for improvement in this mission and we'll be applying the same tiger team approach to drive data driven continuous improvements on our industrial security services. We'll benefit greatly from streamlined regulatory processes, spending more time doing our jobs and less time just doing paperwork. And finally, better trained personnel and more resources can also improve speed, accuracy, and consistency. Our security training mission launched the DCSA Security Academy last October. And in August of this year, the academy will graduate its first cohort of students from the industrial security training program. Just a few weeks ago, the academy launched a new curriculum for information system security professionals. These courses will help ensure that our industrial security mission continues to perform at a high level with standard review processes across the board.

Also in support of the NISP, our counterintelligence mission has seen an impressive increase in the quality of suspicious contact reporting coming from industry and from academia. On average, DCSA receives more than 30,000 suspicious contact reports each year from cleared industry. Since fiscal 24, we're seeing an impressive improvement in the quantity and quality of that reporting. Of these reports, approximately 3 to 4,000, about 10 to 15% have counter intelligence value.

So in conclusion, again I'll echo Jeff. In the current environment, we have to work together. It's the operating environment and the threat environment. Efforts to revive the industrial base and modernize acquisition must be met with concomitant change in authorities, resources, and expectations for security to be viewed as part of an integrated mission or acquisition approach. If not, we are increasing our risk and attack surface and setting up security to continually be viewed as an impediment or a drag on the system and not as an enabler for the capability outcomes that we all seek. Without security modernization to meet the moment, we risk losing our decisive military edge on the battlefield and we could see an erosion of our broader economic competitiveness.

Our aim is always to protect the data, workflows, and technologies, enabling military lethality, warfighter dominance, and to guard against surprise on the battlefield. If we do not, the enemy will be ready for our warfighters and our allies. Our adversaries will have countermeasures, and it will cost lives. Protection of the industrial base is an enduring process. A way of life that we enable through the NISP and through the collective work of many stakeholders in government, cleared industry, and cleared academia. To achieve security modernization, we need to ask some hard questions. Are our rules and processes still fit for the threat environment today and into the future? Is the NISP framework adaptable enough to meet the threat environment we will face over the next generation or out for the next 35 years? And as the administration and Congress move out rapidly on acquisition reform, this is the moment to convene, to partner, to consider these questions and revisit the industrial security policy framework and review the roles, authorities, and approaches to shared risk management. We seek to achieve greater efficiencies without compromising national security. This can reduce the cost of security being borne by both the taxpayer and our industry partners. We are committed to improving our business operational performance to be ready for these increasing demands on our mission and increased authorities. Security is a team effort that involves DCSA, other government agencies, cleared industry, academia, and the research community. None of us can do it alone.

I spent the last year engaging and listening to industry leaders at various levels: CEOs, CSOs, COOs, other C-Suite executives and a lot of facility security officers. The common theme that emerges is that they are all ready and willing partners for change. Industry leaders are patriots and they enable the nation to be ready for the fight. As we kick the arsenal of democracy, our industrial base, into overdrive, we must be ready to review and reconsider how that entire team can work together differently to meet the current moment and to rise for what the future demands. Thanks very much.   How'd I do?

Michael Thomas, ISOO: Questions for Mr. Cattler?

LaToya Coleman, Industry: LaToya, Industry NISPPAC. Mr. Cattler, I have a question for you. Industry would like to get a better understanding of how, moving forward, DCSA will better engage and communicate with Industry as you guys move forward with development and deployment. It's our understanding that you guys are outside of the planning phase now and more into the implementation phase of NBIS. So I would like to know how you guys plan to engage and communicate better for that particular application and, in addition, going forward with NI2 and SWFT and all of the other systems that you guys have in the pipeline.

David Cattler, DCSA: In a few ways. Meetings like this. The one we had last week. In these speeches, I've encouraged everybody to check the website and follow us on social media. We're putting out a lot there. We just had this discussion a week ago, right? So, the how still needs to be developed. It's been tasked. It's in work. I'm not prepared to answer you right now exactly how all that's going to work, but as I say, I have directed it. We will do it and we'll get after it.

LaToya Coleman, Industry: Thank you.

Michael Thomas, ISOO: Other questions?

Jane Dinkle, Industry: Jane Dinkle, NISPPAC Industry. In preparation for this meeting, I reviewed the November NISPPAC public meeting notes and at that time we were talking about the new or updated SF-328 and its release to Industry. It has now been released to Industry and is part of the system. And back in November, we commented on that. I realized that the SF-328 doesn't have to be updated unless you have a significant change. You don't have to update it just because it's an updated form. I understand that. However, the current requirement is that when you have a significant impact to the SF-328 information, it must be updated and submitted to DCSA within 30 days.   We requested back during the November meeting that because of the significance of the changes to the SF-328, that be extended to 6 months; that Industry have six months to report those changes through an updated SF-328 submission to DCSA and you agreed.

DCSA agreed. Thank you. However, I've not seen anything put out to industry to say that that timeline has been extended from 30 days to 6 months. So, I'm just curious now that the SF 328 is here, it's implemented, and Industry is starting to use it, when can we hope to see some communication regarding the timelines being extended to 6 months? Thank you.

Matt Reading, DCSA:. Hi, Matt Reading from DCSA. Jane, appreciate the question. Now that the 328 is out, the work begins. I think we have to kind of rebaseline what the form is. Make sure that we have a clear understanding of what implementation and changes are going to be, because as with any new administration, as policy begins to emerge from the comprehensive review, we want to make sure that we have a joined up approach to what the implementation timelines are. So as with anything with DCSA, we want to partner up with the NISPPAC, get the working group together, and talk about the communications and the implementation of that. Using the leverage and the power that the working groups have been able to produce. Director Cattler mentioned the balance scorecard. We have a similar pathway for a couple of the forums. The 328 is one of them. So looking forward to that partnering and certainly the communications products that will flow both through government and Industry channels as a result of that work.

Jane Dinkle, Industry: Thank you.

Jennifer May, ISOO: Next we will hear from Miss Lisa Perez, the Chief Policy and Collaboration Group, Special Security at National Counterintelligence Security Center, Office of the Director of National Intelligence. Lisa.

Lisa Perez, ODNI: If you could go to the first slide of our briefing. So this slide shares some details about congressionally directed actions or the CDAs. So of the many CDAs we have, several of them are industry related. If you could go to the next slide.

We're currently working on four of those CDAs and including those listed on that slide. But for the sake of getting to all the topics, I'll focus on the two that were requested by LaToya. So a policy on submittal for access to classified information for key management and oversight positions. This is the overhead policy that Latoya mentioned. The draft is indeed still with our general counsel, and as we speak right now, the leads of this effort are meeting with our general counsel as they try to move this policy forward. I was not, unfortunately, able to get a timeline on the next steps, but we'll request the lead to reach out to LaToya to inform her of the timelines and then maybe she can share that information.

Another CDA that Latoya requested information about is for the policy on sharing of covered insider threat information pertaining to contractor employees. This policy draft is being reworked to better address Congress's requirement and is in our internal center coordination which of course does also include our general counsel. So possibly the same people are involved and potentially they're talking about that in the meeting today, but they didn't relay that bit of information to me beforehand. I would guess that they actually are all speaking on it. If you can go to the next slide, please.

So the Security Executive Agent Directive (SEAD) 4, hopefully that's what you're seeing on your slide. It provides 13 national security adjudicative guidelines and those are used in the evaluation of an individual's eligibility for access to classified information or to hold a sensitive position. And if you could go to the next slide, please.

So based on feedback received in recent years about SEAD-4, we are gearing up to conduct a comprehensive refresh review to ensure the guidelines are effective, that they're efficient, and continue to promote uniformity in adjudications. We're leveraging research, previous case damage assessments, and of course looking at all of the adjudicative concerns. Our research group is establishing some surveys that will begin to sort of feed the sources of information that we'll talk about as we move forward.

The timeline includes initial scoping which is completed. So the research and literature review is ongoing right now and then onto the small interagency working groups that will hopefully begin in the coming months followed by the formal interagency working groups that we hope will wrap up by the end of the fiscal year of course before drafting the product in maybe early fiscal year 26 and then publishing by the end of the first quarter in fiscal year 27 hopefully at the latest. If you can go to the next slide please.

