NISPPAC Meeting Transcript

September 2, 2026

Michael Thomas: Thank you everybody for being here today. Welcome to the stately McGowan Theater and the 76th meeting of the National Industrial Security Program Policy Advisory Committee. My name is Michael Thomas. I'm the Director of the Information Security Oversight Office and I have the honor of being your host today and serving as our Chair.

For over three decades, the NISPPAC has served as a critical bridge between our Government, and the elements of American Industry that provide the methods and means - the critical innovations and the commercial infrastructure that help guarantee the continuing security of our nation. Each time we gather here for a meeting of the NISPPAC, I aim to use these opening moments to situate this shared mission in its wider historical context. We are at the National Archives, after all. I see it as a chance, every time for me to learn, to pay my respects, and to share with you how I see your work, and I hope that in that you all really do feel seen and that you feel proud of what we're striving for together: a single, integrated, cohesive, industrial security program, protecting classified information while preserving our nation's economic and technological interests without redundant, overlapping, or unnecessary requirements that would impede those interests with security based on actual risk rather than the disjointed accumulation of bureaucratic cruft…security requirements that are duplicative and yet somehow also contradictory, the sort of requirements that focus on near absolute risk avoidance for a very specific set of circumstances rather than serving reasonable and holistic risk management. This is, for Government, I grant you, a pretty audacious goal. In fact, my long ago predecessor, former ISOO Director, Bill Leonard, once said that "in Government, anything that is intended to be integrated and cohesive is not easily achieved, and once achieved, not easily preserved", which is exactly why this forum, the NISPPAC, remains so vital.

The National Industrial Security Program was born as a post-cold war Government reform project. William Perry, Deputy Secretary of Defense under President H.W. Bush acknowledged that, with the fall of the Soviet Union, "we should be able to dismantle a significant part of this big, complex, expensive apparatus…" At the same time in 1993, they could not have predicted the Global War on Terror to come, much less a new wave of international authoritarianism, or the return of great power competition. The impact of new electronic capabilities for espionage, cyber warfare, drone weaponization, the tidal wave of AI adoption, or the power of quantum computing to throw all our accepted security norms into disarray, and these dramatic shifts over the ensuing decades make our continued attention to the NISP mission more important than ever. Time and again, we've seen how our Government turns to Industry to address emerging gaps arising from the ever-changing landscape of threats and opportunities that shape the contours of our national security, and the federal Government found itself in a moment almost exactly like this one in 1917. We found ourselves confronted by international conflict, amongst great powers following on the heels of a global pandemic. This was a conflict in large part defined by the emergence of new military and intelligence technologies and the need to think about the battlefield in new ways. In January of 1917, our British allies intercepted and decoded a telegram from the German Foreign Secretary, Arthur Zimmermann, which, shockingly, proposed a military alliance between Germany and Mexico against the United States, offering up Texas, New Mexico, and Arizona, if Mexico came over the German imperialist cause in the ongoing war in Europe. This was the tipping point, catalyzing American public

opinion against Germany, bringing the United States militarily into World War I, but there was a major problem, and the incident of the Zimmermann telegram called it out starkly. The United States, in 1917, completely lacked the technical capability to intercept, and decode, German transmissions the way the British had. Nor, at that time, did we have the ability to protect our own communications from similar exploitation. Literally not one federal department was engaged in cryptographic activities, which had been almost entirely neglected since the end of the American Civil War, 60 years earlier. As it happens, telegraphic communication was the backbone of the Union strategic command, giving them a decisive edge in helping them win the war. Both sides, the Union and the Confederacy, use the telegraph, But only the Union was able to centralize its command while maintaining near-absolute operational security. They accomplishED this by successfully industrializing the technology. They created a dedicated civilian military/hybrid organization, the U.S. Military Telegraph Corps. It laid over 15,000 miles of wartime cable, employed over 12,000 telegraphers, and transmitted more than 6.5 million messages. Would you be surprised to know that not a single one of those messages was decoded by the Confederacy during the entire war? And you want to talk about a situation room? Let me talk to you about the situation in the War Department telegraph office, where President Abraham Lincoln spent countless hours coordinating the Union's multi-theater battle strategy. Incredible…and completely abandoned in that window between healing this historic breach in our history and America's emergence as a global power.

In the meantime, from the telegraph, to the radio, to trans-oceanic cables, by 1917 there was both an enormous new intelligence gathering opportunity, as well as an absolutely terrifying new attack service for which we as a nation were fully unprepared. And there was only one answer, one place for America to turn. That was to the theater…or more specifically to the plays of William Shakespeare.

Let me explain. It starts all the way back in the late 1500s, with a conspiracy. Some of you of more literary-minded friends may already know this, but some claim that William Shakespeare was not in fact the author of the famous plays that bare his name, Hamlet, MacBeth, Romeo and Juliet. These conspiracists – these Anti-Stratfordians are checking in right now. They claimed that there are clues to the true author of Shakespear's plays to be found in the plays themselves. Secret messages, waiting to be decoded. Enter George Fabyan. Fabyan was a midwestern textile magnate and the sort of turn-of-the-century Tony Stark, complete with epic facial hair, and he counted himself amongst these Anti-Stratfordians, fingering Sir Francis Bacon as the true Bard, and he set about trying to prove it.

At Fabyan's pioneering Riverbank Labs facility, built in 1913 on 300 acres an hour outside of Chicago, he assembled a team and they went to work on his pet theory. Now, let me say, this was far from the weirdest thing going on at Riverbank Labs. Fabyan was also interested in experimenting with the healing powers of musical harmonics and the grounds were littered with all sorts of novelties: a windmill, a lighthouse, Japanese gardens, a grotto, greenhouses, a zoo, a farm, and a villa designed by Frank Lloyd Wright.

Amongst Fabyan's early recruits was Elisabeth Friedman, who was at the time a 24-year-old multilingual expert in the classics, who had last worked as a substitute principal in Wabash, Indiana. At the time Fabyan rolled up in his black limousine to sell her on life at Riverbank, Elizabeth was jobless, having quit the school and returned home to live with her parents. You got to think

joining his sort of particularly bookish avengers was an easy yes at that point.

In the course of her research at Riverbank, exploring this Bacon/Shakespeare theory, Elisabeth, with no formal training and with only pen, paper, and her substantial intellect as her tools, she became one of the foremost cryptographic experts in the entire world. And with the onset of World War I, the U.S. Government came calling with their particular problem. They had nobody like Elizabeth Friedman. And Riverbank Labs "Department of Cypress" was formed to aid in the war effort. Now, Elisabeth eventually went to work for the War Department directly, later still, she led Coast Guard efforts to bust rum runners during prohibition, cracking some 12,000 messages from smuggling rings, gathering the evidence that was ultimately used to indict Al Capone. In fact, she was the most prominent cryptanalyst in the world during the interwar period, due to her testimony in these many high-profile cases. And her service continued into World War II, where she led a clandestine unit that broke the complex Axis and Enigma-derived ciphers, neutralizing Nazi spy rings in South America. These contributions remained classified until 2008, although J. Edgar Hoover was happy to take credit back in the 1940s for the FBI.

Elisabeth, was in a word, extraordinary. And along with her husband, William, the Friedmans, mentored a generation of cryptanalysts, becoming the mother and father of America's cryptographic capabilities, and modern signals intelligence. And it all began at a private research facility, with the Government sharing its most sensitive information, in the interest of solving technical challenges that the Government could not solve on its own.

Freidman passed away in 1980 and we sit here today, barely one working life beyond her legacy. A legacy that might never have existed without the partnership between the Government and the private sector at Riverbank Labs. This is a good time to mention that George Fabyan offered his services to the Government for free. Being a Tony Stark-style millionaire, playboy, philanthropist, has its perks, I guess.

Once again, we sit at the unnerving precipice of challenging questions about how our Government will be able to field the capabilities it will need to deter or defeat a new array of global antagonists and adversaries, and that brings us to the present day and the work ahead. We have been diligently seeking to adapt, not just our military and intelligence capabilities, but the NISP itself, to a new global threat environment that demands new ways of doing business. This 76th meeting of the NISPPAC, I am confident, will carry us further down that road. And I look forward to the comments from both Industry and Government today, and the conversation that ensues, which will further flesh out both the journey ahead and the destination that it's leading us towards.

Thank you. And let's get started.

Heather Harris Pagán: Thank you Michael. Good morning everyone. I'm Heather Harris Pagán, the Designated Federal Officer for the NISPPAC. Before we begin, I want to thank the volunteers for their work today in making today's meeting possible. Thank you.

For those in the theater, please take a moment now to silence all mobile devices. We have restrooms located outside the theater. When exiting the theater, the men's room is to the left, and the women's room is to the right.

Food and drinks (except water) are not permitted in the theater, but we do have a cafe to the left when exiting the theater for food and drinks during the break. In the event of an emergency, please go out the way you came in and exit the building immediately. Please use the microphone on the stand towards the front middle if you have questions. For the NISPPAC members on stage, this is a reminder that your microphones cannot be muted or unmuted manually, so please avoid sidebar conversations.

All NISPPAC meeting announcements are posted in the Federal Register approximately 30 days before the meeting, along with being posted to the ISOO blog. Today's meeting is being recorded and will be available on the ISOO website within 90 days, along with the slides and meeting minutes. To help our record-keeping, if you are virtual, and your name is not visible through Zoom for Gov, please email your name to nisppac@nara.gov for our attendance records. This includes those watching live on YouTube and those calling in on the phone.

For questions, we prefer for our virtual attendees email at nisppac@nara.gov or utilize the Zoom for Gov chat. If you are on the phone and cannot email, press *9 to raise your hand and *6 to unmute as a last resort please. For speakers, if you are in person, please use the podium and advance your own slides. If you are a virtual speaker, simply say "next slide" to our team. Please note all audio connections via telephone and computer should be muted when not speaking.

We have scheduled a 20 minute break at the halfway point. A reminder to our Government members: please ensure your financial disclosure is on file with NARA's Office of General Counsel. This is an annual requirement for your service to this committee. If you require technical assistance, please send an email to nisppac@nara.gov. We will now begin the roll call. When I call your agency or name, please state your name for the record. Department of War?

Jeffrey Spinnanger: Jeff Spinnanger.

Heather: Office of the Director of National Intelligence?

Lisa Perez: Present, Lisa Perez.

Heather: Thank you, Lisa. Department of Homeland Security? Alright, no one from DHS? Department of Energy?

Monica Marks: Monica Marks.

Heather: Thank you. Nuclear Regulatory Commission?

Michael England: This is Mike England from the Nuclear Regulatory Commission.

Heather: Thank you, Mike. The Defense Counterintelligence and Security Agency?

Allyson Renzella: Allyson Renzella.

Heather: Thank you, Allyson. Central Intelligence Agency?

Don: This is Don with CIA.

Heather: Thank you, Don. Department of Commerce?

Daniel Boling: This is Daniel Boling with the Department of Commerce.

Heather: Thank you, Dan. Department of Justice? No Department of Justice?

Glenn Bensley: Glenn Bensley, Department of Justice, and Lori Ellison.

Heather: Thank you. National Aeronautics and Space Administration?

Vaughn Simon: This is Vaughn Simon for NASA.

Heather: Thank you, Vaughn. National Security Agency? No NSA? Department of the Air Force?

Andrianna Backus: Annie Backhus.

Heather: Thank you, Annie. Department of the Army?

Laura Aghdam: Laura Aghdam.

Heather: Thank you, Laura. Department of the Navy?

Jason Steinour: Good morning, this is Jason Steinour. I'm joined by Dr. Andrew Jones and Robin Nickel.

Heather: Thank you. Department of State?

Kim Colón: Kim Colón.

Heather: Thank you, Kim. Thank you. I'll now move on to the Industry members. Isaiah Rivers?

Isaiah Rivers: Present.

Heather: Thank you, Ike. Jane Dinkel?

Jane Dinkel: Present.

Heather: Thank you, Jane. Katherine Andrews?

Katherine Andrews: I'm online.

Heather: Thank you, Kathy. Christopher Stolkey?

Christopher Stolkey: Present.

Heather: Thank you, Chris. LaToya Coleman?

LaToya Coleman: Present.

Heather Thank you, LaToya. Charles Sowell?

Charles Sowell: Present.

Heather: Thank you, Charlie. Leonard Moss?

Leonard Moss: Present.

Heather: Thank you, Leonard. Jennie Hardy?

Jennie Hardy: Present.

Heather: Thank you. I'll now take the roll call for speakers. Thomas Giancoli? Tom, are you there? Tracy Brown?

Tracy Brown: Present.

Heather: Thank you, Tracy. Perry Russell-Hunter? If anyone else is speaking during the NISPPAC that we have not heard from, or we don't know about, please speak now. We request that everyone identify themselves by name and agency, if applicable, before speaking each time, for the record. We have had a few changes to the NISPPAC membership. Mr. Robert McRae departed DHS. Ms. Breanna Palmer will remain the alternate for DHS. Mr. Daniel Boling has been designated as the alternate for Commerce. Mr. Steve Barbieri remains the primary for Commerce at this time. Mr. John Voorhees is no longer the primary for the Air Force. Ms. Annie Backhus is still the alternate. Ms. Robin Nickel has been added as an alternate for the Navy. There has been no change to the primary or other alternate for the Navy. This is also the last public meeting for a few members. Mr. Jeff Spinnanger, the Department of War member, is set to retire next month. He held off on retirement just for this meeting, so thank you Sir! I'm just kidding, they won't let him go. This is also the last public meeting for two of our Industry members, Ms. Jane Dinkel and Mr. Ike Rivers, who is also our Industry Spokesperson. Jeff, Jane, Ike, thank you so much for your contributions over the years to the NISP and security mission as NISPPAC members. The new Industry members will be announced at the next public meeting, along with the new Industry Spokesperson. For all of the departed members, thank you for your contributions over the years. We look forward to continuing the work you have done with the new representatives.

The last NISPPAC public meeting was held March 18, 2026. The minutes from that meeting were certified to be true and correct, and were finalized by Michael Thomas on June 16, 2026 and posted to the ISOO website on that same day.

I will now address the items of interest from that meeting. The Department of War asked ISOO to assist in engaging with the Small Business Administration regarding military departments' ability to meet small business requirements. This is still open.

Industry asked OUSWI&S to work with the military departments to expand the SCI Indoctrination authority for Industry, and work with them for a better process moving forward. This action item is still considered open.

Industry requested cooperation from Government entities in devising sanitization procedures for solid state drives involved in spills. This item is still considered open.

Industry requested that ISOO coordinate with the CSAs to provide guidance to Industry on all Executive Orders with suspected NISP implications. This item has evolved, and is currently with NISPPAC Industry to help ISOO focus in on their priorities.

Industry requested that ISOO convene a meeting of the CSAs to discuss CUI. This item is still considered open.