You should be seeing a slide on trusted workforce 2.0 so the slide provides an overview of trusted workforce 2.0 personnel vetting reform effort that includes leadership by the DNI, director of OPM and OMB through the performance accountability council along with the Under Secretary of Defense for Intelligence and Security. The objectives of the reform effort include rapid delivery of trusted workforce to execute missions of the government, improve workforce mobility, and of course increased insight for risk management. So from the bottom of the slide you can see that there are three phases of the iterative implementation. Phases one and two are completed and we of course now are in phase three which addresses implementing the full trusted workforce 2.0 personnel vetting model. That means getting the capabilities finished, deploying expanded personnel vetting shared services, and focusing on improvements in performance management as we expand the collection of metrics under the new vetting model.

And in fact today there was some discussion back and forth with Mr. Cattler regarding some of the implementation and services. So what we at ODNI have been doing as of late includes releasing the joint refinements to the federal personnel vetting management standards appendices and that ensures they continue to align with trusted workforce 2.0 framework and a key focus of the update outlines workforce reporting requirements for continuous vetting and that was for the low-risk and the nonsensitive positions out there not our national security [positions]. So just want to reflect that for the national security positions there's no significant changes in that policy. There mainly were again for the low-risk and non-sensitive positions.

And then another recent issuance included updates to quality assessments of background investigations and we just wanted to make sure that we included coverage of investigations that will be completed under the new investigative standards for agencies who will be implementing the full set of new investigative standards, a few of those beginning this year.

And then separate from policies, ODNI is working on capabilities that will support further implementation of the trusted workforce 2.0 personnel vetting model. And namely, we're working on updates to scattered castles and the development of a system known as the transfer of reciprocity information system aka TORIS that will support the intelligence community secure sharing of personnel vetting information that's necessary for the mobility of personnel between agencies. So, for example, if you complete a personnel vetting questionnaire through DCSA's eAPP, and should you be transferring to an intelligence community agency, we envision, of course, that system would be able to transfer the questionnaire to the intelligence community agency you'd be transferring to. The eAPP functionality is expected to be deployed in TORIS in fiscal year 26. As we get closer, we'll be able to get more fidelity on a more specific timeframe. There will be other capabilities within the system, but we're still working out all the details of that. Again, as we progress, we will share more information.

So regarding the question about SCI processing timelines and a request for the working group certainly seek support and participation for this. First, I would like to get with LaToya to gather more details about the Industry perspective. That will help inform a request to the community for participation in a working group. So I'll follow up this meeting today with an email to her so we can connect.

And then we are thankful for the input from Industry regarding training reciprocity and we'll seek discussion within the community on addressing this ask and of course hopefully getting to a point where we lessen the burden on industry in this area.

EO requirements came up. I did recently mention at the NISPPAC industry day that we expect to announce the reissuance of a number of the trusted workforce 2.0 policies and artifacts in response to about a half dozen EOs. So most of these updates have no effect on Industry. But as we move forward, addressing the different presidential direction provided through EOs wherever it is fitting, we'll seek communication and coordination with Industry partners. Again thank you for foot stomping on that. Make sure we don't forget what's much appreciated.

And moving on, I know I don't have a long timeline. I know there is a great deal of interest across Industry regarding ICD-705. With Tessa Dutko being there, please welcome her and she'll provide more information with you on that topic.

Tessa Dutko, ODNI: Thank you Lisa. Again, my name is Tessa Duko. I am a technical security and policy officer at NCSC. And today I just want to give you an update on what we are doing in coordination with industry to update the 705 series policy to have SCIF upgrades and compliance with current standards and support the increased protection of SCI. I do want to just start out by noting that kind of reiterating what Kathy had stated earlier in the meeting that over the last few months we have really increased our communications with Industry and it's really been helpful in understanding what are some of the complex challenges that industry deals with separate from what the IC internal deals with in their mission to support the IC partners. Through that communication we have started increasing our representation from Industry in a number of forums within ODNI. I do have a slide at the end that will list those if you are interested, but just to kind of quickly cover them here, that includes the data center working group which is our newest working group we stood up.

We've had I think three meetings now. That is a forum that is specifically for cloud service providers supporting SCI mission functions for data centers and just at our last meeting last week we were able to share draft policy with them, some of which I will discuss here, and get some really valuable insight about the challenges that they face when they're constructing and operating data centers for IC elements. Separately we do have representation from NISPPAC at the PTSWG, the physical technical security expert working group. This is the group of IC representatives that are responsible for drafting and approving and implementing 705 series policy. The importance there is really just some of the challenges even brought up today by industry are things that we can bring back to the IC and have an open discussion on. What can we do to address some of these challenges and kind of really support the mission there better?

Finally the third is the industrial security representatives meeting that is led by the special security directorate, Lisa Perez and her team, that include the ability for NISPPAC representatives to engage directly with some of the CSAs from the IC elements.

So today I will just move into probably the most interesting topic for 705 related to what we are doing to get SCIFs up to compliance with current standards. So in January the director of NCSC issued a memorandum that essentially stated that the current technical and physical security threat levels within the United States and elsewhere no longer possess the ability to protect SCI in the way we wanted to and what was necessary unless they complied with current standards.

And as many of you may be aware, legacy SCIFs made up 50% or more of the current SCIF footprint across the US and worldwide. That includes DCID-121 and DCID-69. And so what that memo did was, it was a three-step approach. We got in a room with the IC elements. This was a catalyst from Industry's concerns that they were getting mixed messaging from the IC on what they needed to do to get into compliance. And so to get on the same page and get to a standard process, the IC agreed that we wanted to get the POAMs for any SCIFs that were not currently compliant with 705 completed by the end of 2025 and then to implement those POAMs by the end of 2028.

And as part of that, the ODNI wanted to really get a comprehensive understanding of what that footprint looked like and within 120 days get feedback from the IC on any SCIF that they accredited that didn't meet 705 standards. We have completed that data call. We have feedback from all of the elements to include those that are accredited for Industry by IC elements and we are working with them to get the POAMS in place. Moving on to the next slide.

As part of that process in upgrading SCIF, we are pushing an entire upgrade to the 705 series policy. So I'm very quickly going to cover what that looks like right now. The first of those is the ICS 705-01, which is the basic implementation guidance for ICD-705 and how you manage and operate your facilities. And what we are doing right now is we are updating our facility types. We are updating our risk assessment process. Part of this that's very interesting to Industry is the risk management approach and the need to do a risk assessment in many cases that is not well outlined for you in that policy. And so as part of that we are going to be issuing a form that will give an outline that can be used by IC elements and I think this will be really helpful to Industry, of what do you look at and what do you actually assess when you're doing a risk assessment process. That will go much deeper than what is currently there, which is what is the physical risk, what is the technical risk, what is your counterintelligence risk.

The other thing that we are looking at in 705-01 is getting security-in-depth a little bit more defined in a way that is helpful for reciprocity. So when you have security-in-depth in your facilities and you say I have two layers maybe that is not accepted by another IC element and so what we will do is we will have a standard outline for what are the components of accepted security-in-depth. If whatever you are using as a layer meets these criteria, it is considered a layer.

Moving on to ICS 705-03. This is the direct result of an R&D project out of NCSC where we looked at what were some of the issues with reciprocity and vulnerabilities to the wall types for SCIFs. As a result of that, we will be implementing an instrumented testing format for the community. So right now, as you're aware, you are not doing instrumented testing for acoustic standards. Many times it's a "can you hear me?" type of test. This will be replaced by required instrumented testing. This standard is going to be behind for issuance of all of the other policies I'm discussing today. They are on track to be finished by the end of calendar year 2025. This ICS [705-03] will probably not be done until roughly the spring of 26. And that is just because we are still getting processes in place for getting your equipment and how you would program that equipment and things like that which you will get far in advance of any need to comply with that policy.

Moving on to 705-04, this was already issued about six months ago. This just outlines what are the required mitigations if you are going to bring foreign partners into a SCIF that has no foreign (NOFORN) information when they are supporting a critical mission set. And most often we get this feedback especially from our foreign partners in the Pacific and the need for them to be able to support those critical missions. This policy allows them to do that in a safe manner.

Finally, ICS 705-05. This is the data center ICS that I referred to that the Industry representatives and cloud service providers did get the chance to review in our last data center working group meeting. The IC has seen this once and provided comments. We received a ton of valuable feedback at last week's meeting from industry about parts of that policy that would be a major challenge to them; where they would like if possible for them to be able to work closer with their accrediting officials to deviate from some of the areas when they had mitigation measures in place to address the deviations and things like that.