In addition to those action items, we also had questions that were asked but not answered during previous public meetings, but are answered on our public facing web page as an additional link for the report to the last meeting, and sent to those that asked the questions.

Are there any questions or comments on the action items from the last meeting?

Michael T.: I have one.

Heather: Alexis, can we…

Michael T.: Let's give it a try. I just wanted to note that on the CUI item, that's one that's been long-standing, since I think my first NISPPAC meeting, May of last year, and when you go back to your desks today, you check the ISOO notice board, which I know you probably check every day, like I do, you'll see a couple of new notices concerning CUI, trying to bring some clarity to the current regulatory landscape, and addressing in particular some of the questions that Industry has had, and I think that puts us in a good moment in the coming months to sit down and have that conversation, so I just want to note that we're taking action on that. That was it.

Heather: Thank you, Sir. Now, moving on to the next item on our agenda. We will now introduce our speakers for their updates. Mr. Isaiah Rivers, the NISPPAC Industry Spokesperson, will provide the Industry update. Ike?

Isaiah: Hello. Hello?

Audience: Hello.

Isaiah: This is a little bittersweet. So I can't just wing something that's bittersweet, so I'd had to jot down a couple little words, and, I'll kind of talk through these words here. Give me one minute, please. One minute. First, thank you, Michael. Thank you to you and to Heather for always taking care of Industry and bringing both bridges together from our Government partners and our Industry partners. But before I begin, with the Industry NISPPAC updates, I just want to take a moment to acknowledge that, as Mike said, this meeting in particular, is a meaningful one for, not only for me, but for Jane Dinkel as well. This is our final NISPPAC public meeting, serving as both the NISPPAC member and the Industry Spokesperson, but I still got 28 more days left at the helm, so we do still got a lot of things to get after this next month. For me, as I reflect on the past 4 years, it's been incredible. I'm grateful for the opportunity to serve in this capacity, and to be part of an organization that actually plays such an important role and strengthening the partnership between Government and cleared Industry. When I first came on the NISPPAC, you know, you think that you know everything. I understood the importance of the mission, but I really did not think I fully appreciated the relationship and the trust and the shared commitment that would come with this responsibility. Over these past 4 years, I've had the privilege of working alongside some incredible, talented people across the Government and the DIB. I've learned a tremendous amount from our Government partners, but I want to give a big, special shout out to ISOO, again, for bridging this. One of the things I truly value about the NISPPAC is ISOO's commitment to making sure that both sides of the table have a seat, the Government and Industry. That commitment to bringing people together, creating an environment for candid dialogue, and giving both perspectives an opportunity to be heard is what makes this partnership so valuable. I would be remiss if I did not give a big special shout out to Miss Heather, so, Heather, if you can please come up here

real quick. I want to present Heather with our Industry NISPPAC coin that we kind of put together about a year ago. So, Heather, here's our coin, so thank you very much. Heather, you have truly been a ground pillar of this organization, a steady presence, a connector, and someone who constantly helped keep the Government and Industry moving in the same direction, and if you didn't know Heather, you would find out real quick, if you don't give something to her at a timely basis, she is yelling at you, so trust me, over the last 4 years, I've been yelled at quite a bit from her and stuff, so thank you, Heather, for everything that you have done for this community.

I also have a deep value for working with Industry partners. One of the things that makes NISPPAC Industry unique is that we can bring together companies from different sizes, different missions, and different perspectives and find a common ground around challenges facing cleared Industry, but above all else, I do want to thank and recognize what I affectionately call my Industry NISPPAC and MOU fam, right, and just in case you don't know what fam means, it's family. That group has meant the most to me. We have spent countless hours together on calls and meetings, working groups, conferences, and sometimes in very spirited discussions about issues that affect our companies, our employees, and ultimately our security mission, and if you've never sat in a conference call with Leonard and Charlie Sowell, and you will be in a treat if you sit next to them too, so, it's been great. We didn't always agree, and frankly, I think that's one of the strengths of this organization, because in order to protect the warfighter, we had to challenge one another, we asked difficult questions, we pushed for clarity, we advocated for Industry, and more importantly, we did it with a shared understanding that the objective was never simply to make things easier for Industry. Our objective was to make the National Industrial Security Program better and protect the warfighter. Being a NISPPAC member has never been about representing someone's one company, one sector, or one individual's perspective. It has been about listening to Industry and identifying common concerns, finding constructive solutions, and making sure that those perspectives are heard by our Government partners, but I leave this role with tremendous confidence because of the people sitting around this particular table, and the relationships that we have built for Government and Industry. To my Government partners, thank you so much for your partnership, your professionalism, and your willingness to listen, and your commitment to the mission. To ISOO, thanks again for continuing to create the space where Government and Industry can come together, have honest conversations, challenge one another, and work towards solutions. To my Industry partners, thank you for your trust, for giving me an opportunity to help carry out the collective voice afforded. And to my NISPPAC Industry and MOU fam, thank you, thank you, thank you for everything. Serving alongside of you has been the most rewarding experiences in my whole entire career. Today does not mark the end of my commitment to the mission or to the people who make this community. I will always be an advocate for a strong Government-Industry partnership, strong national industrial security, and a secure and resilient defense industrial base. We have indeed been better together. Mr. Matt Roche, that was one of our sayings back in the days when he was our NISPPAC DCSA rep. We have been indeed better together as we built relationships, created dialogue, and helped move conversations forward. But there is no time to relax, as there is so much more work to do. I'm grateful, I'm proud, and I'm humbled to have the opportunity to serve. And so, with that, we're going to go ahead and start with today's meeting, updates for the Industry NISPPAC, and continue to work ahead.

But before we get started, I also would like to call my good friend Jeff Spinninger up here. Jeff, can you please come up? Please? Hurry up, Jeff,

let's go, we don't got time. This guy has been a true advocate for Industry, for this particular group right here, NISPPAC Industry and the MOUs, and he has also been our voice as well, and what I love about Jeff is the fact that he keeps it real. Sometimes, when we get to these situations, we like to sugarcoat some things. If you know Jeff, he doesn't sugarcoat anything. He may talk a little bit more, but he doesn't sugarcoat anything, but Jeff, all jokes aside, we truly appreciate and value everything that you have done for this community, from the Government side, from the Industry side, but really for the warfighter, and we just want to say thank you, and we love you. I have to say this because, I wasn't gonna give any shouts out to them, but I have to because they've been in my face for 4 years. There's a couple of folks from DCSA that's always been there for us, and they're in the audience today. Mr. Justin Walsh, Mr. Dave Scott, Mr. Matt Kitzman, Mr. Booker Bland, and the guy who actually was the DCSA NISPPAC representative for years with Heather Sims as Mr. Matthew Kitzman [meant Mr. Keith Minard]. So, thank you very much for your duty for us, and one of my favorites that's sitting on there now, Ms. Allyson Renzella, because she has taken care of us. If there's anybody else that I forgot out there, then, you know, you have to excuse me. So what we're gonna do is, we're gonna… can I…flip these slides, Heather, for the updates? Okay. Oh, I did forget about this.

We have been busy over the last few months. I'll flip the slide here. Okay, we've been busy over the last few months, right? Here are just some of the things… places we've been at over the last few minutes. NDIA, NCMS, ISWG, DCSA CAB, SSCI, ODNI NCSC, and DOHA. Those are just some of the things that we've been up to over the last few months. We have been having a lot of accomplishments, and I'm just gonna throw some out here, but you can add to this list. ICD 705 initiative, security review rating scorecards, self-certification of open storage, DCSA 140 amendments, insider threat ISL, classified infrastructure as a service, rewrite of the FCL handbook, NISPPAC Insider Threat training for the program officials, SEAD 4 rewrite, multiple policies with ODNI NCSC. The list can go on that these fabulous individuals have been doing, right? And sometimes you just don't see it, sometimes we just don't talk about it, because before we have these conversations with you, we want to make sure that we have that true evidence, right? Because you all will fact check us in a heartbeat, and that's what you're supposed to do, but this group has been tremendous, and I just want to give this group of individuals, to include our MOUs, a round of applause, so with that, as I said, Jane and I will be coming off, starting 1 October. We are in the midst of our elections. September 9th, we have our last part of the elections. Thank you, Greg Sadler, a former NISPPAC member, for running elections for us. So next week, Heather and Michael, will send you over the list of individuals. Once the new members are selected, those individuals will get together, and then they will vote on who the next spokesperson is, right, and so, we'll make sure that we pass that on to the public when we get the opportunity. And so we're gonna get right into this. I'm going to turn it over to the Clearance Working Group Chair, which is Ms. LaToya Coleman from Mantech.

LaToya: Oh, no, they can hear me now. I can hear myself now. Okay, thank you. And, Keith, I wasn't, you know, very, I wasn't observant enough to see how much you look like Matt. You were thanking Keith, but said that?

Isaiah: No. No, it's on here. It says Keith Minard and Matt Kitzman.

LaToya: Okay. Alright, so we'll go ahead and go with the Clearance Working Group. So as we close out the fiscal year 2026, I want to start by acknowledging the progress we've had and made together. Industry remains fully

committed to our partnership with the Government to ensure a secure, agile, and efficient vetting landscape. However, as we look to the future, we need clarity and actionable status updates in a few critical areas to ensure we are operating as effectively as possible. This, by all means, is not all-encompassing, but we are going to cover a few of those areas.

First, regarding the DCSA modernization and operations, while we appreciate the ongoing efforts to manage investigation inventories and mitigate backlogs, Industry remains deeply concerned about the rollout of Trusted Workforce 2.0, specifically Phase 3 implementation of Rap Back fingerprint collection. We are seeing many individuals being asked to re-fingerprint despite having already completed Rap Back enrollment initiatives with other CSAs. This duplication of effort is mission-hindering and administratively burdensome. We need to identify the specific policy and technical blockers preventing fingerprints for Rap Back from being shared across the federal government. We look forward to a solution that streamlines this process rather than adding unnecessary friction.

Additionally, we would appreciate further status updates on the broader roadmap for the migration from NBIS to DISS, as well as clear timelines for key initiatives like PVQ.

Second, regarding OUSDI&S initiatives: We've previously expressed concerns regarding military departments' SCI processing timelines, and advocated for a review of the contributing factors. We are encouraged by the Department of the Air Force pilot program aimed at reducing these processing times, and we appreciate Annie for working through this. And we are seeking an update on that pilot and an understanding of when Industry can expect to see those results.

Additionally, we request an update end status of expected outcomes from the GAO report and the MITRE FAST study. With over 170-plus recommendations on the table, Industry needs a clear roadmap on how to best prepare for these upcoming changes.

Finally, regarding the ODNI oversight, we have engaged with NCSC and continue to engage on policies concerning the submittal of applications for access to classified information for contractor personnel that was released June 2026, and we look forward to further revisions that incorporate the feedback we've provided. So what we've done as a result of this policy being released is we've had subsequent conversations and meetings with NCSC and expressed those concerns that we had with that policy in the language that it included. So, NCSC has, oh-so-graciously agreed to review that policy and take into consideration the recommendations that we provided. So we hope to see something from that very soon.

Furthermore, we are looking for a status update on the comprehensive overhaul of SEAD 4. We provided substantial comments this past July, and we are eager to understand the timeline for adjudication of those comments and the expected final outcome of the directive. We are eager to hear your updates on these items, and we look forward to the continued collaboration.

Isaiah: Thank you, Heather. Let me put this on record to get it right. Appreciate you, Matthew Kitzman. Appreciate you, Mr. Keith Minard. Also, a few individuals that are regular, former NISPPAC members, they always come back. Mr. Quinton Wilkes, Ms. Tracy Durkin, and Mr. Derek Jones, and Mr. Greg Sadler. Truly appreciate you all's continued commitment after leaving the NISPPAC. Sometimes people get on and go away. You have been constant and

steady. It's like you never went away. It's like we have a ninth member, a 10th member, and an 11th member, and that's how we can get some things done. So, I'll turn it over to one of our current members, Mr. Leonard Moss from John Hopkins, and he'll go… oh, I'm sorry, I'm turning this over to Jennie Hardy. She's going to go over the NISP Systems Working Group. Go ahead, Jennie.

Jennie: Thank you, Ike, and good morning. It is always an honor to get to be here to represent Industry, but really, it's all of us here sharing the same mission. It's not about you, DCSA, it's not about us in Industry, it's about us, collectively, and everything that we are working toward in supporting a strong, resilient defense industrial base with systems that are intuitive, stable, and let us work efficiently. I can't remember in my tenure a time where we worked with the quickness that we are working with now, with the implementation schedules of these systems, and the rapid changes that we are adapting to. So, the points that I'm speaking of today address just that. First, stabilizing the systems that will feed into NI2 and better connecting common processes. NI2 will bring together tools for entity vetting in the 847 process. Industry sees this as a chance to address long-standing NISS challenges by modernizing and connecting workflows to reduce redundancies. NCCS for the DD254 workflow was deployed just before we met the last time, and we continue to appreciate the partnership that we have with DCSA and the ongoing development of that system, but that system illustrates an opportunity, as does the future movement of NISS into NI2 to modernize and connect the processes. Doing so helps to enable trust from Industry in adopting new processes, and getting users to adopt these systems, across all stakeholders, DCSA, the Government, and Industry, so we ask to stabilize these legacy systems as they move into NI2 first, ensure the systems work, so that we don't have additional redundancies or work that's required that costs all stakeholders time and money. Design an integrated model where related workflows are connected and not fragmented.

In point two, under the NBIS and NI2 transparency, in the last public meeting, we talked about roadmaps, and we've been talking about roadmaps for a while, specifically the request for operational roadmaps that make sense to Industry that we can follow.

I would like to follow up on that and be a little bit more specific. What we're looking for are more capability schedules, so that when we have these rapid rollouts, understanding when we're working with a minimum viable product that goes live which features are in use day one? Which features are deferred to later updates, and timelines and delivery milestones that we can plan against. It's often in the details of this what's live versus what's not that we have mass confusion in Industry, and that erodes the trust in the modernization of the systems that we're all working toward together. Greater transparency into that will go a long way in helping us all prepare and reduce the burden on all stakeholders and on DCSA, who has to answer questions and provide support and feedback and training and follow-up. This helps organizations prepare earlier, coordinate across teams, manage risk, and builds confidence in the modernization path, because people can see how the journey will unfold.

For point three, we are asking for a different way for us to provide and receive feedback through a 360 feedback loop. We are all together again. It’s in us working behind the scenes on these systems. What many people don’t see is that we’re often in daily meetings together. We have ad hoc meetings, we have regularly scheduled meetings, and in all of those we are providing industry asks on behalf of all industries, big and small companies. What we

would like to see is a formal feedback loop that gathers input from the stakeholders. So, industry, government, DCSA, all together alike, provides updates on how that feedback is used, and identifies ownership and timelines for resolving high priority issues, and one of the critical pieces to the feedback loop is also understanding what will not be available for implementation…what cannot be done, suggestions that Industry is making, and why, so that we can understand and be able to tell the story and help communicate to Industry.

So, these asks won't slow the pace of change. We're not slowing down here, but they can help us stay focused, safeguarding national security and supporting the defense industrial base. We appreciate so much the ongoing efforts and the partnerships that we have, Industry to Government. Thank you for your time.

Isaiah: Thank you, Jennie. I'd be remiss if I did not give shouts out to the person who actually dominated me 4 years ago. Without her, I probably would not be here, and that's Miss Heather Sims, from General Dynamics. She was the one that was a great pusher for me to do this, and I am so grateful for that, because I've learned so much from her as well, so, Ms. Heather Sims, if you're online, thank you very much. Alright, turn this over to Mr. Leonard Moss, from John Hopkins, who chairs the NISA Working Group.

Leonard: Thank you, Ike, and I just wanted to first start out by highlighting and thanking the fabulous Jane Dinkel, Ike Rivers, and Jeff Spinnanger. You three are amazing. Thank you for your contributions to this nation. You will not be forgotten, but you will be missed. So thank you all for your contributions. So I also want to thank everybody in this room, because many of you were at ISWG last week, and I want to thank all of you who supported ISWG. For those of you who don't know, that was my other world, you know, being the chair of ISWG for the last 6 years, LaToya. And it's been a remarkable, remarkable, run, serving in that capacity, chairing, because that's the opportunity we have to partner with our intelligence community, right, and when I get into my update, one of the things I'm asking is to strengthen the partnership, the NISA Working Group, with the intelligence community.

So what I'm trying to do is to leverage, as I leave the ISWG, that partnership that we had with ISWG, with the NISA Working Group, because I see a tremendous opportunity, and that's one of the big asks that I took this role in October of last year, and since October of last year, we've been trying to strengthen our partnership with the IC community in the NISA working space, and the reason this is so important is because what the NISA Working Group does is we focus on classified systems, right, and everybody can imagine, one of the biggest challenges we have in Industry is getting our classified systems accredited in a timely fashion, right, so, one of the things we're trying to do is to say, well, let's look for opportunities where we can build some synergies like what we've done with DCSA, and I foot-stomp DCSA a lot, and I get beat down for it, because it’s the truth, but we have a tremendous partnership with DCSA, and I have to, you know, I acknowledge him, but I have to give another shout-out to Mr. Dave Scott, because Dave Scott served in the role of leading this organization, where we built this partnership where it really works, and I really want to say that. I want to talk about something that's working. I'm up here to try and find some solutions, right? And I think that's what we're all here for. We want to find solutions. We're not here to beat up on anybody. We're not here to complain and… because, you know, that's just not going to get us anywhere. We want to find some solutions.

So, I say, when you got something that's working, why not model it, right? So, the partnership that we have with DCSA, we're trying to model that, and that's the first bullet I have here.

We've been trying to strengthen this engagement with the IC, and we did have a wonderful meeting with ODNI and NCSC a few weeks ago, and they offered to help in this regard, and we're gonna take them up on that. So, but that's the first ask I have, is for all of you, all of you CSAs, we need your partnership to strengthen that relationship, the NISA working space. One of the things we're trying to do is just begin with metrics, right? We get some great metrics with DCSA where we can hold each other accountable. We want to do the same thing with our IC partners, so that we can, again, not talk past each other because when you talk to them, I can give you a great example when we have the ISWG conference, we'll have a wonderful panel, all the IC leaders, and they're amazing, and I really appreciate them for showing up for us, but sometimes, their numbers don't match our numbers, right, and so what we want to do is to make sure that when we talk numbers, we're talking from beginning to end, because at the end of the day, we're all here for the mission, right, and so, if we're saying to take us… I don't know, a year to get a CSA approved, and you're saying it takes 3 weeks, that's a big disconnect. So we want to say, well, what are all those months where we have a disconnect?

So what we want to do is, let's have a conversation where we can really get to what is really causing the challenge, and find some solutions. So that's my first ask, is really to help us get metrics in the area of the NISA space, specifically the classified systems with all of our IC partners and all of our other CSA partners.

The other area I wanted to talk to real quickly is on the CSFC front. I want to, again, give a shout out to Jeff Spinnanger, and to Dave Scott, and to DCSA, because at the last public meeting we identified a challenge that we were having with the [Commercial Solutions for Classified] CSFC and Industry, and that is, you know, a lot of our folks are getting these devices, but there's not a whole lot of guidance. So, our concern was national security and protecting the information that they're processing on these systems that they can have in their car, in their hotel, but we couldn't have them in our facilities, so, you know, Jeff and Dave, after the last NDIA meeting they got together, and they put out a Voice of Industry article on this particular topic, and they allowed us to have them in our spaces, which is great. So that's a great step forward, but now we need to go to the next step and provide guidance, because our folks are saying, well, now what does that mean? Can I bring them into closed areas? Can I bring them into this space? Can I bring them to that space? So, one of the things we're doing with the NISA working group is we put together a white paper, and some recommendations, and we're working with my good friend, Mr. Vaughn and the wonderful Tracy Brown, and we're bringing that to them to first start with DCSA and say, you know, how do we work with them in this space, but then, we need to go back to our partners who are actually issuing these devices to say, next steps, and thank you, Annie, for stepping up. Annie was one of the first entities that agreed to work with us to help us come up with some guidance and some guidelines around this because we love these devices, don't get me wrong, the ones saying, take them away, because they're amazing, but one of the things we want to do is say, you know, we could probably, and I'm going to get in trouble for saying this, we could probably save a lot of money, right, if we used more of these devices, so, having said that, you know, I understand, you know, we have our process for SIPRNet, but we could save a lot of money with these devices, so we really want to look at that and say, you know, what's the pragmatic, real solution for the

Government and for Industry? I think, you know, there's a happy medium there, so we want to work… that's the next step, but we'll follow up on, you know, guidelines and guidance after the Voice of Industry, because a lot of folks appreciated the Voice of Industry, but after that, Voice of Industry, I got a bunch of emails and a bunch of calls to send. Okay, now what, Leonard? What's the next step? So, I appreciate you all for getting in and out for us.

And then the next thing we wanted to talk about real quickly was, artificial intelligence. This is… this is taking…and I want to give a shout out to my good friend, Larry Clark, who's up there in the booth operating and making us all look good. Thank you, Larry. Larry has been working with his leadership to try and stand up an sub-team to focus on AI, and I hope that, you know, this gets moved sooner than later, and the reason I say that is because, you know, AI is here, and I know half of you probably wrote half your speeches with AI, so we all use it, right, and you'd be foolish if you didn't use it, because it's a wonderful, wonderful tool, but there's also a lot of risk that comes with AI, right, and as security professionals, we have to be mindful that in order for us to enable the mission, need to get ahead of this risk, so that's one of the things that Larry's sub-team is going to try and focus on. Industry has put together some brilliant folks who do AI for a living, and we're ready to support this initiative that Larry's standing up. We've had, I think, three, two or three meetings so far, and I think we're off to a great start, but I really would like to see that move forward. But I think Larry's in the process of getting it approved, through his leadership, so I really encourage you all to support that initiative.

Okay, real quick, on DCSA, again, I can't sing their praises enough, but we really did make great progress since I've been here in October, the primary focus has been the DAAG, right? The DAAG was released October of 2025, and I became a NISPPAC Industry member, October 2025. So all of our focus was on the DAAG. We had lots and lots and lots of feedback for DCSA. And again, thank you, DCSA, for willingly taking our feedback. Now, it's been a year now and we still have some of those feedback that we haven't reconciled, but the majority of it has been reconciled, and I tell you, Tracy don't mess around. You know, you give something to Tracy Brown, she's gonna get you an answer. So, Tracy, wherever you are, shout out, but Tracy don't mess around. She gets us some answers, and we may not always agree, but she will get you some answers. So, we still have a few more items that we haven't reconciled yet, but we're getting close on the DAAG, and then the big elephant in the room for us is Rev 5, right? Let's just be honest and straightforward. We were all thrown for a loop with Rev 5, because we were told Rev 5 was gonna be published and implemented October 1st, right, and all of the summer Industry was going to work with DCSA to, you know, address concerns and challenges and then we got a loop in July and said, hey, Leonard, you guys, we're gonna have to do this in two weeks. The voice from on high said this has to be implemented now. So, it was actually implemented July 31st, and we're all, you know, trying to make sure we can catch up and we have given a lot of feedback, again and most of that feedback, DCSA has responded, but we haven't had a chance to discuss it, because we had a meeting that was going to happen before the public meeting that we had to reschedule, so, we're going to regroup in September, later this month, and address the feedback, because what we have to do is, even though we had this expedited implementation of Rev 5, we have to still make sure that, you know, we take the concerns of Industry and the challenges you know, seriously, and make sure that even though it's already been implemented, you know, if you go to eMASS, it's Rev 5 now, so you can't do any more Rev 4, but the great thing about it was that they have this wonderful person at DCSA called Lucy Rodriguez. I don't know if y'all know her, but you should get to

know Lucy Rodriguez. She's awesome. She did these demos for us, and she did this training for us, and I'm telling you, it's yeoman. It's phenomenal, and I want her to do more of it. I know she's busy, but because of the expedited implementation, and Ike tried to set up some more training with ISC, but, you know, we weren't able to make that happen, but Mr. Vaughn did arrange some additional training for us, but I think we need more, because there's a lot of small companies out there who are not able to participate in some of those demos and training, and they're going to need some help, so I just encourage you to conduct some more of those trainings where you can. I think there's one more scheduled in October, but it's a lot of folks who are impacted by this, and again, we got a two-week notice that it was going to be implemented July 31st, and it was supposed to be October 1st, so we gotta take that into consideration and consider the impact on all of those, especially those small companies that have to operate within this environment.

And then the last thing I have is to just ask everyone, if you have the CSFC items, and you have info and recommendations, please send those my way, because we're going to be sending that white paper that we put together on the CSFC, starting with DCSA, but then we're going to send it to all of our partners, and hopefully we can work together to move this forward in the right direction. I believe that's all I got for you.

Oh, I'm sorry, one more, Ike. We wanted to also just remind you that we brought up at the last meeting this challenge that we're having with destruction of SAP IT material, and this is a problem because we have just one vendor. And, you know, we have to find solutions that's going to work for all of Industry, so we have some suggestions, we have some recommendations, again, we love our white papers. We wrote another white paper, and we would like to get some support on implementing some of these cost-effective solutions, because again, this impacts all of you and your mission. Thank you for your time.

Isaiah: Alright, we'll turn it over to Mr. Chris Stolkey from BAE. He is the chair of the Insider Threat Working Group.

Christopher: An update from the Insider Threat Working Group. We have a couple sub-working groups, as you can see on the slide, working a couple issues that are impacting Industry. The first one is insider threat for employees that sit at customer sites. This is a gap the group identified that impacts a good chunk of the DIB. So just think of sending an employee that goes, sits at a customer site, and oftentimes we don't hear anything about an employee. There may be bad things happening, and they're not telling us about it. Sometimes that employee is just sent back without giving a reason. The challenging part is often our Government partners will say, I would love to tell you, but I can't. Our hands are tied because of law, policy, something or another. It's a difficult position to be in, and we need to get better on it. I'm going to touch on that a bit more when I get to my last comment there, or my last bullet.

The other group is, they're focusing on mitigating threats from fraudulent applicants. The good news is this group worked really hard, and they put together some great training material, and if it's not up today, it'll be up shortly on the NISPPAC page on the NCMS site. So, if you get a few minutes, I recommend checking that out. Some great pointers on how to deal with this potential threat. As it says on the slide, we continue to have a good relationship with DCSA. We really appreciate the ability to review the insider threat ISL that came out. If you haven't seen it, recommend reading it. It

just put in place the requirements that were put out by DCSA last year. I also appreciate DCSA updating the ISL to include a link to the NISPPAC developed training. If you looked at the first version of the ISL and you tried the link, may not work. They went back and they corrected it, so please check that out. Well, I also applaud DCSA for taking action. We understand why they released the initial guidance and a VOI, but eventually following up and actually putting it in an ISL is something that Industry really appreciates, because it allows us to go to an official source for information.

Lastly, like Leonard said, we're trying to increase our collaboration with the IC. We've taken some steps to do that. Just recently, we had our meeting at ODNI, specifically NCSC. They're really open to the idea. Last week at Leonard's conference this week, met with many of the agencies, they are all open to the idea, and that's great, because it's really important for all insider threat programs to have good information sharing, and related to that, and again, this ties to the comment I first brought up with employees that sit at customer sites. A few months ago, maybe spring, we saw an early draft, it was not widely circulated, of a memo called, Sharing Covered Insider Threat Information Pertaining to Contract Employees. Specifically, it created steps that the Government could take that would allow them, not require them, allow them to share insider threat information with Industry. We provided comment on that. We've not seen an updated memo on that. While certainly the memo didn't give us all we asked for, rarely are we so lucky. It was a step in the right direction, and we want to continue that momentum. So, we asked ODNI to stay on that. We talked with NCSC a few weeks ago on that, and we're looking forward to receiving an update on that. Thank you.

Isaiah: Thanks, Chris. I turn it over now to Jane Dinkel, Lockheed Martin, the Entity Vetting Working Group Chair.

Jane: Is this on? It is. Okay. I'm really pleased to announce some significant projects that we've been able to bring to a close recently, even within the last two weeks since these slides were provided to Heather, there's been some additional progress that's taken place, so I'm really pleased to say that the four years I've spent on the NISPPAC, we actually accomplished something. Thank you, thank you.

So, first of all, the FCL Orientation Handbook, we worked very closely with DCSA on updating that document, and it is published on the DCSA website and available for Industry to use. It is incorporated with 10 job aids that have also been updated, that are also posted there on the DCSA website. We also worked on a project called the Electronic Control Plan, and the intent of that was to… those facilities that are under FOCI that are required to have an electronic control plan, were able to combine their CMMC certification plan to meet some of those ECP requirements, so rather than duplicating that document, if a facility had achieved Level 2 CMMC certification, they could use that, or kind of use that as an appendix to meet those ECP requirements. Now, with the CMMC program being reassessed, the ECP template that we produced is kind of on pause til we see what's going to happen with the CMMC program going forward, but that is available and ready to launch once that reassessment is completed.

Also, we have been working on a Government Security Committee Desktop Reference Guide. This is for facilities that are under FOCI mitigation instruments, and they have a Government Security Committee with outside directors or proxy holders, and this is really a compilation of
guidance, templates, and references for members of that Government Security Committee to use to help them implement their duties, so it tells them things

like what's required during an annual meeting, what to expect during an annual meeting, what they need to be accomplishing during their quarterly meetings, if they're reviewing a visit request, what kind of things must be incorporated into that visit request, so, it really simplifies and gives a very practical application guide for Government Security Committee members, especially those that are new to that role, so it leaves much less guesswork for them, so I'm very, very pleased to say that that tool is ready to be launched. We're going to be working on implementing that out to Industry, so you'll probably see that within the next week or so.