So the point being is we are getting really great feedback from Industry on these areas and we're looking at that. We're sitting down with our IC representatives and seeing how we can integrate some of that feedback into the policy as it's in draft, instead of going back after it's already been signed and trying to fix something that we could have proactively worked on during the initiation phases. Next slide.

Finally, there's two policies here I just want to discuss very briefly that impact 705 greatly but are not slotted under the 705 series that are also currently in draft in coordination with the IC. 702-01 this is the technical security and signals countermeasures for SCIFs. So as many of you are aware, and I think Kathy brought up today, there is somewhat of a disconnect between the TSCM and TEMPEST worlds. What are we doing as far as the TEMPEST countermeasures that are required? What are our processes? Are we even defining what those processes look like when those two groups are talking to each other? And so this policy does outline and define what are the required steps when you're integrating TSSC. And so I just want to be clear here, TSSC is the integration of two separate disciplines under one umbrella. So TEMPEST and TSCM remain separate disciplines but there will be conceptual frameworks for how you are looking at TSCM versus TEMPEST and how those two components must talk to each other when you are determining TEMPEST countermeasures for facilities when you are doing TSCMs and they will be the nexus for replacement of what is currently the procedure guides which is how you conduct the TSCM. So as that moves along, we will keep Industry informed of that so we can have some of the discussions that Kathy had brought up today about what is Industry's role in how those assessments are done and where can Industry play a critical part as we see staffing concerns and things like that.

And then finally IC124-01 which is the electronic medical device review process. This looks at a consolidated and standardized framework for IC elements to utilize when they are reviewing medical devices against the threat to their facilities posed by those medical devices. So, it's really just like I said, a standard process where you can bet a medical device for what its capabilities are only, not what type of device it is, what are the capabilities that it possesses that may pose a threat to that SCIF. And then separately, how the IC element is able to assess the SCIF itself for what technologies may pose a risk. When you compare those two codes, you can see whether or not any technologies in that device itself may pose a risk to the facility. And what that does is, it still allows the authority of the IC element to say “I can accept the risk of this device” or “I feel comfortable with having this device given the mitigations that my facility possesses”, but it makes everyone look at the device and the facility the same exact way. So from an Industrial perspective, if you're supporting multiple IC partners, the hurdle of getting this device separately approved in a long timeline possibly by different IC elements should be very consolidated by this process, as you will have one code that can be shared with any IC element to very easily vet against their facility. That is again, currently in draft, and it has been shared with the community. We are adjudicating comments and then we will move it forward. Also expect this policy to be completed by the end of the calendar year.

Finally, I don't want to get too in the weeds on the tech specs because it by itself is in the weeds as a document, but if you want to go to the next slide, I will surf the wave tops really quick on the tech spec. We are revising all 14 chapters. Chapter 2 is going to have that updated risk assessment process. It's going to have that updated security-in-depth criteria I talked about. And we are also working really heavily with the CAP/SAP community to get reciprocally accepted compartmented areas which is a pretty big deal if you have to deal with compartmented areas, you know, that you're going through a multi-step process to get any number of caps approved within that area. So what we're doing is we're working with the CAP community to say what do you feel is acceptable for a CA space If they possess these qualities, right if you have met all of these standards you're not having any waivers, will you accept that as a standard CA without additional mitigations or any other additional requirements for those caps. So we have shared that with the CAP/SAP community and they are providing comments currently.

Chapter 3 we have our documentation and construction requirements. We are looking to remove the U.S. person's requirement for construction and update it to U.S. citizen requirement for construction and also allow the use of CSTs domestically as a threat mitigation if the AO deems necessary.

We are also updating our chapter 6 which is very important to the DOD and their support to Temporary SCIFs (T-SCIFs) shipboard SCIFs, airborne SCIFs and then also we will have a separate T-SCIF checklist so that you are not using a traditional permanent SCIF checklist to accredit a T-SCIF. Next slide.

Chapter 9 will have an acoustic testing framework once that ICS is issued on the acoustic requirements. Chapter 10, we'll have your Personal Electronic Device (PED) guidance for how you are adjudicating your medical devices and reviewing them. Chapter 11, we have added some updated guidance on fiber optic cables, which should be included and considered as part of the upgrades to your CIFFs that you're currently doing. And then finally, we are working with the TEMPEST advisory group to update the TEMPEST checklist and trying to get to a more standard review process for TEMPEST.

We are updating our fixed facility checklist to mirror what we have talked about in the upgrades for all of the rest of the tech specs. So obviously, as we update any number of chapters, the fixed facility will be updated to reflect that. And then we are also working to update our co-use agreements which Industry is also a part of as I know they have a big footprint in the co-use world. So I will stop there, and any questions if we have time?

Michael Thomas, ISOO: Any questions for members? We are running a bit long, so we're capturing questions from the chat via email. But questions in the room?

Ike Rivers, Industry: I do have one question for Perez. Lisa, can you hear me? Lisa, are you still on?

Lisa Perez, ODNI: Hi. Can you hear me?

Ike Rivers, Industry: Yes, the only question I have is regarding the covered insider threat [policy] for covered employees. You said that the policy is back in process. You remember initially that Industry was involved in some of the language. Since it's being reworked, is Industry going to have the ability to be part of seeing that rework?

Lisa Perez, ODNI: I did not get a response. But I will again inquire about, okay after we get through this next phase, is it going to go back out again for further coordination and then I'll send you a follow-up email. Is that okay?

Ike Rivers, Industry: Thank you.

Jennifer May, ISOO: Next we'll hear from Don, the Chief of the Central Intelligence Agency's Security Policy Staff. Don?

Don, CIA: Yeah, I'm here. Just a couple of items. In an earlier meeting, a question was asked about CIA's FOCI vetting process. So here's the information that my colleagues passed along to me.

The agency's supply chain and acquisition assessment branch is responsible for vetting companies as part of the foreign ownership, control, or influence process (FOCI). Documentation that's submitted by relevant companies is used to supplement other available information and is closely evaluated to determine whether any foreign ownership exists, within an entity, or within its organizational structure. To aid in the company vetting process, it's requested that each of the submitted documents are complete and accurate. This would include having the documents signed and dated, having the key management personnel list, including all key executives, and ensuring that 100% of the company ownership is accounted for. This can include providing information relating to any parent entities and including a response for any of the questions that are answered affirmatively on the SF-328 document.

On the second item with regard to the question on the earlier memo that indicated that clearances would be terminated for certain overhead personnel, we can share the following information on the topic. With the new CIA Office of Security Record System now automatically interacting with the contracts record system, all clearance actions for individuals must be tied to an active contract. In late February 2025, the technical team completed the termination of some clearances that were not tied to an active contract or previously known as a J-contract. These should not have impacted any other overhead clearances that were on active contracts. For the individuals formerly on the J-contracts who still need access, we recommend that a form 4311 be submitted.

The form should indicate that an untermination, or however you want to say it, with Contracing Officer's Technical Representative (COTR) signature be submitted as well as something indicating that it's a contract number change. The active contract number would then be cited. It's important to note that there are now costs associated with all clearance actions. So there must be contractual efforts and funding in place for those linked to an active contract. And that's on those two items. And then Jen, my colleague and alternate, is going to speak just briefly on training and CTTA testing. Jen, are you there?

Jen, CIA: I just wanted to touch on two items that I heard discussed earlier in the meeting. One is training and consistency with training and allowing acceptance of other organizations training. So this is an area where CIA does accept IC elements training, except for when an individual has our high-side system access, then all training must be done on that system unfortunately. But if the users or the personnel do not have our high-side system access, then we will accept training that is provided and taken by IC elements.

The other item I wanted to touch on is CTTA testing. From a resource perspective, we do not conduct CTTA testing. However, if the spaces are built to the standards that we provide, then we will provide an accreditation without the testing and we prefer not to have the companies pay for or conduct their own testing. Any other questions for CIA?

Michael Thomas, ISOO: No questions? Alright. Thank you very much.

Jennifer May, ISOO: Up next is Mr. Richard Dejausserand, Deputy Director, National Security Services Division, DHS for their update. Rich.