The NDAA 847 clause. That clause, public comment period, has closed. Hopefully you had an opportunity to submit some comments. Those comments have been reviewed and adjudicated, and there will be a response that will be posted back on the Federal Register where those comments were originally submitted. So those responses to those comments will be posted there. Going forward, there will be a public notice once the clause has been officially approved, and there'll be a 6-month implementation period. DCSA, I just spoke with Matthew Kitzman yesterday, and their expected implementation date of execution of day one will probably be March 1. So you can put that on your calendar, and again, keep in mind that that has to be quoted in… that clause has to be quoted in your contract, so it's not just applicable across the board, but it has to be quoted in your contract to be applicable.

And then finally, the Turbo FCL project. That is still in beta testing through the DARPA website, and through December, its use is voluntary, it's not required for you to use it, but it can help you prepare your FCL package for DCSA to make sure that it is more complete and finalized when you go to submit that to DCSA.

I would be remiss in exiting my swan song without acknowledging the wonderful folks that I have worked with and partnered with, both within Industry and Government. They've made the last 4 years it's just an amazing, experience for me. I consider them friends, and I especially want to thank Ike Rivers for his leadership for the last 2 years as our spokesperson. He refers to all of us as fam or family, and we really feel like that toward each other, and we really like working with each other and work with each other like a family. And I also want to acknowledge and express my appreciation to the Government for their partnership. I am a firm believer that both Industry and Government want to do the right thing. We just need to know what that is. We really want to do the right thing, want to meet in the middle, we want to partner with each other and make sure that our end goal is the same, which is the protection of national security, so, I am extremely grateful for the four years that I got to serve on the NISPPAC as an Industry member, and I'm very humbled by any acknowledgement that is given to any contribution that I've made, and I just want to say thank you to all of you for your time.

Isaiah: Appreciate you Jane. Okay, we gonna turn it over. Heather, I think. Slide of that thing is not working now. You take care of it? Okay, Ms. Kathy Andrews, I think she's online here. She's from Northrop Grumman. She is the physical security working group chair. Kathy had some conflict, as far as work. She had some much-needed stuff she had to be at her duty section to take care of, but she is online. Kathy, I want to turn it over to you. Can I go back here? Hold on. Alright, Kathy?

Kathy Andrews: Thank you, Ike, and good morning, everybody. My apologies for not being able to be with you in person. As many of you guys know, ICD 705 has been at the forefront of our priorities over the past few years, and while the

requirements are demanding, we have also seen a meaningful increase in Government/Industry collaboration as we work to understand and address the real world implementation challenges behind the policy. I think we've made some substantial progress recently due to some site visits that have been especially valuable, allowing us in Industry to demonstrate the difficulties of implementing 705, especially in those legacy facilities, and the practical constraints our operators and engineers navigate every day. With the recent rescission of the 2025 memo establishing facility upgrade deadlines, followed closely thereafter by ODNI's directive to maintain operations and currently accredited SCIFs, we believe that policy decisions are starting to be appropriately balanced, balancing the speed to the warfighter, as well as ongoing cost pressures, so thank you very much for recognizing this. Next slide, please.

Despite this positive progress, Industry continues to remain concerned about the inconsistent implementation of policies. We appreciate the opportunity to continue to engage with both NCSC and the Department of War at all levels to achieve a balanced approach. I believe we can get there, but much like my colleagues have mentioned, it's going to take the maintenance of the continued transparency and collaboration that has increased so much in the coming months. So I thank everybody for their efforts, and look forward to taking us to the next level and reporting that at our next public meeting.

Isaiah: Thank you, Kathy. Kathy can't see him, but Mr. Adrian Shepherd is in here from DIA. Adrian, Industry NISPPAC thanks you so much. I know you get pulled so many different places, but your partnership, from a DIA perspective and from a personal perspective to Industry, is so invaluable, and so thank you so much for always being here. We know it's tough. But we thank you for that. I turn it over to Mr. Charlie Sowell. He is the Policy Working Group Chair.

Charles: Couple of things that we're tracking, first that's not on the slide, but is important. We are following the FY27 NDAA and IAA draft legislation and reporting on Industry impacts of that. One of our key areas that we've been working with ISOO and our Government partners on is guidance related to all of the executive orders that have come out since 2025. There have been hundreds of executive orders, and many of those executive orders directly impact cleared Industry and most companies supporting the U.S. Government. I'm pleased, that we're hearing progress where through ISOO's leadership and through DoW, it sounds like we're going to be getting some, some helpful guidance from the U.S. Government writ large on how these executive orders impact cleared Industry and Industry more broadly, and we really appreciate the effort that's gone into that. So thank you for the hard work and the cross-Government coordination that's led to that.

Industry continues to look at the CMMC pause from DoW. We applaud that pause, we appreciate the reviews that have gone along with that, and we have contributed our recommendations for future implementation, so thank you for the work on that.

And then, lastly, the Government studies update. We've been working with ISOO and through the Policy Working Group to explore an AI-enabled review of the NISP, and we've completed the document collection. We have a library of information of past NISP documents, and we also interviewed the original NISP Industry members for their insights on why the NISP was established, you know, from an Industry perspective, and what was different today than was from there. So our next steps are reviewing that information. AI-enabled, but human-led,

reviews of that and coming up with some recommendations. So, with that, I'll turn it back over to Ike. Thank you.

Isaiah: Oh, thank you. Who moved the slides around? Yeah, okay. That slide is there. I think that was Lisa. Where's Lisa at? Does everybody know Lisa Reidy? Alright, so she really is the backbone of NISPPAC Industry and the MOUs, because she is the coordinator, and she's the one that puts all the meetings together and all the slides together. So, Lisa, none of the things that we do is not possible without you, so thank you so much for your dedication. Thank you.

I do have an ask. So, Heather, she talked about a lot of the things that were still opening, right? In this trade, the NISPPAC, in the MOUs, we… we… we need some help with that. I don't think we can continue to go meeting after meeting, and without getting some of these closed, so, whatever Industry NISPPAC can do to help get some of these items closed, or some clarifications, we are here, right, and we need to do that. It'd really be nice to go down that list at the next public meeting and says, hey, we have no open items. Now, mind you, the NISPPAC has been around since 1993. There's always been open items, but let's see if we can kind of knock some of those open items off the list. That is extremely important for national security, but it's really important for the warfighter, so that would be my personal ask if we can try to get at that, and again, Industry NISPPAC is here to help with that, and that is all that we have from an Industry NISPPAC perspective.

Michael T.: Thank you, Ike. Any questions for NISPPAC Industry? Hearing none, we'll turn it over to Heather.

Heather: Thank you, sir. Next, we have Mr. Jeffrey Spinnanger, the Director of the Information and Acquisition Protection Directorate for the Office of the Undersecretary of War for Intelligence and Security, who will give the update on behalf of the Department of War as the NISP Executive Agent. Jeff?

Jeffrey: Alright, well, good morning. It's a bit bigger crowd than the last one, which is really encouraging, because when we were doing these things remotely, it's amazing what you could start talking about without really any fear of being able to read the room, or what people are thinking about what you say, which is maybe where some of the candor comes from. But I'd like to start out by just sort of joining the chorus and some of the thank yous. You know, first and foremost, you know, for the kind remarks that were made, you know, regarding my tenure, I appreciate it very much. This really is kind of a labor of love. I used to be in the audience, you know, with my boss, and I really did have aspirations to do exactly, what I'm doing right now, and and it's gonna sound a little trite, but it's entirely true. It was a bit of a dream come true to be able to do this, because it's very high-consequence stuff, and, G-d help us, G-d help me, but I love it. So, thank you for that. But none of that is capable, you're not able to get much done, without just the, just oceans and oceans of collaboration, an occasional gnashing of the teeth. I was gonna try to make my ringtone play for what my ringtone is when Ike calls me, and then I decided maybe I shouldn't do that, because it needs to stay rated PG, I think. And so, but, you know, all kidding aside, you know, it's how beneficial is it that, one, we, have the ability that we can communicate, and it's bi-directional, and I won't ask him what my ringtone is, but it's bi-directional because it's necessary, it's incredibly important, and the opportunity for candor is really kind of built on a foundation of trust. I promise you there's not a lot of happiness engineering going on, and I think if you were keeping score, the number of times where the answer is not the

pristine answer, but it comes from, hey, this is what we can do, this is what reality looks like. There's common understanding, and from that common understanding, then we can get to, what he, frankly, what you said so eloquently, you know, related to you know, our priority, which is, which is on the warfighter. And if it's not that, then really you don't have any business being here. So, sorry, I want to say thank you to Ike as a spokesperson, but it's a team sport, right? He can't do any of it on his own, and the fantastic cast that, you know, that is represented by the folks that are here in Industry today, and all of those that have been in the seat before have been, you know, fantastic partners. So many of them are in the room today, which is really great, and that candor has been kind of a consistent theme, and that's how we're able to get stuff done. That was a wonderful laundry list. That might conclude all my remarks that Ike laid out there, but those are real accomplishments. You know, the work continues, you know, and again, as you said, I'm sure there were due outs in 1993. Hopefully there are not any due-outs from 1993, that'd be bad, but I think it's really great. And Jane, as a departing member, I just want to particularly call out the partnership here and some real controversial issues, you know, to put points on the board we like to talk about here is really great. So, if I may ask for a round of applause for all of these folks, and then so, we don't do anything alone, and, you know, sometimes it does feel a little bit lonely, in a building that has 30,000 people that come to work in it every day, but this can be kind of isolating work. It's very difficult, and so frequently the building can kind of feel like it's kind of fallen in on us, but we have a really, you know, great team within I&S, and so y'all get to see me kind of a lot, but the fact of the matter is that, you know, we have a really great team. Many of you all know I want to introduce, so Patrick Harris is here, and Jamie Long in the audience. We stole Matt Roach from DCSA. We're going to return them at some point. I'm not sure how they feel about that, but we've been happy to have him, and so, you know, they'll continue to do the work that we continue in support of the importance of the industrial security program, but I'm really happy to have my battle buddy, in the audience today, right? So, and also, right now, my boss, just by the way, so just please be nice, but, you know, Jill Baker is just sort of, you know, I mean, she, you know, everyone knows her, is fantastic, but we get into some pretty weighty stuff, and then occasionally a little bit of bourbon, so…I realize this is on the record, but it doesn't matter now, so… and none this morning, I should clarify, but yeah, not yet. So, I'm really happy to have, you know, Jill here, and so we don't want to get inside any decision loops within the department, but, you know, Jill has just been steady across the board, I would say, and I'm really happy to have her here today, as well. So thanks a lot, Jill, for making some time today, to, to, to be here. Before I dive in, just a couple things I think might be a little bit easier. Of course, I have some good jokes, and just as if on cue, right, since there have been 76 of them, I was a little concerned, because I'm pretty sure Perry's been here for, like, 74 of the public meetings, and he showed up, and it was good, because otherwise I was going to have to talk about how old Minard is, and, you know, but it kind of speaks for itself, right? So, and… and I can see how they confuse you and Matt, right? They do look a lot alike, and so… although the glare off your… like, it's just perfect right now, so…but yeah, really happy to have, you know, Perry here as well, right? So we've known each other a long time, and I'm glad to see you here today as well. So with that, before I kind of go in, I appreciate the updates that came from all of the various working groups, but just sort of in no particular order, I just, because I wrote it on the top of my notes, I was going to ask Annie if he wanted us to provide a brief update on the access work in partnership with Air Force.

Andrianna: Thank you, Jeff. So, the Department of the Air Force recognizes the challenges that Industry's experiencing when it comes to SCI indoctrinations, but not just that. Also, SCIF accreditation timelines, system access, all things to get your personnel that need access to SCI to work as quickly as possible. We also experienced that somewhat on the Government side and so, Air Force A2, specifically within the DAF, has worked with I&S on a pilot, an automation pilot right now, which is tentatively right now called SCIF Workflow Tool, but it's more than just SCIFs. Like I said, it's SCI docs, SCIF accreditation paperwork, and classified system activities as well. The goal is really to modernize and automate what we can within that process, where the DAF has touchpoints, to streamline it, and improve the timelines, as well as improve the quality of paperwork that goes between different offices. We are in a stage right now where we're collaborating internally within the Department of the Air Force, including the Space Force, as well as I&S and DIA. So, there are not many specifics to share right now in the public forum. We do have a tentative initial deployment within FY27, but of course, that can fluctuate based off of Government shutdowns, possible furloughs, funding issues, new priorities, personnel going to greener pastures, etc.

Jeffrey: Locusts, right, yeah, of course.

Andrianna: But we are absolutely committed to making sure that we include Industry in those efforts, so that whatever is developed does work for you. It does not detract from any efforts that DIA is working on and that we have a system that works, which, Jennie, you spoke earlier about DCSA systems, the same applies to ours. We don't want to be duplicative, we just want it to make things better, so we will continue to provide updates and make sure Industry is an active member in these conversations.

Jeffrey: Thank you, Annie. Yeah, just to piggyback on that one just a little bit, as we kind of scroll through these things, this problem surfaced for us. Obviously we've all known about it for quite some time, right, but to me, I like a little bit of show and tell about how NISPPAC works, right, so being able to kind of surface these issues with some data and put some real, you know, teeth behind it. That's very valuable for us from, you know, within the policy slot, but as a function of active, what I describe as active oversight, and so, being able to continue to note that, you know, there's, you know, we're taking some initiative here, we're trying to build some efficiency in it. I would be remiss, though, if I, I don't want to be accused of not being candid in my last one of these things. So, our goal isn't just to try to be better at a bad process, right? So let's be very crystal clear about that. And so we want to continue to shine attention on it, and so the first of probably what will end up being several asks here for both the working group, NISPPAC as a whole, and reminder, right, we just heard a lot from Industry, but NISPPAC is highly reliant maybe a little bit more so on the Government themselves, because it's all of our policies, right? You know, that are the tension that we're trying to address. No guarantees that we're going to change it, but at the very least, we need to understand it a little bit more, and to see what the value is in a million hours of folks read the newspaper while they wait for the administrative process leading to access, right? So, and that's all after eligibility was established, and so we need to continue to surface this, and I can tell you that it creates unsatisfying looks on the faces of seniors in the department, and we all work for the same guy when we get to the top of the food chain, but we have to be able to make it make sense to understand why the best thing that we can do today is to drive just 2 tons of efficiency related to eligibility, something that I actually don't think anybody mentioned as a function of all the updates, which is just an amazing, you know, turn of, you

know, a show of progress, you know, with, with, chiefly aimed at DCSA, which is really quite remarkable, and it happened, and we didn't even say anything about it, which is really great, but as we turn the conversation into the access side of it, we have to be grounded in what our baseline in…you know, the way contract terms are today, right? So, the contract begins when eligibility is established, right? That's when the till begins to run, as it were. And so, you will have no stronger defender, certainly from, you know, me and my office and the folks that come beyond, to be able to defend and understand the value in that delta, if it makes sense. And so the blunt truth of it is, and just the first, that we would ask ISOO to continue to hold us to task here on this issue, is to really understand what that looks like, and so, with a shout out to the initiative of the Air Force, nobody asked the Air Force or the command that's doing this work to undertake this, right? They took it on in their own initiative, and that's fantastic. The thing that will continue to move it forward and maybe create real options to use the word efficient, in the way it's actually defined, is more attention on it. So that's kind of a continuing ask here as this continues to report out, because it's a hugely consequential issue. All the conversation is about SCI, but we could put the SAP moniker on the same issue, and we'd probably have maybe even a more stark problem within the department, and it's a huge cost. So thank you for the continued attention on it, LaToya and the team, and the continuing work of Air Force. And so, I love, asking for people to do work that I won't have any responsibility for, and I hope that you will ask Annie specifically about this at the next update, so you're welcome. Right, so, we were passing notes earlier, she didn't see that part in there. So, so anyway, so just to, just wanted to jump on that one, first and foremost. I really appreciate the comments made.

Several Industry members mentioned the GAO and the FAST. Right? These are tools for the department, right? So we, you know, we didn't ask the GAO, I don't know if the GAO is listening, but we're really happy that you did it. That's on the record, right? So, I gotta try to erase that whole bourbon thing from earlier, but we did ask for the FAST, right? We did that. We were very deliberate in the FAST, and some other things that we'll talk about, you know, a little bit deeper in my remarks because these became just incredible opportunities, and for the work that Charlie and some of the really gray beards are thinking about as it relates to the origin stories of the NISP, maybe what the future needs to look like from a policy perspective. Data needs to tell the story. And, my experience, here and in prior positions, tells me that the most valuable data that relates to industrial security probably ought to come from Industry. Thank you, that was a really profound set of revelation there. When we commissioned FAST, we really aimed it out into Industry, right? You've heard us kind of, you know, extol the scope of it, and I'm glad to see our MITRE partners here, for the great work, but as LaToya said, and maybe a few others. The whole goal wasn't just hey, a new study, right, we can put it next to the old study, and then in 10 years from now, we can use those to make another study. That wasn't the whole purpose, right? We tried to be a little bit more action-oriented, and we did ask for, hey, there's recommendations, and there's a litany of findings and recommendations, and there's no chance in heck that we're going to deliver on 76 recommendations and, you know, the answer at the other end. On the other hand, those… some of those, as we continue to examine them, and I will say, we got top of the food chain attention on it, right? So, the Deputy Undersecretary in particular has taken a very keen interest in the mother of all POA&Ms I'll call it, that we've built out of this thing, to really try to hold ourselves to some degree of accountability to lay out options, right, so that's ultimately what we're really fighting for here, and I think we're delivering on that, but the continuing attention is necessary. Again, you know, we should be prepared, certainly in the beginning

of the year, to be able to provide a bit of a more substantive update, kind of across those, particularly a handful of those that are prioritized, and which are reflected in some of the remarks. I think we could do a little bit better job of being able to align some of what the working groups are looking at to those things that have connective tissue to the study itself. That's very beneficial for this audience and for the program as a whole, but I think maybe more importantly, it'll continue to help and make it make sense to the leadership that we're really trying to influence as it relates to some of the decisions that we're pushing after.

With that, I do wanna call out, right? So one of the open items that kind of remains, and I appreciate it, Heather, and you know, to kind of pushing through, but the issue related to small business is really quite critical. Hopefully, you know, many of you saw the Secretary himself spoke about the value and the incredible importance, you know, the innovation side of things, right? Those smalls…we want to make sure…the NISP is incredibly important. National security and all the protections that we're aiming at are incredibly important, but if we create a scenario where it appears that there are barriers, then we're creating decisions for our leaders, that we're not giving them good options here, and security's about, among other things, about creating those options. We have a real disconnect as it relates to some small business rules and some statute that were laid in now several years ago, and some disconnects within the CFR itself. We've talked about it a long time. I'm a little disappointed that I'm not going to be able to see some option or resolution of that during my tenure, and I'm going to have to chalk that one up in the loss column because this was a big issue before. It's not getting smaller, and so it's not something that the department can solve. We can continue to call it out, but as the purveyors of the 2004, we really need to, first step, call a meeting. Let's get the Small Business Administration. We'll certainly get the smart people from the department, and see if we can't lay out some options. But I do think, I can't really think of anything more consequential right now, that we could be doing, that really kind of gets after what is, a very, prominent theme within the national defense strategy, so okay, that’s the tough stuff.

Okay, so, we, a couple things just on the policy front here, and as I'll continue to try to map these to some of the updates, right? So, you know, Volume 1, thank you very much to NISPPAC Industry, and to anybody who helped to participate in it, right, but the reissuance of Volume 1 is… it's a little bit behind the clock. We've been banging on a lot of policy within our portfolio for quite some time, and so, and we were intentionally prioritize this a little bit behind some of the others that have, you know, a connection to Industry, particularly special access, but it's out now. We were able to, you know, to really, you know, appreciate, one, you kept pace with the clock, right? Unlike not all of the department's components, Industry met our timeline, and Patrick and Jamie weren't gnashing too much at teeth based on the comments and inputs that we got, and so we're in a pretty good place. I will tell you, we are all the way through. 46 Department of War components have provided, you know, their editorializing and inputs to the draft manual, there are no… is that right? No non-concurs? Do I have that right? They're like, what? No, is that right? Or almost no? Almost no. Alright, well, damn. Alright, so…but nothing insurmountable, is that fair? Okay, alright. Patrick's like, stop talking about that, right? So, yeah, so we're closing in, you know, it's always difficult to put timelines to things, but it's very important. We could use some Industry support here, because frankly, there are some deltas, in terms of what the NISPOM says and what the Volume 1 says. This creates real problems for DCSA, a little thing like a little more flexibility in key

management of personnel. I'm working on it, Matt, I promise. So I told you I was going to mention your name. I was just throwing myself under the bus. You know, Matt and his team kind of surfaced an issue that would provide a little more flexibility, in… as a function of the process that leading to facility clearances. This is a particularly acute problem in academia. We have sort of this cookie-cutter idea in our policy statement about how would a board, you know, want to look like in a university, and it turns out that they're all very different, and this is a bit of a vexing problem. There's quite a bit of latitude within the NISPOM, hopefully you're familiar with that, but, but less so in the department's policy, and there's several others of these kinds of examples, specifically on the IT side of things that's not really reflective of the way in which we work today, and so being able to iron those things out, DCSA certainly uses the Volume 1 as a playbook more than any others, but the fact of the matter is that, you know, all the components do as well, and of course, everybody who signs up to have DCSA provide their the industrial security services across the Government, they might not read the fine print, but it also says you have to follow our policy. And so we need to get that out the door, so it's up there. Our new boss, Timothy Brown, the new DDI for counterintelligence, law enforcement, security, understands that. We've been getting him, you know, spun up on what it's like to be responsible for federal regulation and the departments implementing policy on that, and he still took the job. So, we'll see. But, you know, continuing attention, and I really do appreciate one of the things that helps us be able to get over the line inside the debates that can happen across components, particularly within the military departments, but we're able to say, hey, we got Industry, you know, to take a look on this, and here's what their comments and edits look like, and honestly bolsters us, right? We're a pretty smart group, especially with Matt on the team, but, like, we don't have a complete, you know, clairvoyance over the entirety of the department, but Industry, being able to utilize these folks to get broader allows us for, you know, a degree of confidence, in the process that maybe we wouldn't have, you know, but for the work.

Appreciate it, I think Jane mentioned, TurboFCL. Really happy for that, glad that my team, you know, we've been working with DARPA and with DCSA to try to be, you know, be mindful of the application, you know, put it to practice and use. You know, to create some efficiencies. I'll continue to foot stomp. We gotta do better than just be efficient at lumbering process. The simple fact of the matter is we are right to say that things are getting better, but they're nowhere close to where they need to be. Not within the framework of the industrial security program, where the flash to bang from contract award to performance needs to be as close to instantaneous as is possible, and we are not ready for that yet.

You know, the continuum work, the FCL handbook, and other things that were mentioned today, those are reflections of how the process needs to work, but our goals have to be mindful of real security work. The real purpose of the industrial security program isn't all this administrative stuff that really defines or occupies most of our minds. It's the actual performance of the in support of national security work that's supposed to happen when the contracts themselves are underway. We're not quite ready to have that be the primary conversation, but I think we are trending in the right direction. We don't want to miss the opportunity to applaud the improvements, but we have to be mindful of the fact that we are nowhere close to where we need to be, and that becomes even more of an acute issue when we think about 847 going out. It's not going to be this deluge kind of issue that had been been laid out before, but as it begins to… and I appreciate Jane saying it the way that she did, but as it makes… it starts to make its dribs and drabs onto contracts, the

requirements themselves are going to have us do what they do to move them forward. The timelines are being shape up pretty well with the way in which DCSA has prioritized NI2, which is really convenient, and I'm also pleased to say, you know, DCSA, through a lot of its own internal work and some partnering with our team. I use the analogy that, like, if we had to do this in a… remember anybody ever… I use this really fun bowling analogy, I think it's kind of fun, and what the hell I'm talking anyway, but you ever learn how to score bowling, like, by hand, right? Today, you go to, like, maybe it's like, nobody goes bowling, but if you do, right, it's all electronic. But in the old days, you had to do it by hand, and it's this kind of weird, wonky math, right, especially if you get a strike and all this other stuff and in gym class, when I was a kid, we actually learned how to do that. Well, that's kind of where DCSA is right now, right? They're not waiting on the system in terms of their preparation, and as a function of the way in which you know, we need to be able to drive down some of these timelines, particularly as it relates to new entrants, which tend to be dominated by small companies. You see where we're going with this, right? Which is very responsive to the priorities of the Secretary. We can't wait on the system. We cannot continue to pine away about that stuff, and so these guys are now really good at scoring bowling, you know, and the analog, if necessary. But it's looking like the timelines are going to line up pretty well. There's a homework assignment, though, as it relates to the rollout of this, particularly as it relates to the NISP and nobody's looking for redundant process or requirement, right? So every company that's represented in this room and sort of around this table, you already have a couple of advantages where 847 go, in the form of you have a 328 on file, particularly if you're performing. Now, it needs to be probably a little more current, right? So part of our oversight has been that, hey, those things can get a little stale, and we can be looking at… we saw some examples where, you know, currency was defined, you know, at a time, you know, like, the date on the 328 was, like… I'm like, hey, I turned 30 that year, and I remember it really well, but it's hard to imagine that a company hasn't changed at all in its posture over, you know, a 24-year time period, right? I'm being a little bit exaggerating, mostly because I forgot how long ago that I turned 30. I should have said 40, because it would have been a little more close to the example, but there needs to be some currency. DCSA is recognizing that. That's where the data and the data systems will be helpful in it, but that's not something that the Industry should be passive about also, right? So you can watch the news, and you can see it just the same as we can, and being able to kind of be in front of that, right, and the affirmative responsibilities that companies that participate in the program have to make sure that their information is current, just like we all have to do with our personnel security I think will go a long way to dialing down any concerns that an existing cleared defense contractor should have, even if that company's under foci mitigation today, and so I put that out there, and if it turns out I'm wrong about that, then, well, it doesn't really matter now, but I'm very confident that I'm not, and I think they've really rightly postured to take the best pieces and parts of it and I wouldn't be remiss if I didn't continue to remind folks, right, that when Congress put the provision in place, like, let's see the complement, folks, right? So the idea, hey, FOCI's a real concern, and the Congress believes, as they, I think, in the right to do so, that the way in which we consider it as a function of industrial security, which has been going on for a long time works, right? It works so well that we should start to use it as an acquisition criteria as a function of award, so there's a serious complement in there, and there's a real challenge, but leading from the front, programmatically, is a public… is a Government and Industry opportunity that I, I really think we should take, very firm advantage of all the more as, as NI2 moves, you know, moves in a very good direction, which, which certainly it is.

The other thing related to that, and I didn't want to miss it and start to wrap up here, and that is, you know, the other thing that's happening where NI2 is concerned, and just data, just in general, and I think it was Jennie, I can't remember, but I'm going to just give you some credit, because I feel like I've talked about Ike and you know, Leonard set me up last week, and…
I'm standing too close to Charlie, so it's, you know…so, anyway, but I think it was you, you know, like, you know, where you were talking, I think you mentioned transparency, right? Like, I will tell you, when I first joined the NISPPAC, it was Kim Baughner used to sit, like, right there where the monitors are, and continuously kind of talk about the challenges that she would have as a Government person being able to be able to access and utilize the data that is collected, principally by DCSA, but from Industry, and her own execution and requirements, you know, within State Department's program and over the time period since then, real testament to the leadership and foresight of DCSA and some of the evolving requirements here, and that is that, you know, there's greater access across Government and Industry, right? So your comments related to its importance in Industry are really fantastic but I have to be very, very candid with you, it's really Government itself that needs to be the beneficiary. DCSA is as a data services provider in this way, because industrial security becomes a team sport when we get to the performance on the contracts and I love the fact that we're really starting to be able to have that conversation in a more objective way and I would continue to see it, to move forward, particularly as NI2 comes along. It's not gonna be a perfect system, right? DCSA is DCSA, they're not Microsoft, right? And so they're having to build this thing at the same time period, but making it kind of dynamic, our office, you know, certainly, you know, continue to play an active role in the requirements and such but, you know, it's always going to be a journey that won't ever end, but I think the fact is that there's more use and utility that's coming from it as a real opportunity and that's the thing that we really need to focus on, because if the goal is the perfect thing on the way out the door, then that's not realistic, and it's also not purposeful, as it relates to mission.

Okay, so, lastly, last couple things here. Appreciate, Michael, thank you very much for saying CUI, so I don't have to.

Oh, AI, right? So, yeah, I think it's great, the work that Larry's doing, right? I continue to volunteer. I'm gonna volunteer twice. Devin Casey's not here with me, he's on my team. He might be listening, he probably just hung up but he's an active participant in the work with respect to the 45 or 60, I don't remember the timeline that CIO established for CMMC is concerned. There's a fun little intersection there between CUI and CMMC, and Devin Casey's pretty much the smartest guy in the department on that, so we're really happy to have that. So for my Industry working group, you know, counterparts here, right, so, happy to lend that voice. They're meeting pretty regularly, to try to put out some options here on, you know, hey, let's relieve some of the burden, but let's also keep our eye on the prize, that there's real national security interest in cybersecurity on those commercial side systems.