Rich DeJausserand, DHS: Good afternoon everybody. Thank you for having me and thank you for attending. I appreciate it. I just want to update on the three questions that Industry had. I don't want to take too much time, but I will also say that DHS is prepared to attend and participate in any CUI working groups. DHS has not fully implemented CUI. But that's not to say that we're not prepared. We have monthly working groups with all the components to ensure that we have draft training. One of our challenges is that DHS has over 12 law enforcement categories. So, trying to determine how we're going to categorize those law enforcement categories, i.e. like LES, since DOJ owns LES but DHS uses LES. With the Transportation Security Administration (TSA), they have sensitive security information, multiple categories. So, we don't know how to categorize those with CUI, but we have working groups. We're ready to go once the executive order, if and when is signed, to move forward with CUI. But happy to participate in any working groups that ISOO or anybody brings up. We're happy to be there.

Regarding information sharing with Industry, we have multiple layers of information sharing. We have our information sharing and analysis centers (ISACs) provide a platform for sharing information about threats, vulnerabilities, with Industry. We also have our DHS alerts and notifications that we send out. We do that through not only our DHS industrial security headquarters, but we do that with our acquisition and procurement partners. We have multiple online platforms and portals that we can share resources. Industry can access timely information and different reports and guidance and, in addition, about two years ago we started with LaToya, our DHS Industry focus groups where we've met with Industry partners, we go over protocols, different initiatives that we're working. We are also open. We invited Latoya and others and actually met with our Chief Security Officer of DHS. Happy to do that.

And the last question was the reciprocity of training. Same thing. DHS accepts 99% of all of our IC partners' training. It's very rare that we don't accept a training. To this date, I've been doing this job for four years now, I've not seen where we have not accepted someone's training. But with that, that's all I have. Unless there's any questions for me.

Michael Thomas, ISOO: Any questions for DHS?

LaToya Coleman, Industry: LaToya Coleman, NISPPAC Industry. So for clarification, you mentioned that you are waiting on the executive order to be released in order for you to implement CUI. Is that correct?

Rich DeJausserand, DHS: That is correct.

LaToya Coleman, Industry: And the second one is a comment. I will absolutely take you up on that offer to meet with the CSO because one of the concerns that I have is even when the executive order drops, how are you guys planning to implement it if you're struggling with the law enforcement categories today? So that would be of interest how that will affect Industry going forward. Thank you.

Rich DeJausserand, DHS: Yeah, so let me clarify. That was a challenge. We are working with DOJ. I think where we're going with law enforcement sensitive information as LES is we may have it as a category DLES, Department of Homeland Security law enforcement sensitive. We have implemented how we're going to implement that. We're just waiting to see what the actual executive order says. Does that make a little more sense?

LaToya Coleman, Industry: It does. But I'll still take you up on that offer.

Rich DeJausserand, DHS: Absolutely. Happy to take you up on that.

Greg Sadler, Industry: Thank you, Greg Sadler from Industry.

Rich DeJausserand, DHS: Thank you.

Greg Sadler, Industry: One question on your training reciprocity. You referenced that you accept IC partner training. Do you also accept DCSA collateral training that's provided across the community?

Rich DeJausserand, DHS: Yes, we do.

Greg Sadler, Industry: Okay, thank you.

Rich DeJausserand, DHS: You're welcome.

Michael Thomas, ISOO: Further questions? Alright, thank you.

Jennifer May, ISOO: We will now hear from Ms. Jaime Gordon, Program Planning and Management, Office of Security, Department of Energy, who will be providing their update. Jaime.

Jaime Gordon, DOE: Hello there. So, I'm going to address a couple of the questions that we had. The first question that we did have was how often does DOE perform business assessments? So most of our analysis is conducted through our eFOCI system which is our system of record. We do complete formal business assessments or some variation of that type of assessment on a case-by-case basis based on the offices and the resources. So, I would encourage if there are any specific questions regarding the business assessment that you go ahead and contact me or one of our other NISPPAC representatives and we can actually get you more information specific to that actual assessment.

In addition to the communication channels or vehicles that we use to disseminate information, we do have multiple policy panels, working groups, and various information resource platforms that we put our information out. So these are just a list of some of the working groups. TheProgram Management and Policy Panel does meet quarterly. We have the System Testing Working Group, Physical Security Performance Testing Working Group, Security Awareness Shared Interest Working Group, eFOGI Working Group and eligibility determination and things like that. We do have these that go on throughout the year. If anyone is interested in attending or being invited to any of these particular working groups we're always putting out information and making sure that we can get that outreach as broadly as possible. So please feel free to contact any of us here at DOE through the NISPPAC and we can get you involved in any of those. And unless there's any questions, that's all we have from DOE.

Michael Thomas, ISOO: Any questions for DOE?

(No questions raised)

Michael Thomas, ISOO: Alright, thank you very much.

Jennifer May, ISOO: Thank you, Jaime. Up next is Mr. Chris Heilig, Chief of the Personal Security Branch with the Nuclear Regulatory Commission for their update. Chris.

Chris Heilig, NRC: Hi, good morning. Thank you very much. So my colleagues here at the NRC did not provide any information for me to pass on to you. So we don't really have any reports or updates. But I'm happy to answer any questions if anyone has any.

Michael Thomas: Chris, that is a remarkable exercise of self-restraint and candor. Thank you for that. If there are any questions for the NRC we will take them, otherwise, Chris, you are the only thing standing between this very diligent group and their midday break.

(No questions)

Michael Thomas, ISOO: Ok. Thank you very much for joining us. We appreciate it. It’s 12:12. We will reconvene at 12:22 to pick up the next portion of the meeting. Thank you so much. Thank you, everyone.

(Break observed)

Michael Thomas, ISOO: Alright, everyone. Let's return to our places. We're going to get the meeting started in one more minute. Thank you very much.

Jennifer May, ISOO: We are now moving into the portion of the meeting where we normally get reports from the NISPPAC working groups. You've already heard from Industry, some of the CSAs and CSOs on the high level point of what was discussed during the Physical Security Working Group which took place on January 22nd and Clearance Working Group on March 5th. We'll also hear from DOE and NRC for their security clearance metrics, along with DCSA for their information systems and personnel security metrics.

First, we're going to hear from Ms. Monica Marks, the Acting Director of the Office of Departmental Vetting Policy and Outreach, within the Office of Environmental Health, Safety, and Security at the Department of Energy, who will be providing their metrics. Monica.

Monica Marks, DOE: Thank you and good afternoon everyone. The metrics I'll share on the following slides are provided by the Defense Counterintelligence and Security Agency.

Overall, DOE continues to meet the goal over the last two quarters with an average of 20 days for adjudications. DOE's timeliness overall has decreased to 19 days as the department has transitioned from traditional periodic reinvestigations to continuous vetting and targeted investigations when necessary. The cause of the increase in initiation time was due to technical limitations to capture an updated SF-86 and continue the clearance without requesting an investigation. The feature was not available until late fiscal year 25 quarter 1.

Now that the settings have been updated, the Department can now obtain necessary information and release the cases properly.

DOE currently has 1,152 pending adjudications with 75% of those being initial investigations. As we always say, if our Industry partners have concerns, we can assist from a DOE industrial security perspective. Please don't hesitate to reach out. We are ready to assist as necessary. Are there any questions?

Jennifer May, ISOO: Excellent, thank you. We're now going to hear from Mr. Chris Heilig, Personal Security Policy Program Manager, Nuclear Regulatory Commission, providing their metrics. Chris

Chris Heilig, NRC: Hi, thank you very much. This briefing will take just a minute longer than my last one.

[Laughter]

Chris Heilig, NRC: The gist of it is, our initiation timelines have always been okay. They're not great. We're still working on that. Trying to get applicants to fill out the forms, it's really the hurdle that we are trying to overcome. But I'm happy to report adjudications are pretty much on point. We had a slight slip up in quarter 2 of fiscal year 24, but otherwise it's been great. and I'm happy to report that thanks to DCSA, we are now signed up for eAdjudication. So, I'm hoping to get those averages even lower.

The next couple of slides, again, I won't go through every one of them but they break them down into the individual categories but again adjudication timeliness is great; initiation not that great. Other than that I don't have anything else to provide. Again happy to answer any questions.

Michael Thomas, ISOO: Questions for Chris?

(No questions raised)

Michael Thomas, ISOO: Alright, thank you very much.