And then finally, on the AI front, well, two other things, right? So thank you for the flyaway kits conversation. Leonard, I just wanted to… I am gonna… I will talk to you in this moment. No, I'm kidding. The ISWG was fantastic, really opportunity for candor, but you said, hey, don't want to get in trouble, for what you said, but we can save a lot of money, absolutely, and be more communicative and be more expedient, and be more secure and spend less money, right? Those are the benefits that kind of come from this. So, again,

testament to how this all works, right? You all raising the issue so that we can get past the absurdity of, yeah, by all means, go out and make the classified call in the car, but you're not… dear G-d, don't come into the open air… open storage area, right? It feels like Ashton Kutcher should parachute out of the ceiling because we're being punked, right and hey, allowing common sense to enter into the mix here, but really, that's not where the conversation needs to end, so certainly we need some more guidance, although I think our friends at DISA do a pretty good job of that. I went and became a student of it. You know, remember the training I took, because I had one of those things for a while. Very happy, among other things, that I've gotten to turn in, was that particular little device, because it does become oh, crap, it's ringing again, kind of a thing, right? So, like, you can't… you run out of reasons to, like, well, I'm sorry, I didn't see that over the weekend, or whatever, but… but all kidding aside, right, there's real use and utility and beneficial security, and so I don't think this is where the work ends at all, and certainly we need some more guidance, we should have that. But again, one of the asks that we have of Industry, if you're starting to hear resistance in this, we need to know that. DCSA needs to know that, so they can make sure that they're empowering their workforce to be more understanding. DCSA also needs to be able to know that, so that if a military department or somebody's issuing these things, that they need to know, right? They need to be aware of that. To me, it's entirely within the remit of industrial security. I don't care if the people work on a military installation or they work at, you know, in you know, whatever, a facility in you know, Arkansas someplace. And so, it makes no difference. Being able to be knowledgeable of that, I think, is key, because as we continue then to refine the guidance and whatnot, both to Industry and to Government, that becomes kind of a wash, rinse, repeat part of it, but more than that, it should also be the thing that invites larger considerations of the use and utility of these things. We were talking about, I guess I was with a colleague, talking to my boss, and said we need to spend more time talking about what security limits us from doing with our Industry partners, not what it enables or what it secures and in IT, it's no more fundamental than this, and so the real vexing problem here that we can get after is today I can send an email to any contractor on my team on any network that I want to, and they'll be able to respond to that within the confines of our spaces. The promise of these things is a greater degree of interoperability, not just for those contractors that provide services and support, you know, mostly administratively, but in a production environment. It's the same security requirement. Why don't we have the same core capability? And the answer isn't because of something that's written in the NISPOM or in the NISP, it doesn't trace itself to the EO, which doesn't even contemplate systems. The word does not appear in the executive order and so what it is, it's a… we're in a… we've always done it this way, and because we've always done it this way, that's a real limb fact for us. Well, this is the time to really throw that out the window, and now we can capitalize on something that's kind of happening on its own, and really advance it and I think we should be quite provocative in that, so that we can be more communicative with Industry, right? We constantly are talking about information sharing, the latest cyber, this, that, or the other thing. Well, how much better would we be if we'd be able to share using these devices, right? Imagine if a scenario where every FSO and the NISP has one of these things, and when we need to tell them something that we really can't send them, we can't secure it any other way, and probably shouldn't use Signal. I'm not sure if that's a fun joke or not today. Ugh. Damn, I was doing pretty well, I thought, so… but all kidding aside, right, like, this is something, like, these exist, right? So we should be thinking about that and Leonard's point is exactly right, and I really do think it should be called out. That is not an

expensive solution, right? You know, we've tried something like this before, right? Some of you are old enough to remember DIBN S. Right? You know, this is way beyond that and one of the challenges that I'm leaving for my office is to… we're pretty good at issue papers, that's how we get some money, that's where I'll help Annie. I was looking for a little credit there from LaToya's question for earlier to help with the SCI things, but we can go find some scoop-up money, right, to be able to kind of show the value of that but if you think about this thing programmatically, and we really did put one of these in every FSO's hands, we're not going to break the bank at all, but what we are going to do is we're going to enable security and so that's the way that we should be looking at it, and I think because of the power of NISPPAC, if we keep our eye on that, I think we'll create that kind of options for our leadership pretty fast, and so that would be the challenge.

And then finally, just on the AI front, you know, just to kind of close out from there, yeah, it's game-changing kinds of stuff. I mentioned it in one of the working groups, so I want to do so here and I really am trying to be a little bit deliberate about trying to sign us up for work that's going to be beyond my tenure, but this one's real high consequence, but it's also high opportunity, right? So, there are a couple of studies that our team has commissioned, you know, that are going to start to come to fruition in the fall. Devin Casey, again, is kind of our lead for that, because he's got a… I mean, he doesn't… if those of you know him, he's got a devious mind. He hides it pretty well, but it's starting to come out, and I think it's really good for us, because there's challenges and there's opportunities, where some of the conventional AI, certainly leading edge is its own concern, so other people are working on that, but from a security vantage point, right, really kind of wanting to understand what those are, because there's just a whole lot of…you know, nobody's telling me not to, so I'm going to. So, you know, helping to define what some of the guardrails need to look like but with some of the opportunities to really utilize the word efficient in a way that's consistent with its definition. Said more directly, the department's got a lot of classified information that we kind of foist in your direction that probably shouldn't be and I think AI is going to help us kind of get after that pretty fast. And so, with that, I would ask, to add to the to-do list here, but beginning with the working groups, and certainly leading up to the next NISPPAC, we would look to be able to carve out a little space to be able to provide us, provide a little bit of an update of what our findings are telling us, because it will be immediately consequential to national security work, particularly where classified is. So Devin will love that. So,
So with that, I think I'll just close out by saying, you know, where I'm been, thank you very much. This is, it's just been, it's been, you know, just a tremendous, honor to serve in this role, in this capacity. You know, some great teammates across the board, and I'll miss it. So thanks a lot.

Michael T.: Anyone have questions for the Department of War? One last chance to take a swing at Jeff.

Heather: Alright, thank you, Jeff. We will now hear from Ms. Allyson Renzella, the Senior Policy Advisor for Industrial Security at DCSA. Allyson?

Allyson: Alright, good morning. I know I'm standing between you and a break, so I will try to keep my remarks as brief as I can, but I did have a lot of asks from Industry, so I'm gonna try my best to get through it all and I apologize, I am going to rely on my notes, because I want to make sure I address all your topics to the best of my ability, but before I do that, I just want to acknowledge Ike, Jane, Jeff, really thank you for your leadership,

partnership, and commitment. We've had a lot of spirited discussions over the years, and we didn't always agree, but, you know, that's okay, because I take it that's because we care, right, so, that's the important part. So, you'll be hard to replace, but I'm sure we're gonna run into you still, and be involved. So, look forward to continuing the relationship.

Okay. So for personnel vetting, Trusted Workforce 2.0, I have some updates. The investigation inventory, that'll be covered later on, and the clearance working group updates, and we understand, you know, we know there's still quite the investigative backlog and, you know, acknowledge Industry's continuing concern. We have multiple mitigation strategies underway to address, to try to get after this, for the high request and submission rate the program is experiencing. We're trying to posture ourselves for the near future expectation of also increased requests, so to address some of these, we are strategically assigning work to areas that have capacity to complete it in the most efficient way possible. We continue to leverage virtual methodologies. We are aligning internal resources to areas with the greatest need, and we're assessing future inventory changes.

As far as Trusted Workforce 2.0 implementation, I've also got some updates on that. We are on track through several concurrent initiatives and aggressive efforts by different DCSA directorates. NBIS delivery and implementation is the highest agency priority, right behind NI2. We're currently focused on dismantling a legacy system landscape and replacing it with a modern user-centric platform. I'm going to talk more about NI2 and NBIS here in a little bit. But as of the end of this month, we will begin development for the individual engagement platform, self-reporting. It's expected to be completed and deployed then. An important note, we hear you. The FSO will not be left out of the self-reporting process and will be included.

Rap Back. That's another topic that everyone's interested in. So, we have Phase 1, 2, and 3 populations. They're all being enrolled concurrently at the fastest possible rate. We're exploring technical options to further increase that rate. More importantly, the list of all Phase 3 personnel, these are people with no prints on file, have been communicated out to Industry, with specific instructions on how to proceed to obtain the fingerprints. That is with a deadline of next year, September 30th, 2027. So, as long as you have claimed your employees through your security management office, your subjects, that are enrolled with IC-specific Rap Back programs, we are trying to obtain those prints first, through those IC-specific programs, instead of having all your people go get new fingerprints. So, I understand that is still occurring, sounds like. So we'll have to look into those instances, because, you know, we are trying to focus on not having to re-finger from people if we already have them on file through someone else. So, as of August 20th, we're about halfway done. There are currently 633,936 Industry personnel enrolled in Rap Back, with approximately another 600,000 remaining.

Okay, moving on to the personnel vetting questionnaire. We're currently refactoring the PVQ initiative and DISS. Changes will be expected to make the platform more easily readable, with less issues pertaining to validation. Additionally, there will be a pre-fill capability for future submissions and form navigations. Rollout began June 1st, with a small group of early adopter companies, initiating the PVQ for 5 year updates, and a broader rollout will follow in the future. As of 18th August, 13 Industry companies have submitted 214 PVQs. I'll talk again more about this during the NBIS update here in a little bit, but developers are working to resolve the issues identified by Industry.

Okay, so with the NISA Working Group, I know you guys brought up the implementation, the rollout to Rev 5 for NIST 800-53. Tracy Brown's gonna talk about that during the NISA Working Group updates.

And then I'd be remiss, you also brought up sanitization procedures from solid state drives, as an open action item. I think from DCSA's perspective, we consider it kind of closed. We formalized our procedures through our DCSA assessment and authorization guide. We've worked with NISPPAC Industry to address any inconsistencies or confusion that they were seeing out in the field and we provided an update to them in June. Spillage mitigation policy is found on the Committee on National Security Systems Instruction 1001. We also let Industry know, you know, you should work with the information owner for allowable dispositions of equipment involved in the spill, and ensure those procedures are approved within your incident response plan.

Moving on to entity vetting, FCL modernization, and FOCI expansion efforts. There's a lot going on in this arena. Entity vetting is working very hard to get their timelines down. Current stats, 77% of mitigation actions are being completed within 45 days or less. 38% of vetting actions are being completed within 14 days. Entity vetting has several initiatives underway to meet the evolving needs of stakeholders, both through process changes and planning efforts, to support the migration of NISS into Increment 2, and also support the FOCI expansion efforts.

Jane stole my thunder. The FCL Handbook was published just the other day, so thank you again, you guys, for working with us and providing feedback. Some changes to highlight in the handbook: we have now FCL adjudication and appeals processes, so you know, that is kind of a due process if someone gets denied an FCL or gets their FCL revoked, that process has been codified now, in ways that they choose to appeal, they can. We also included simple and complex org structures, for all business types. That's one of the many job aids that's out there now. We also hope that will help with the FOCI expansion efforts to make it more readily available what we're looking for, what we need to vet companies.

We also worked with all our stakeholders, government partners in NISPPAC Industry on revisions to the SF328 instructions. The goal was to enable a more efficient and streamlined process to complete the SF328. The instructions have been updated and posted to the GSA form site as of July. The instructions were modified to scope requirements to the information necessary to render a risk determination while reducing the burden on Industry. This will also become increasingly important as we get closer to implementation of FOCI expansion. We've also drafted guidance for change conditions. We have a draft industrial security letter making its way through the coordination process. This will provide Industry guidance on when you need to submit a new SF328. It includes a reminder that your annual self-certification should include that validating that the 328 is still accurate. There's also a recommendation to report change conditions. So this is a recommendation, to report change conditions as soon as they become known, rather than waiting until after an acquisition, for example. Many times we see once a company, you know, you're in a merger and acquisition talks, when you get close to finalizing that acquisition, we've found that typically the the main details of the acquisition don't change all that much, so we're encouraging companies to go ahead and report that once it becomes known, so we can start working with you earlier on potential mitigation, for especially, obviously, I'm talking about foreign ownership.

Alright, some other changes we're working on related to FOCI and FOCI expansion. We are updating our FOCI templates. As Jane also mentioned, the electronic communications plan, but we're also working on the other FOCI templates, too, so it's a little early yet. We're not ready to share those drafts, we're working through them internally, but when they are ready, we will work through NISPPAC to make sure we get your feedback.

Also, to prepare for FOCI expansion coming early next year, FOCI assessments will be reviewed and updated as necessary for those companies currently in the NISP so that as new companies come online with FOCI expansion, we can focus our efforts there, and not on companies that are already cleared. I know we had a question from Industry about our denials or adverse FOCI determinations from other federal agencies reportable to DCSA, and yes, these determinations would presumably be coming from other cognizant security agencies in their respective role to mitigate FOCI and make FCL determinations. It will most likely be shared for reciprocity reasons when both entities have equities.

We also are tracking that NISPPAC Industry has requested a comprehensive implementation plan for FOCI expansion. We've been doing a lot of work behind the scenes on this to be prepared, primarily, we've been focused on internal processes, requirements for NI2 to support it, training, and trying to get our DoW acquisition counterparts engaged. You can't separate FOCI expansion from NI2. It's an integral part of the successful rollout. So Industry, as a key stakeholder, will be included in the requirements and process mapping review first. So that's… that's the first thing we're going to ask, is that you come in, you share with us what you need from a requirements perspective, and then testing will begin in earnest probably, early in the new calendar year.

Okay, now I'm going to rely on my slide. So, NI2. I know you guys have been asking for a roadmap, particularly focused on capabilities. So we are committed to providing a clear, concrete, and achievable roadmap that focuses on delivering real value in the near term. Our plan is centered on transparency, clear timelines, and realistic approach to this modernization. So, first of all, what is NI2? It's a modern, secure, web-based platform replacing our outdated, fragmented legacy systems. Think of it as it will be a central hub for industrial security that brings everything into one place. Why it matters? It moves us from slow, manual, paper-based processes to a digital-first operation. This eliminates redundant data entry, reduces human error, and provides a single authoritative source of information and the key benefit that we're working toward is that it creates a shared operational picture for both Government and Industry. It's designed to provide the right information to the right person at the right time. Timelines and milestones. So, our roadmap to 2027, our path forward is defined by two parallel tracks. Track one is retiring our legacy systems and automating workflows. So, over the summer, we've been working to finalize our data assessment and lock in the requirements for migrating from our old system. This upfront work is crucial to ensure a secure and stable transition. Our current timeline, so by December, this will be a critical cutover. We'll deploy the new modernized industrial security capability within the NI2 platform and begin phased user testing. Early 2027, we'll officially decommission NCAISS. I can attest that it's an outdated and vulnerable access management system. This will simplify and secure user access by managing it directly within the NI2 platform. And then Track 2, FOCI, I know there's a check mark that says delivered down there. From a technical perspective, it has been delivered. I know you guys, it's not out there. You can't use it. We are fully aware of that. We get it. Late this year, we're going to launch the individual engagement platform, which is also the same term you've heard for NBIS. So, for the first time, you can submit FOCI

documentation directly, even before making a bid. So we hope this makes the process more efficient and then the goal of February 2027,that is when we will finalize incorporating the DFARS rule, so we know it's out. There were comments made, but we haven't seen the final DFARS rule. So once it goes out again, once it's finalized, we have to make sure that the system supports whatever those final requirements are. By March, and that's when we're tracking that FOCI expansion could start to be implemented, we will be ready to shift from manual reviews to automated real-time threat detection by integrating new data sources, NI2 will automatically flag potential FOCI risks, allowing our teams to focus on the most critical threats. Okay, the trajectory for NI2. So, our new approach is built on providing clear, consistent, and actionable information. There'll be a unified view, and NI2 will replace siloed tools with a single integrated system. This means everyone is working from the same play book, enhancing oversight and operational efficiency. Our workflows should be automated. The platform automates the routing and tracking of tasks from start to finish. This eliminates offline communication, emails, manual handoffs, ensuring that the process integrity is there in providing clear visibility into the status of any action or milestone and we want to have a collaborative environment. By creating a shared, secure operational picture, we are fostering transparent collaboration between Government and our Industry partners. This accelerates vetting and oversight timelines, building trust, and strengthening our collective security posture. So, over the coming weeks and months, we will not be operating in a vacuum. We are actively committed to a robust feedback loop to ensure the system meets your operational needs. Our product development and customer success teams will be conducting direct, hands-on outreach. The initial outreach will be to obtain input and feedback on DCSA's update industrial security clearance processes and workflow. All strategic coordination feedback collection and updates will be channeled directly through NISPPAC to ensure your voice directly shapes the near-term evolution of NI2.

Okay, and last but not least, NBIS, everyone's favorite topic. So we have our strategic trajectory laid out here. Much the same as NI2, we're executing a systematic modernization of the federal Government's personnel vetting infrastructure. We are actively dismantling legacy IT landscape that has long been limited by fragmented databases, siloed software, and manual handoffs. Historically, systems like BIES, PIPS, and Mirador handled initial casework and ongoing monitoring. These legacy systems are highly transactional, disconnected, and scheduled to be permanently retired in FY28. In their place, we are establishing Integrated Vetting and Monitoring, or IVM. This is targeted for full capability in Q2 of FY27. IVM is a modernized, unified data environment. It automates workflow the moment an investigative request is received, enrolling the individual in continuous vetting, and seamlessly routing it to the final eligibility determination. By transforming from legacy PIPS and VIS to IVM, excuse me, we are turning a slow, multi-layered administrative process into a highly automated end-to-end pipeline, speeding up the investigative process and getting people to work faster.

On the front end, we have the applications you may be more familiar with, such as the Individual Engagement Platform, or IEP, which acts as our direct portal for applicants. IEP feeds into DISS, which houses our joint verification system for security officers, our case adjudication tracking system for adjudicators, and our specialized appeals module. Okay, and then my final slide, the NBIS Progress Overview. This is our high-level roadmap. So to support the planning and preparation and ensure absolute transparency, our roadmap is structured around clear, incremental software releases. This is a very high-level snapshot based on capability releases and trusted workforce milestones. We are

building an operational customer roadmap. This will be our external customer-facing guide. It will be written in plain jargon free operational language, specifically designed to showcase critical process functions and outcomes. It will map out clear software release windows, transition periods, and exactly when legacy systems will retire, giving your team plenty of runway to adjust without any operational hiccups. We are targeting to have this ready for you this month in September. To back that up, we also have our internal product delivery roadmap. This maps out the deep underlying technical execution and deployment phases required to make sure we actually hit our customer-facing commitment and milestones. By running these roadmaps in parallel, our ultimate goal is to give you alignment, execution, and compliance. We want to take the guesswork out of NBIS deployment so you know exactly what is coming, when it's coming, and how to prepare and then just really quickly, I wanted to kind of walk through a few of our key applications, so I'll give you a few more details.

I'm not going to go through this entire timeline, but a few things I want to point out: CVS to JVS. The goal to transition from Central Verification System to the DISS Joint Verification System, JVS, is our single low-side repository. So, hard milestones and releases. In May, we enabled the federal agency adjudication rules. We automated scripts successfully to migrate and assign those federal agency adjudication roles to active CVS users. In July, we delivered mass adjudication and file release requests to support the data quality initiative. And this month, CVS transitions to read-only, and JVS becomes the system of record.

Current action items and support. So, in agency action, we are ensuring all personnel are correctly mapped to their security management office in DISS. Our target window is Q4 of FY26. That's our final low-side data migration and low side repository consolidation, and then CVS becomes read-only and then we have support availability. We have system liaison office hours Monday, Wednesday, Friday from 12 to 2 Eastern Standard Time.

Another initiative is the Initiate Review Authorized Migration to DISS JVS. So we have transition deadlines with no downtime migration. So by September 30th, we will have new case initiation completely ceased in the legacy IM agency system and then by November 30th is a hard deadline for processing in-flight cases. Legacy IM agency system sunset begins. And then future rollouts scheduled, resolving MVP operational gaps. In July, we delivered pre-fill case reports, and email editing. In August, we deployed the split case capabilities mass subject initiation and DISS IRA tracking in the IEP status tracker. By September 24th, we will deliver return case submissions, progress saving tools, and countdown timers. And then the goal by October 30th, finalizing correction email previews, multiple order form templates, and auto-required field indicators. And then, more details on the individual engagement platform and self-reporting. IEP is our unified user-facing web portal. It transitioned our process from ad hoc, reactive actions to a proactive self-service model. So, as I said, this month we'll launch the self-reporting Capability IEP. It will allow applicants to report out-of-cycle life events, such as foreign travel or marriage, directly via an interactive PVQ-mapped online module. The FSO paradigm shift enhances the FSO role from manual data entry to high-level strategic oversight. FSOs remain integral to the process, but rather than transcribing data into a blank form, they receive a pre-validated digital package to review. Okay, so what's next for FY27 in Q1 and Q2? There will be event-driven notifications allowing agencies and industry partners to configure custom alerts for self-reported changes. And then finally, the PVQ phased rollout, we are tying our initiation and self-reporting systems together, and

the refactored PVQ accessed through the eApp interface. So, PVQ will be implemented in phases. In July, we launched an NGA/Industry pilot and DCSA employee 5-year updates. By the end of this month, we will begin integrations with the MILDEPS, HR systems, and eApp, and then Q1 FY27, PVQ will be live for DCSA as an investigation service provider, followed by non-DCSA ISPs, and then by March 2027, we will launch PVQ for all initial vetting scenarios, and then by this time next year, we should have full operationalization of the PVQ for all vetting scenarios enterprise-wide and standard legacy forms, like the SF86, would be sunset. So this concludes my remarks for today, but I will pause for any questions.

Michael T.: Alright, Allyson, thank you very much. Questions?

Jennie: Allyson, thank you so much for those remarks, and for being such a great partner to us. I want to just shout out how much I appreciate the updates that you provided for NBIS, but mainly for NI2. That was really helpful to see that information, and we look forward to continuing to work with you.

The comment I'm about to make, you may not be able to answer, but I want to say it early for the sake of the other people that are going to participate in today's forum, that they may have answers to this too, and it has to do with Rap Back Phase 3 and the lack of reciprocity between agencies. So, we appreciate that DCSA is willing to reach out to other agencies to pull prints. The super heroes, formerly known as the liaisons, have been wonderful to clarify that they need the individual's name, agency, and a POC, and they will reach out to those agencies. It's a very painstaking process, but to attempt to get prints. All that said, to my knowledge, DCSA is the only agency reaching out to other agencies to get prints, and with all agencies having the Rap Back requirement, I'm curious to know if you are receiving requests from other agencies to do the same to manually request reciprocity?

Allyson: That's a great question, and you're right, I'm not able to answer that, but I would be curious to hear from other people presenting if they are undergoing the same initiatives. But I will take that back, that's a great question.

LaToya: So I actually have a question in regards to the IEP. You mentioned that the FSO will be a part of that workflow for the IEP. This is actually the first time I've heard that since the CAB, where it was kind of a bit of confusion, in regards to the FSO being involved. Industry looks forward to seeing that, hopefully, ahead of it being deployed, because one of the things that stood out to me was, that you mentioned is strategic oversight, and further definition on that is what I'm looking for, because is this gonna be… you know, there's a lot of questions that I have when you say strategic oversight.

Allyson: Right, so yeah, the way I understood it and what I was provided is that, yeah, you will receive those pre-filled questionnaires so that you can review it, validate it, and it would be then submitted. I don't know if I have anyone here on the line who can elaborate, but that is my understanding. I don't want to speak out of turn.

LaToya: No pressure at the moment, but we definitely want to have a follow-up conversation, sooner than later, to make sure that we understand exactly what we are going to receive at the point of the IEP being deployed.

Allyson: Absolutely.

LaToya: Thank you.

Leonard: Allyson, I just want to say, and this is really for you, Heather, as well, for the record, that I concur the solid-state drive matter is closed. It is done. It was resolved and addressed. Thank you.

Allyson: Great. Thank you. See, we can cross one item off the list. That's a win.

Jeffrey: I think we might have some work to do on the IC side, right, but I'll take the win, right? So, thank you.

Michael T.: Other questions? Alright, with that, we are ready for a break.

Heather: Next, we will hear from Ms. Lisa Perez, the Chief of the Policy and Collaboration Group, Security Directorate, National Counterintelligence and Security Center… Security Center, Office of the Director of National Intelligence. Lisa?

Lisa: Yes, can you hear me?

Heather: Yes, great. Thank you, Lisa.

Lisa: Good afternoon, everyone. So, to Jeff, Jane, and Ike, I always want to take a moment to say thank you for your years of engagement as a member of the NISPPAC, as well as for the many accomplishments made as part of your involvement. A lot of great things have been said about you all today, so know that you essentially leave a legacy.

And then SEAD 4 was one of the things we were asked to provide an update about. So we're thankful for the NISPPAC Industry representation during the comprehensive research phase that led to the recommendations for the revisions with the Security Executive Agent Directive for the National Security Adjudications. We did complete an initial draft of the directive, which NISPPAC Industry representatives provided review and perspective via comments, which have since been adjudicated into a draft, that we are in the early stages of interagency coordination and currently, of course, that engagement is happening with our legal counsel. We are aiming for October for issuance of that.

And then the ICD 705 is another topic we were asked to provide an update on. So in relation to ICD 705, the Director of National Counterintelligence and Security Center had issued I think the last memo that came out was 6 August 2026, and in that memo, it clarifies how currently accredited legacy SCIFs built per pre-ICD 705 standards, such as if it was built under DCID 6/9, how they may continue operating, but of course not indefinitely. They must be evaluated at least every 5 years, with normal maintenance and repairs as the way of addressing deficiencies, and of course, if protections are found to be obsolete, or if they cannot be remedied, the SCIF needs a waiver to keep operating, and must be scheduled for upgrade or reaccreditation to the ICD 705 or decommissioning.

Now, going forward, right, a lot of changes are happening, so going forward, we are working on revisions to the Intelligence Community Standard documents to incorporate feedback from Government and Industry partners, and update language

to reflect guidance issued in these recent memos, the one I just mentioned, and then the one previously.

Sharing of covered insider threat information policy. I did hear that come up as well today. So as you heard earlier about that, a policy on sharing covered insider threat information was developed and coordinated. We are thankful to NISPPAC Industry leadership for their review and sharing of perspectives that were helpful in drafting the version submitted into our internal agency review process. We've had some staffing changes within ODNI that led to a pause in the internal coordination of this particular policy document. So, good news is we do now have personnel in place to revive this coordination. I'm expecting work will pick up on within probably the next few weeks, so, if focus can stay on the final coordination efforts, I'm confident the policy will be issued well before the next NISPPAC meeting,

I saw in the agenda online that there was, a topic of TORIS, and so many of you have probably recently heard about TORIS, or heard some more information about TORIS, so I don't have a whole lot new that I can share, but just to provide you a little bit more information, or reiterate information you may already know, so the Transparency of Reciprocity Information System, TORIS, will make relevant intelligence community personnel security data available to agency decision makers when they need it as part of the personnel vetting. So what this means for Industry is improved applicant experience, where individuals who will become part of the intelligence community will use the same form for filling out security paperwork, a reduction of duplicative personnel security paperwork, that's the goal, and then such as the personnel vetting questionnaire, where that individual will fill out once, rather than multiple times, or once per customer or employer, so, greater mobility, of course for cleared contractor personnel with faster transfer of trust decisions, because the right information will be available to the right people in the processes of these transfers and then improved data sharing amongst agencies with standardized security data formats and sharing mechanisms within the intelligence community bidirectional sharing with NBIS, of course, and then moving towards the personnel vetting record standardization for the community. So we look forward to continued engagement on this advancement of TORIS development, and the first iteration of that personnel vetting questionnaire will be launched on JWICS in February 2027 and of course, I am hopeful to have more implementation news at our next NISPPAC meeting and that's all of the updates that I have, or at least all the things I heard that I needed to provide some more response on, but happy to try to answer any questions.

Michael T.: Thanks. Any questions for ODNI?

LaToya: Yeah, I do.

Michael T.: We'll go to the table, and then…Go ahead, Latoya. Please go ahead.

LaToya: Oh, I'm sorry, okay. Lisa, thank you so much for those updates. I do have two questions. The first question is referencing what you said at the very end about the first iteration of the PVQ being released next year. Is that a different version of PVQ, or what PVQ is that?

Lisa: No, I'm referring to the functionality of it. So it's the same form, it's just that, when it's there, I think initially, right, it'll be a first full form completion. I don't know that it will have the ability to go in and do updates of just sections yet. That will just be the… in other words,

someone may be potentially coming in new, they'll fill out that full form for the first time. That's what will be available in February 27th.

LaToya: Okay, and is the goal of that PVQ to be utilized across the IC agencies, or is it specific agencies that will or won't be using this form?

Lisa: So our ultimate goal is that it will be used by all the IC agencies. However, you know, it'll be an iteration of how it's adopted.

LaToya: Okay. The following question I have is in regards to, the policies that you've stated are in coordination. So, you've mentioned that the comments that we've provided, and this is in reference to all of them that you've talked about in your briefing but you've mentioned that the comments that Industry provided have been adjudicated. Is there an appetite to allow a review of those adjudicated comments to ensure that the intent of what we provided in the comments are received in a way that helps implementation and doesn't drive us backwards once the policy is released.