Jennifer May, ISOO: Thank you, Chris. We're now going to hear from Mr. David Scott, Acting Deputy Assistant Director for the NISP Mission Performance of Industrial Security in the NISP Cyber Security Office for DCSA's information systems update. Dave?

David Scott, DCSA: Good afternoon everybody. So just one of the things that we're really super proud of and I also need to give a thanks to Mr. Greg Sadler for his partnership with the National Industrial Security Program Information System Authorization (NISA) working group. We really continue to progress in working on efficiencies, listening to our stakeholders, government and industry, specifically our ISSPs in the field but also through the NISA working group and industry.

So we have in FY25 made a couple of updates already. I'm not going to go through each and every thing here, but one of the big things that we've done is captured workstations and servers. That counts, because we know that there's about 5,000 information systems out there, but that doesn't include all the individual workstations. There are thousands of actual workstations. So we're trying to get a better traction of that and then also make sure that we're tagging that into our national industrial security system of record (NISS) so that we could properly categorize those facilities, which is a manual process right now.

Planned updates; again, we continue to provide enhancements based on our feedback from Industry and our stakeholders. One of the big things that we're trying to do is centrally manage our MOU processes. This is one of my pet peeves. Right now I've got one single cyber security subject matter expert (SME) at our headquarters that works all MOUs with our government and Industry stakeholders. We're looking to automate that through eMASS. Right now we have the capability to move our existing MOUs that we keep at our headquarters into the system and we're going to slowly start tagging those with individual eMASS IDs and we're working through workflows in the next revision so that ISSMs will be able to enter and submit their ISAs in the future and also we're planning for PDS entries etc. So, we're trying to get more efficient and utilize the tool as a business tool for centralized management across the board.

One of the other things that we're working behind the scenes at headquarters is we often get asked at forums about NIST 853 rev 5 and when we're going to go there. We have such a large complex portfolio of 5,000 systems. It's going to take us some time. It's going to be very strategic, and it's going to be in partnership with the NISA working group. We're going to have to. But first, we've got some homework to do that we've been doing behind the scenes at headquarters, which is making sure that we're organizationally defining all of those additional rev 5 requirements. So, we're doing that hard work right now. We've already talked to Mr. Sadler in the NISA working group. In the fall timeframe or in the winter timeframe where we'll [assess] where we're at and partner on the way forward. So, right now the timeline is TBD. It is a long-term project. There's a lot of homework that we're doing behind the scenes, but we're not going to do it in the blind. We're going to be transparent with not only the field, but with the NISA working group as well.

Again, this is just a placeholder in case there's any questions at all as it relates to eMASS or our business processes or the DAPM please reach out to our generalized mailbox.

High-level metrics here. You'll see we have continued to reduce our overall footprint of systems. Going back a few years ago, we had over 6,000 systems. In partnership, really a quality assurance (QA) effort out of headquarters and in the field across all four regions, and of course Industry, really closing out that RMF process. When the contractual requirements for accessing classified had stopped, we wanted to make sure not only we disestablished the system, but we closed it out in our database of record. So we've done significant work and it used to have a high level of expired systems after going through all of those expired systems would really help us significantly lower our footprint, our portfolio of systems, at 4900.

Additionally, in partnership again with the NISA working group in some of the systems that we have out there, enterprisewide area networks, etc. we're able to come up with procedures for co-utilizing systems for different programs, ensuring isolation is appropriate. We provided guidance and those have also contributed to the reduction in systems and then some of the cloud as Mr. Spinnanger talked earlier. We really think as we move forward into additional cloud environments for Industry, there may be a further reduction of that portfolio.

As we talked about earlier, we're now able to track our timelines. DCSA is charged with, and I'm tasked with, providing assessment authorization decisions within 90 days. We're right now at 80+ days, but that includes Industry time. We're still within the goal of 90 days, but DCSA, what I'm being held to, is right around that 62 day time frame. We're monitoring that. I know that Mr. Sadler talked about Executive Orders and we have had a couple of losses in the ISSP workforce, but we have tools in our toolbox to manage that and we're monitoring that weekly.

Also, we have our CORA program, and a lot of them are former ISSPs. We are picking up the slack. The CORA team led by Mr. Vaughn has done an outstanding job partnering with our regional AOs and really offsetting where they need assistance. So you'll see them at security reviews and also picking up packages where we need fit. So we're doing the best we can. We're really grinding out there and they're doing a great job.

Speaking of CORAs, we are on track for 45 CORAs this year. We don't see any interruptions there and we're planning for 60 next year. I also want to footstomp that the schedules are posted pretty much a year out. If you need assistance with finding that schedule, if you want to see if you're on there, I highly [recommend] look at it now. Additionally, we're really seeing success when Industry reaches out early and often as it relates to the CORA, because the test is given out by the cyber leads. So, please reach out early and often. Where we see we're having some hiccups, or some really bad scores, it's when Industry is not reaching out or getting clarity on those requirements.

The DAPM, it's going to be the DAAG, the DCSA Assessment Authorization Guide. We're in the process of setting a CADM tasker out here in the coming weeks to start that formal coordination process. We've again kudos to the NISA working group through Mr. Sadler and actually all the industry representatives. We got a lot of good feedback and we incorporated all those comments within the past year and now we're looking to press forward with a formal coordination with DOD representation and we're really hoping to get that out as soon as possible because that document gets us out to updated all the CNSS guidance and policy that's been put out in the last couple years.Okay, that's all I have. Thank you.

Greg Sadler, Industry: On the DAAG. I mean, is there another group within this audience that can help either prioritize that or push that forward so that it does get released? It's been two years since Industry’s review, things of that nature. We know it's not in your direct lap to push that over the finish line, but how can we help elevate that to get it moving? I'm being selfish from NISA work forums like this.

Jeff Spinnanger, DOD: Yes. I'm happy to jump on that land mine. When issued, and testament to DCSA, right, to cover down on those 5,000 or so systems. That's great. That's about half the Industry equation. And so what we directed from my office was to level the bubble for those other 5,000 or so systems out there that are under DOD cognizance, but not under DCSA cognizance, so for the guide, and the acronym doesn't roll off the tongue like DAAG. But nonetheless, there is guidance out there all tied to the same 853, all with similar, but not entirely the same words. So what we want to do here is to invite and direct coordination by those other authorizers so, one to level the field for what DCSA does, but then to incentivize future conversation for why are they different. Because the end result is moderate, or words to that effect right, and so the pathway shouldn't be all that different, because interoperability is a thing. So we're going to move that pretty fast so when DCSA puts it in, we will use what we call the defense security enterprise to put some expedience to that.

I don't think we'll ask for a lot of coordination. Most of the services, the first thing they do whenever they get a coordination requirement like this is they ask for an extension. We will politely decline. I'm confident that we'll be able to report this in a done category before this body meets again and maybe cut that timeframe in half. So we'll put ourselves on the clock for sort of an end of July update and we'll take it from there.

Michael Thomas, ISOO: Thank you, sir. Other questions?

(No questions raised)

Michael Thomas, ISOO: Alright. Thank you Mr. Scott.

Jennifer May, ISOO: Thank you, David. We're now going to hear from Ms. Donna McLeod, the Senior Policy Adviser of Personal Security for DCSA for their statistics. Donna?

Donna McLeod, DCSA: Thank you. I'm here today to give the updated metrics for personal security, and that includes background investigations, and AVS adjudication vetting services. So, as Director Cattler mentioned earlier, our inventory stands at about 222,000 cases and it has decreased nearly every week in 2025 after peaking over 291,000 cases early in 2025. The inventory has dropped nearly 70,000 cases, a 24% drop. For DOD Industry, inventory for tiered investigation stands at about 33,000 cases, marking a decrease of over 6,000 cases, 17% in the FY. Current inventory consists of 19,000 tier five investigations and 14,000 tier three investigations.

The things that have been happening to help decrease the inventory. We've talked about FBI and some of our delays in getting responses from the FBI. So, we continue to work with FBI regarding our name checks. For over a year, DCSA has experienced increasing delays in receiving FBI name checks due to competing priorities for FBI on the name checks. FBI implemented a new prioritization tool last September which has led to aiding the backlog of cases only awaiting the name check. This population was reduced from 42,000 to 20,000, a 48% decrease in Q2. Progress slowed over the past few weeks due to staffing changes at the FBI enterprise vetting center, but is expected to continue decreasing during Q3.

Currently, 11% of the total investigation inventories are awaiting the FBI name check. We've also increased the use of virtual interviews. We are using virtual interviews where it makes sense to do virtual interviews. So, for the last four months, we have had an increase of 75% of all interviews being done virtually. It's up from 50% of what we were doing last April. We're using overtime where we can. Overtime for federal investigators has increased to 3% from FY24. In addition, our quality review staff are also working overtime. We also implemented an expedited review process in our quality review where cases that are lower level investigations, T1, T2, and T3, that do not have major issues, those cases go through a modified review process.

And then we're also capitalizing on the early implementation of the trusted workforce 2.0 standards. Most recently, the executive agents issue policy guidance where we can adopt some of the trusted workforce 2.0 policies. And so we're looking at how we can adopt those and address the inventory as well. And the director also mentioned the tiger team and the work that's being done through that effort to identify where we can increase our throughput and our demand. And we're in the transitioning phase for the tiger team for all solutions across personnel vetting.

On to the adjudication and vetting services. When we talk about end-to-end timeliness, 19 days initiation time, 215 days investigation time, and 9 days adjudication will give us a total of 243 days end-to-end time. That's on the slide. For our T3 initials through April: 18 days initiation, 73 days investigation, and 47 days adjudication, which gives us a total of 138 total end-to-end time. Investigation timeliness is expected to decrease as the inventory reduction efforts continue, but please keep in mind as we continue to close those older cases, the overall timeliness will increase. So the inventory is coming down but we're addressing some of the older cases. 90% of all initial investigations had an interim determination made on an average of 7 to 10 days. Adjudication inventory, T5, is at 1300 cases, and T3 is at 2300. And that's all the metrics. Thank you.

Michael Thomas, ISOO: Great. Thanks very much. Any questions?

Greg Sadler, Industry: Ms. Donna, real quick question. Greg Sadler from Industry. That use of overtime to help keep the inventory down. Is that having any material effect on the cost of the investigation to the user agencies?

Donna McLeod, DCSA: No, because our cost is already projected out and already published what the cost is long-term. I'm quite sure our finance group will look at and reassess if there will be a long-term impact, but the immediate impact is no, because those costs are already out there.

Greg Sadler, Industry: Alright. Thank you.

Michael Thomas, ISOO: Any other questions?

(No questions raised)

Jennifer May, ISOO: Thank you, Donna. Now we're going to hear from Mr. Perry Russell Hunter, the Director of the Defense Office of Hearings and Appeals, also known as DOHA.

Perry Russell-Hunter, DOHA: So, five things I did last week. [Laughter] That exercise, especially the way we did it in DOD, with each employee copying their supervisor when they submitted that, was a real exercise in remembering the diligence and care and hard work that goes into one of these personnel security cases.

The Secretary of Defense recently talked at a meeting with some special forces folks about the importance of humans as well as hardware. We do the human part at DOHA. DOHA is the federal government's independent agency for reviewing and providing administrative due process, fair and independent hearings, and fair and independent appeals. By doing so, we ensure consistency across Industry because we handle not only the DOD contractors, but also the contractors for 32 other Federal Departments and Agencies.

I want to echo something that David Cattler said earlier which is that, while we each have distinct functions, we don't do any of this alone. Together, everybody in this room, and everybody at this table works to ensure the defense of our nation and the proper treatment of the people who volunteer their time and sacrifice to support that shared effort.

As I look around this table, I see Charlie Sowell, who was involved in the last time we updated SEAD-4. And what I was very pleased to see from the briefing from ODNI was that they're following a process that we proved worked in creating a strong and durable set of adjudicative guidelines. That was a number of years after the 1995 Executive Order that required common adjudicative guidelines. We did finally get it done in 2017. We're ready to do that again and I volunteered Doha to help as we did last time.

Also looking around this table I see somebody who helped me make a good and complete record for the government in several security clearance cases back about 30 years ago. I'm not going to say her name. But I realize that this is a reminder of how much our efforts are shared.

So with that said, the good news from DOHA is that we are now doing more than 85% of our hearings virtually using Teams. So, like Donna and DCSA, we've managed to leverage that technology to get cases done faster, which means that we're getting to hearings faster. We have less than 300 cases pending hearing right now. We have less than a 100 cases pending a non-hearing decision.

Our statement of reasons workload, which is really the front end and this is the important part because it's the notice to Industry contractors, the notice of what the government's concerns are. And one of the great protections of the Industry process is that you can't lose your eligibility, or have your eligibility denied, without receiving a set of enumerated protections, which include a statement of reasons that's as detailed and comprehensive as the national security will allow and the opportunity to appear personally in a hearing, and the opportunity to appeal to an independent appeal panel. But it starts with actually knowing what the government's concern is. And so those statements of reasons, we have a steady workflow.

In fact, over the last several years, we have had a steady workflow of about 2,000 statements of reasons reviewed per year. We are timely on those. So far this fiscal year, 2025, we've performed about 1,100 almost 1,200 legal reviews of statements of reasons. That ensures that what the government's putting out is actually accurate and legally sustainable. Because before we're going to make somebody worry about losing their job, we're going to make sure that we're right about it. So, that's one of the, again, nice protections about the Industry process. But the fact that we're timely on that is also important because it means we're getting the word out to you and your employees, sooner rather than later, about what the concerns are.

We're also accessible. One of my five things was always responding to Industry inquiries. My telephone number is 703-696-4751. That line rings on my desk. I answer it. I'll give you answers. I'm proud of what we do at DOHA. I'm grateful for the time. I'll take any questions you have.

Michael Thomas, ISOO: Any questions?

(No questions raised)

Michael Thomas, ISOO: Alright, thank you sir.

Jennifer May, ISOO: Up next is David Means from ISOO to provide an update on controlled unclassified information (CUI) program.

David Means, ISOO: Good afternoon. I'm David Means, I'm the lead for the ISOO CUI program, and at this point, I no longer need the introduction. I think CUI has been mentioned, I've been keeping a tally in my green book, I think we're at 15 times now so far today. One thing I will say before I get started, I do want to say thank you to the NISPPAC, Ike, for inviting me here to the table. It's everybody's favorite topic. I do appreciate the opportunity to come and speak on this very briefly and look forward to future engagement.

On policy. Jen actually addressed this earlier; spoke on kind of where we are in terms of policy updates. So, I won't deal with that. The only other thing on here, NISP 800-171. I'm also going to leave that alone. We've got our cyber lead back here, Larry. He tries to keep me straight on all things that plug into the wall. But I'm a retired Marine, so I'll be honest. That's still a challenge area for me. So I'm going to leave that alone as well. We can go and breeze past that.

Alright, contracts. I'm not going to belabor this. But what I will say is this. Looking at the data, and kind of the communication that we receive from Industry. I just want to put out there that in your contract, these are the areas that should be addressed. I get questions a lot coming to the CUI box about how do I handle this? I'm at agency A. What do I do with this information? Same with challenges. I've got information, I think it should be CUI or maybe it's not. What I will say is this: ISOO remains here. We are a resource to help you. But I want to encourage you to please go back and take a look at the contract. This is information that the government at that agency will provide to you. I'm not in a position to give an answer on your particular contract. So if this information is not there, please go back to the government to request this information and go from there.

Speaking of which, the program structure. I will always encourage, again, ISOO is here as a resource, here to support, but please go through your contracting officer, your COR. Ultimately, that is the relationship that you have with the government. And then too, don't forget about that agency CUI program manager. Alright, that agency CUI program manager, they're the ones that are looking at that agency CUI policy and they can speak most directly to how it's going to impact your agency. If there's any need to figure out who your CUI program manager is, please reach out to me and we can get that squared away.

And last, but by no means least, I put this up here: cui@nara.gov. Again, we are a resource. One other thing I do want to put out there is this: the NISPPAC is also a resource. If there are questions about CUI, I think it was mentioned earlier about TOP SECRET CUI. Never heard of that, but I would say please utilize the NISPPAC as a resource. The NISPAC has come across and they deal with all the different issues in Industry and they may be able to provide a quicker answer and again they're kind of seeing things like this. So things like TOP SECRET CUI, they can very quickly say no, that's not a thing, or provide you a resource that may take me, I might have to do some more investigating on something they've already figured out. So I do appreciate that.

Last and by no means least, just to reiterate kind of what Michael said, he mentioned earlier, he made a musical reference and talked about lacing up our shoes and running. I will say I'm committed to that, although I think the only thing in my playlist is Eye of the Tiger. About the only song I have. But with that, I remain committed to the program and to being here to assist. That's all I have unless there are any questions.

Michael Thomas, ISOO: Questions for David from the room? We have a couple from the chat,. let's go to those, David. So, maybe we can tag team these because some are actually directed to ISOO. I didn't know they could direct us questions. I thought it was just all of you. I got to check the bylaws.

So we had a question earlier in the day about the need to modernize EO 12829, which we've talked about in various aspects and the question is, what specific actions is ISOO taking to ensure that CUI is formally incorporated into any future update of the EO? and to some extent what's the timeline?

So when it comes to the timelines for an EO that's really on somebody else's desk. You may have noticed David's slide earlier with the org chart that goes from the President downward. That is where we take our policy direction. What we can do is make sure that we are armed with the insights that you offer us about where you're finding challenges and from what level in the system. Be at the EO [level], the reg, agency guidance, where we can fix those problems.

Jeff referenced earlier that some things are really close to home as opposed to being up at the top level in an EO. And so there's different places that we can engage and I think along with that I think from the question of being integrated I think you see CUI is already integrated into this conversation and one of the benefits of having ISOO postured in the way that it is with folks like David involved is that serving as the executive agent for the EO as well as with our role with the NISP, we have an opportunity to provide a forum for an integrated conversation as opposed to the ones that might happen in other forums. So we'd like to ask you, as we look forward to the opportunity to reform, we roll those conversations up into a dialogue that we can capture and address our formal responsibilities to make the relevant recommendations. David, do you have any particular thoughts on the integration of CUI into the NISP review process? Have you had questions like that from Industry to the inbox, so to speak?

David Means, ISOO: I have and while I think the reality is that even though the EO could be updated and incorporated, it's the reality. I do get a lot of questions of: "how do we address this formally?" Even though it's technically seen as separate. So it definitely comes in and I think that there's some opportunity to kind of close the gap.

Michael Thomas, ISOO: That's great. Further questions?

(No further questions)

Michael Thomas, ISOO: Alright, thank you, David.

Jennifer May, ISOO: We're now going to hear from Stacy Bostjanick, the Director of the Information and Acquisition Protection Directorate for the Office of the Undersecretary of Defense for Intelligence and Security, who will give us an update on the cybersecurity maturity model certification, otherwise known as CMMC. Stacy?

Stacy Bostjanick, DOD: I do recognize I'm standing between you guys and the door. So, we'll try to make sure I'm quick here. I'm going to deviate just a little bit, but let's go to the Next slide. I'm hoping most of you know why we established CMMC. Back in the day, we did an inspector general (IG) investigation, Navy cyber readiness review, and found that companies that were supposed to be compliant had basically said they were compliant, and they really weren't. We had DCMA go out and do some assessments. Companies had POAMs that weren't going to even be addressing all 110 till 2099. I'll be dead by then. So, that didn't really help us too much, So we had to establish a means to validate that companies were meeting the required standards that were set forth in the 252.204-712 clause, which calls out the NIST 800-171 for handling of controlled unclassified information.

So we set up an ecosystem, because we recognized that DCMA was never going to be resourced to handle all of the companies within the DIB. And so, we stood up an independent third-party ecosystem that has third-party assessors out in Industry with the cyber accreditation body today doing all of the accreditation with regard to the ISO standards. So, we tried to build integrity into the process. We have a code of conduct that the assessors must meet and we have requirements for them as well. They must attain a tier three suitability determination, because it's viewed as a position of public trust and I have to thank Mr. Spinnanger for helping me with that. We did have a few arguments where I finally said I'm just going to go with a commercial background if y'all don't help me. And so he stepped in and helped us get that set up.

So, how many companies are compliant with CMMC today? We have probably 300 or 400 companies that have gone through an assessment of some type. But, out of the 220,000 companies, that's not nearly enough. All right, let's go to the next slide.

Okay. So today we have the DFARs clause 252.204-712 that I already spoke about. And when we started CMMC, we started with a 48 CFR rule making back in 2020. At that time we also had the 7019 and 7020 clause. 7019 is a provision that makes companies do a self- assessment in the supplier performance risk system before they can submit a proposal to give us an indication, a self- assessment, of where they think they are in compliance. And then we had the 7020 clause because, prior to that, we really didn't have a legal way if we knocked on the door and said, "Hey, we need to come in and do an assessment to get in there." This gives DCMA the right that if I come to your company and I ask you to please give me access to do an over-the-shoulder assessment, you must.

Okay. This is where I'm going to deviate a little bit. We're going to talk about CUI because I've heard a lot of complaints over the years from companies. We don't even know we have CUI. People don't even mark it. What is CUI? So David, I should bring him back up here and make him help me on this, right? Because we have contractor-derived data and we have program-derived data that rises to a level that needs to be considered and protected. Let's go to the next slide and see if I have my data descriptions there. We don't. So, it'll probably be the next clause. We have federal contract information, which is the information that companies have and handle, which would be the proprietary parts of your proposal, the account information. I don't know how many people have been tracking. It's a little dated now, but we were having significant issues with cage code problems, the hopping, skipping, jumping, right? So people weren't cyber secure and our friendly hackers were getting in redirecting their payments. We get calls like, "Hey, when are you guys going to pay me?" And we're like, "We didn't." They were like, "No, you didn't." We're like, " yeah, we did." And so you go back and you look and they had redirected the payment to their bank account. And sadly for most of the contractors, DOD doesn't have another $40,000, $50,000, $60,000, $100,000 to make them whole for the money that they just lost. And who do they go to? DOJ. What are they going to say when you say, "Hey man, I lost my $100,000." They're going to say, "We don't have time for that. That's a little too small for us." so y'all figure it out.

So it's very important that companies become cyber secure and they meet the basic standards of the NIST 800-171. I am no cyber geek, but I have been told that it is really basic. That's not the exquisite protection. That's the basic stuff you need to do. Somebody equated it to what you need to do to keep your neighbors out of your Netflix right.

So today we have the DFARs clause 252.204-7021 that is going through the rule making process. In December of 2024, we issued the 32 CFR rule and I don't know how familiar you guys are with our sorted past. We started with the 48 rule. The Biden administration came in and said, "Hey, we want to revalidate this program, make sure it's doing what it's supposed to do." And so we took a pause and they came back and went: “we forgot to tell you you need to do a 32 rule making along with that 48.” So my team turned to and we published that 32 CFR which is the programmatic rule which explains the program down to the nitnoid because I know all of you have already read my 400 page rule right, you guys have it memorized right, on page 60.

So the 48 CFR will follow the 32 and it has gone through public comment. Last I heard it was finishing its formatting with the DAR council and will hopefully be returned to OMBOIR to finish the second half of the rulemaking process. Now, we also have all heard today about some of the exquisite EOs that have been out there and a lot of them are thought to have implications. If you look at LinkedIn, there are people that are screaming CMMC's dead. It's not. Sorry, but it's going to prevail. It started under the first Trump administration and it will stay. And we've had a couple of meetings with OMBOIR. We have another one tomorrow and they think we meet the exemption rules. So don't write that down because he may change his mind tomorrow. But yes, when we went last time, he said he thought we meant the exemptions.

Okay. So I'm not going to read you this slide. You understand what this means. Can you go to the next slide?

What is CUI and what are the levels? CMMC brings a level of specificity to CUI and we have, if you haven't gone out and looked on our CIO website, a leveling memo. What we have said is for federal contract information which was that what I described before is your cage code that kind of stuff you have to meet the 15 requirements that are in the 52204-21 clause which, actually somebody said might get killed in the 10 for one thing, but it's incorporated in the NIST 800-171. So it will live in infamy in the NISP standard so that is what you do for that SCI.

Then CMMC level two is for basic CUI and we bifurcated it in the rule meaning that if a company handles controlled unclassified information that may not be of particular interest to DOD, and I characterize it as I think you guys have one category that's historical archaeological data right, so that might not be something that we would not be particularly concerned about making sure it had a third party assessment against it. So that a company would be allowed to continue to do a self assessment, but it will be under the rules of the CMMC program meaning you have to compose your POAMs within 180 days, and you have to do your annual affirmations that you're compliant.

So, what would happen if you did an annual affirmation and you were doing the wink, wink, nod, nod “yep. I'm in compliance”. If we realize that, you could be liable under the False Claims Act and the DOJ has ramped up their compliance with that fine regulation and they have been pursuing that.

Now, CMMC level two. If you look at that leveling memo that we put out there, that's CUI that is on the DOD's CUI list of the CUI that we're concerned with. And then level three, which will equate to the NIST 800-172 requirement, and we've chosen a baseline of 24 requirements out of that for contractors to have to meet to be awarded a contract at level three. That is what we would consider our critical programs and technology. Now, R&E is helping me out because they've changed what they call contractor derived information. I think it's contract program information. So some of the definitions are going to change and I know you guys are familiar with the fact that NIST has already issued Rev 3 to the NIST 800-171. So it's job security for my rulemaking team because OMBOIR did require us to tie ourselves to a revision in the basic program rule. So now we're going to have to do a rulemaking effort to inculcate Rev 3. And guess what? They're working on Rev 3 for the 172. So as soon as I finish the rule making for the Rev 3 for the 171, I'll start the rule making for the Rev 3 for the 172.

Now companies and contractors have asked when do I have to be Rev 3 compliant? So what we've done is we have a transition because I know you guys all read that 400 page rule and you know that there's a phased roll-out right. So what we've said is year one what we anticipate is the Department will still focus on self-assessments for companies. Second year, we'll start seeing more of the certifications required in RFPs.

Now our roll out gave us an out and said, if a program manager feels that their program is important enough that it needs a certification year one, then they can do so. Army has already issued an RFI informing Industry that they intend to issue a RFP this summer. It has a CMMC certification requirement. So, year two, you're going to see that in all contracts for level two.

Year three will be where we'll start doing the tier three assessments. Those will be performed by the DCMA DIBCAC and then by year four it'll be full incorporation.

Alright. Now if a company today says man I am not going to be bothered with rev 2 if I'm going for it I'm going for the whole enchilada. I want rev 3. We are working on a transitionary instruction for the assessors that said hey you're doing an assessment of rev 2 because of the rule but you can look at it in a rev 3 environment. All right go to the next slide because I know I'm keeping you guys too long here.

Alright. One of the areas that we've gotten a lot of conversation about is we do have international partners. Now, you guys all recognize that the CUI has a flow down requirement. So, if you have subcontractors, you are going to have to understand what you're passing to your subcontractors and you're going to have to ensure that they meet the requirements to be able to receive that data. So, that brings a whole another level to David's CUI that we've got to figure out, right? Because you're going to have to disaggregate that data. You're going to have to understand that if you have a level 3 program, not all the data associated with that level 3 program is going to rise to level 3. So when you pass that down to your subcontractors, you're going to have a requirement to go, if I take this part away from it, then it drops to level 2.

One of the things that we have said is if you are a subcontractor of a level 3 program, then you will at a minimum need to be level 2 certified. Foreign partners, so, we do have some concerns. I know we've talked a lot about reciprocity today. Our rule does not allow for reciprocity with our international partners. We allow for integration because of the fact that, and I know my industry partners at the table will probably nod and agree with this, it doesn't make good business sense for me to have a more stringent requirement in the US and allow my international partners to have a less stringent requirement to participate. So we have to hold them to a consistent standard across the board. Everybody has to do the same thing. So they are going to have to meet the requirements of the CMMC CFR 32 parts 170 for CMMC. Let's go to the next slide and see what we got there.

Okay, so we've come up with a couple of COAs for our foreign partners. And I think I'm going to skip ahead because I think the pictures look better. Go to the next slide. There we go. I got my pictures. Alright. and I have an individual on my team that I had her brief this and she did so much better of a job. I've got to steal her style. Sorry for your love.

You see the little ball down there? It's got the people in it? So that's what represents our assessors today. And this is a picture of our entire ecosystem. Go to the next slide.

This is our CAICO. This is our training and certification arm. What this is when we talk about our international partners, the international assessors, they can take the same training, they can take the same examination and they will be able to do assessments. They will also have to have an equivalent tier 3 suitability determination in their country that we have a reciprocity with or, and I don't know if any of the people from DCSA have heard yet, but you guys will also help us do a tier 3 suitability determination for them, if they don't have one in their country. next slide.

Okay, so our first course of action for international partners is that some countries did not want US or foreign nationals to be able to do assessments in their country. They had a sovereignty concern. So let's just say maybe the UK had a sovereignty concern. So what they could do is they can have their nationals be trained and work under a USC3 PAO and then when a company in the UK says, "Hey, I need an assessment." They'll be able to go out to the CyberAB website, find those individuals that are UK nationals, pick them to go do that assessment and allow them access to those companies. Easy button for our international partners. This is what we are trying to foot stomp with them to move forward because it's the fastest way they can get there. The one thing I think with this is we do use and have an instantiation of EMASS for CMMC where all of the assessment documentation will be held. They will pass that assessment from their country through the PMO to be uploaded into that database. Next slide.

Okay. Course of action two. If they don't want to have their people working for a USC3PAO, they can establish their own C3PAO. They will have to work underneath our CyberAB because we in the program office have acknowledged the US CyberAB as our single point of contact for the accreditation. They will have to follow the accreditation process under that CyberAB and become accredited. Again, they will use nationals from that country to do that assessment and the assessment data will be passed through the PMO. And I was incorrect, in the first one, the C3PAO, if they're under a USC3PO they'll be able to put the information in eMASS. Go to the next [slide].

Okay and the third one, which is the most painful process, is they can also establish their own accreditation body. Then they would have to have an MRA or an MLA with our cyber AB. They would have to make an agreement for them to be able to work with them and partner with them to be able to process and do the accreditation of the C3PAOs in their country. All right, next slide.

And there we have it. Okay, I think I have explained it well enough, but I am open to questions. Unless you've all fallen asleep. I didn't hear any snoring in the background.

Michael Thomas, ISOO: Questions?

(No questions raised)

Michael Thomas, ISOO: Alright, thank you very much.

Stacy Bostjanick, DOD: Alright, everybody's ready to roll.

Jennifer May, ISOO: Thank you, Stacey. Before we move on to new business, Matt Roche from DCSA said he has a quick update.

Matt Roche, DCSA: Yes. In reference to the standard form 328, reporting on foreign ownership control or influence, there is an information paper that's circulating that covers material change and how those are defined and what meets that standard. So I just wanted to make sure that that made it out and if anyone is in need of that or if it hasn't been circulated, please contact myself or Mr. Ike Rivers. And lastly, my compliments to Jennifer in her tenure here. Well done. And thank you so much.

Jennifer May: Thank you.

Michael Thomas: Any questions?

(No questions raised)

Jennifer May, ISOO: Excellent. Thank you everybody for your time today. We're at the point of the meeting where we're going to ask the staff members to present any new business they have outside of what was already presented during the Industry portion earlier this morning. Any new business?

Michael Thomas, ISOO: Hearing no new business.

Jennifer May, ISOO: Excellent. As a reminder, all NISPPAC meeting announcements are posted on the Federal Register approximately 30 days prior to the meeting along with being posted on the ISOO blog. And at this time, I'd like to hand things over to Michael for closing remarks.

Michael Thomas, ISOO: Thanks. I'll give them here from the table since we're bringing this meeting to adjournment. As we do, you've heard a couple times today that this will be Jen May's last meeting with the NISPAC. She is retiring from a long career in federal service. We are sad to lose her from ISOO but Jen we really wish you well. We thank you for both your work with ISOO and your long tenure and career for the government. As she departs, Heather Harris Pagan, who many of you know, will be stepping into the DFO role with the NISPPAC and then Ben Rogers will be stepping into the ADFO role. So Ben has been our man in the booth today taking care of everyone in the chat doing a great job.

Thank you all for your contributions to the meeting today and I hope if you haven't met them already that you'll take some time before you rush out of here this afternoon to connect with Jen, with Heather, and with Ben. And last thing, I promise, is for our NISPPAC members, for our speakers, please, follow me back to my office for a few minutes so we can say goodbye to Jen together. I'd like to have you join us for just a few minutes.

Hearing no final words, does anyone have anything else they'd like to say about CUI before we go? If not, we'll consider this meeting adjourned. And thank you for your time today.