Lisa: So the instruction from our leadership was to get the comments, conduct the adjudication, and not just with Industry, but with the internal other agencies' review as well, and then to move forward because they were trying to truncate the issuance of it.

LaToya: Okay, so, Industry would like to request a follow-up conversation in regards to those adjudicated comments. We provided quite a few of them, and some of them, we are afraid that they could be misunderstood. And this is just from the respects of how the policy that was released in regards to what we consider the overhead billets policy, how that was put out, and I think that some of that information may have been misunderstood. So, again, Industry would like to have a follow-up conversation to review or to discuss, how those comments may or may not have been included in the, the policy that's currently going through coordination.

Lisa: Yeah, we're happy to set up something with leadership. I would say with respect to the overhead billets, or not the overhead billets, the key management personnel, is that what you're talking about, and the oversight personnel? Yeah, so that one was constrained by what specifically is in the statute, so not so much our decision on adjudication of comments, just for everyone's awareness.

LaToya: Thank you.

Lisa: Thank you.

Isaiah: Hey, Lisa.

Lisa: Yes, hi.

Isaiah: Hi, this is Ike. I don't want to beat the dead horse when it comes to the Insider Threat for Covered Employees. However, we started talking about this at the public meeting in 2022.

Lisa: Yes.

Isaiah: As was mentioned, right? I'd be remiss if I didn't sit here in front of a room full of Industry personnel to say that 4 years is a lot of years, and I know we've been changing administrations, but Industry was asked numerous

occasions to provide some input, and we did, and we have to move this across because we have Industry companies that are out there that have to take individuals back from agencies that are sending them back with no information, and companies have to make a decision whether or not they're going to keep that individual not knowing why they were sent back. That is a risk, in a huge way.

And we don't to have to come together again and say, we really gotta do it now because somebody just went into an office and shot up the place, right? I only can say it that way, because that's what really could happen here when you don't know why someone has been sent back from an agency. So, Industry NISPPAC and the Industry at large pleads with ODNI to try to see how we can get this pushed over the finish line, because 4 years is a long time. Over.

Lisa: I fully understand. Thank you very much. Again, I'm hopeful that this will be revised, here in the next coming weeks, again, it was in the internal agency process. It just paused in there, with the change of personnel, but again, people are now in place again, and we'll be able to pick back up on that.

Michael T.: And Lisa, we have another question for you in the room.

Lisa: Okay, thank you.

Mike Dillemuth: Hello Lisa. Lisa, my name is Mike Dillemuth with Dillemuth Security Services. I want to take you back to ICD 705. Based on your comments, I'm not sure you're going to be able to answer this question, but let me at least ask it, just in case. I've received numerous or several inquiries from my Industry colleagues on when will the next update to the ICD 705 tech specs be published and the big concern is, at least for the people that I'm working with in construction, is the lack of the templates and the checklists that were in the previous edition, but got deleted from the current edition, but are expected to be in the upcoming edition. And so there's a constant inquiry, like, when is the next edition going to be published?

And a second question, sort of related to that, about a year, year and a half ago, somewhere around that time, I believe the Government said they were gonna update or publish some new ICS 705s, dealing with the construction of data centers, medical devices, inside SCIFs, things of that nature. Like I say, about a year, year and a half, give or take. Any idea when any of those ICS documents will be published, and any idea as to when we can expect an update into the tech specs for 705?

Lisa: I do not have an expected completion for any of these items, and the latter two, I'll certainly have to take back and inquire, where those are in terms of, are they being worked or who's working them? But with regard to the ICD 705 stuff, they are feverishly working, and again, there'll be coordination with agencies and Industry representatives to try to get it all finished, but again, they're definitely working feverishly. Like I said, the other memo I just mentioned, it just came out a matter of days ago, so they are working hard.

Mike: Fair, fair enough, thank you.

Lisa: Thank you.

Isaiah: For the gentleman that just spoke, just make sure you reach back out to Industry NISPPAC. Kathy Andrews will be your point person, and we can get

that information. She will work through ODNI to try to get that information, and as she does, she'll ensure that she…pulls that back out and shares that with Industry. Over.

Mike: Thank you.

Michael T.: Thanks.

Lisa: Thanks for adding that, Ike…

Michael T.: Yeah, thank you, Lisa. Any other questions for ODNI? Alright.

Heather: Thank you, Lisa. Thank you, everyone, with questions. Next, we will hear from Don, the Chief of the Central Intelligence Agency's Security Policy Staff. Don?

Don: Good afternoon. I think the only thing we wanted to address was the question for all the agencies with regard to the memo, the DNI memo having to do with the certain contract personnel, the overhead personnel, and implementation. The only thing we can give at this point… that just came out a couple months ago, so, the agency is currently reflecting on the requirements in that memorandum and trying to determine how implementation will actually be carried out. There's a lot of players in that, as far as how we do things contractually, and we'll provide more information as soon as available. That is all I have, unless you have questions.

Michael T.: Alright, thank you, Don. Any questions for CIA?

LaToya: I do actually have, more so of a comment. Don, you may want to get with Lisa Perez on that, on that policy, because there is a current review happening of that policy and the language that's included for some revisions, so you may want to get with her before you take too much time on implementation.

Don: Yeah, thank you, LaToya. I actually have been doing that, and I have seen the changes on that, which aren't ready to be discussed yet, but yeah, thank you, we're, we're on it.

LaToya: Thank you, Don.

Michael T.: Yeah, thanks, Don. Any further questions?

Heather: Alright, thank you. Next, we will hear from Ms. Breanna Palmer, the Deputy Director with the Office of the Chief Security Officer at the Department of Homeland Security. Bre? So I do know…great, fantastic, you are there.

Breanna Palmer: Hi, yes, good afternoon. I apologize, I'm in the field, so, I don't have camera, and I may have to run, depending on the storm status, but good afternoon, everyone, happy to be here. DHS really didn't have a lot of questions that were sent out by Industry, so, as far as updates, I can tell you that we are actively working in the Trusted Workforce 2.0 space and I do have statistics to show kind of where we are with that implementation and how that impacts Industry specifically. We're also pushing out, what's called the Enterprise Secure Forms System, which is ESFS, and what that does is our contracting officer representatives, they reach out to our Industry partners, and it's a way to bulk import all contract personnel into our integrated

security management system, since we don't necessarily use DISS/JVS. Yeah, what questions can I answer for everyone today?

Michael T.: Questions for DHS?

LaToya: You just mentioned that you guys don't use DISS/JVS. Is that the plan for you all not to utilize DISS/JVS at all?

Breanna Palmer: So, we use it, it's just not our primary source. Our primary source is the Integrated Security Management System and we use DISS/JVS for reciprocity. Currently, only TSA uses the NI2 portal. Everybody else, all of the rest of the components are currently using ESFS and the ISMIS system.

LaToya: So is it safe to say, based off of what I just heard you say, that, that DHS information will not be in DISS/JVS?

Breanna Palmer: No, we participate. We put our information in there. We do participate in the information sharing, but all of the case management occurs in the integrated security management system. So we share the information. DISS/JVS does have it, so for reciprocity and transfer of trust, it's available there. That's just a repository for us. It's not active for case management.

LaToya: Okay, thank you.

Breanna: Yes.

Michael T.: Any further questions? Thank you very much, Bre.

Heather: Next, we will hear from Ms. Monica Marks, the Director of the Office of Departmental Vetting and Assistance at the Department of Energy, who will be providing their update. Monica?

Monica: Thank you. Do you have my slide?

Heather: This is just for the update.

Monica: So we, did anyone have any questions for DOE?

LaToya: I actually have a, not so much of a question, but more of a comment. I've been receiving quite a few questions and concerns across Industry in regards to DOE. I didn't have a lot of time to submit anything, you know, to give you time to be able to research, but I do want to follow up with you at a later point, so that way we can start to engage a little bit better between DOE and Industry NISPPAC, to address some of those concerns that we've been receiving from some of our Industry, members.

Monica: Absolutely. Okay, thank you. Did anyone have anything else? Okay.

Heather: Next, we will hear from Mr. Michael England, team leader for the Security Operations Team with the Nuclear Regulatory Commission, who will be providing their update. Mike?

Michael E.: Good afternoon, everyone. A quick update for the NRC. First we want to answer the Industry questions. The NRC went through a historic reorganization, agency-wide, starting on June 15th. So, what that means for the group is, when it comes to training and certain CIO governance models, we are in the act of trying to find bodies to put in those positions. Our Chief

Human Capital Officer is working to fill several vacancies, so for Industry, we are not not answering your question, we just don't have anybody in the position to answer your question, so we're quickly trying to work that out and also, that goes for Industry also, too, when it comes to our clearance timelines, they went up a little bit due to the amount of vacancies we have to fill, and we're trying to fill newly created positions. That's all I have for the NRC. Any questions?

Michael T.: Any questions for the NRC? Alright.

Michael E.: Thank you.

Michael T.: Thank you very much.

Heather: We are now going to hear from Ms. Tracy Brown, an authorizing official representative for the NISP Cybersecurity Office. Tracy? Sorry, hold on. I'm so sorry, folks. Got a little bit ahead of myself. Alright, we're now going to hear from Ms. Bre Palmer again, the Deputy Director with the Office of the Chief Security Officer at the Department of Homeland Security, Bre?

Breanna: Good afternoon again. So, I know that for our industrial partners, predictability and speed in personnel vetting are critical to staffing your programs and delivering on your contracts, so today, I'm just going to walk you through our fiscal year 26 quarter 3 metrics, focusing on how our processing timelines and continuous betting programs are impacting the cleared workforce.

At the enterprise level, DHS has completed 21,545 personnel vetting cases this quarter. Looking at our overall timeline averages, reciprocity is around 10 days, preliminary determinations average 25 days, and final determinations are averaged at 100 days. For Industry, that 10 day reciprocity number is the key highlight. We're moving cleared personnel into the system quickly on the front end. Our total vetted population currently stands at roughly 508,000. Within that, 323,000 are national security eligible, or the NSE category. We know that a significant portion of this NSE population relies on your highly specialized and technical engineering workforce.

On the continuous vetting front, we're managing a massive scale, over 233,000 individuals enrolled in continuous evaluation, and over 285,000 in Rap Back. We processed over 500,000 alerts this quarter, maintaining an average continuous vetting adjudication timeline of 13 days. We're operating at a high volume, but the system is managing the payload efficiently. Next slide, please.

This slide tracks our entry on duty, or EOD, timeliness. Overall, the time for a favorable onboarding determination increased from 35 days in quarter 2 to 42 days in Quarter 3 and in order to be transparent, I just want to let you know what is driving that 6-day increase. First, we saw a massive surge in complex national security cases, which more than doubled, from 79 in quarter 2 to 185 in quarter 3. Second, the investigation timelines grew slightly, across the board, however, when we break this down for our contract workforce, the front end numbers remain highly competitive. For contractors, reciprocity averaged just 13 days, and preliminary investigation determinations averaged 17 days. We know that your time to hire is critical. These metrics show that if you bring us a cleared candidate, or someone needing an interim approval. We are getting them approved and onboarded in roughly 2 to 3 weeks. The bottleneck remains in the downstream investigations, which average 76 days for

contractors. While this is nearly a month faster than the federal employees of 103 days, we know that the delay impacts your program readiness, and it remains a primary focus for our leadership. Next slide, please.

So this slide details, more of our EOD timeliness broken down by individual DHS component. As you know, working with different components within DHS can sometimes mean navigating different administrative cases. When reviewing this component level data, we're looking at both volume and duration to identify our bottlenecks. For Industry partners, the takeaway here is that we're using this data to identify outliers. Our goal is to standardize the onboarding experience so that your personnel experience predictable, consistent timelines, regardless of whether or not they're supporting CISA, CBP, TSA, or any other component. Next slide, please.

Turning to our continuous vetting, I want to address how this impacts the cleared contractor workforce. As mentioned, we generated over 500,000 CVS alerts this quarter, however, I want to draw your attention to the risk distribution. 92% of these alerts are classified as low risk, only 6% are medium risk, and just 2% are high risk. This should be highly reassuring to Industry. It demonstrates that the transition to continuous monitoring is working exactly as intended. We're successfully triaging a massive amount of data without creating a flood of false positive clearance suspensions for your employees. We're also prioritizing that 2% of high risk alerts for immediate attention, while processing the low risk alerts efficiently so they don't disrupt your workforce. Next slide, please.

So this slide focuses on SEAD 3 self-reporting. We completed 18,000 self-reported cases, primarily driven by foreign travel and financial disclosures. We appreciate the rigorous compliance programs you've implemented within your companies to educate your workforce on SEAD 3. You're doing your part to report these activities. Our operational objective and our commitment to you is to ensure that our closure rates keep pace with your incoming reports. We're actively monitoring this pipeline to ensure these self-reports are adjudicated quickly, so your employees' clearances aren't left in administrative limbo. Next slide, please.

So, to wrap up, DHS is processing vetting at an immense scale, and we are heavily focused on protecting the rapid onboarding pathways for our contract workforce. Through our quarter 3 data review, we identified several administrative challenges that we know caused friction for Industry, specifically inconsistent tracking of reciprocity and legacy data errors caused by copy and inherent functions in our tracking system. We know that these are exact, that these are system bugs that cause cleared contractors to get stuck, so, in order to fix this, we've launched a data integrity action group to clean up our data sets, and we're rolling out standardized sessions to ensure reciprocity is processed identically across every DHS component. We're also looking at and evaluating, go ahead and next slide for me, I'm sorry. Yeah, I think I skipped ahead, I apologize. We're looking at implementing AI to work with our data cleanup, so we're introducing AI to our integrated security management system. It's going to look for blank spots, errors, numbers that seem erroneous or out of place, dates where there should be text, text where there should be dates, and we've got our analysts actively going through those responses as we try to standardize. This is just analysis of the metrics from fiscal year quarter two, up to 26 quarter two to quarter three. Next slide, please.

And I already spoke to this slide. Again, it's just our case data integrity, data entry, and metric calculation, and reciprocity. It's an ongoing process for us. Next slide, please.

Again, data cleanup. As I mentioned, we're using AI to go through these reciprocity data issues, identifying where special sensitive is identified in a data set. However, per policy, the position should have been preliminary determination, so we're seeing lots of errors, and we're trying to correct and standardize that where the intent is that we will be on one standardized system by quarter four of fiscal year 27, ISMS will look the same across the board. Next slide. Alright, thank you. Does anybody have any questions for me?

LaToya: I have a question. Sorry. For DHS, is the plan for PVQ implementation in line with the path that DCSA is going, or do you guys have a different timeline on implementation?

Breanna: No, we're on the same path as DCSA.

LaToya: Okay, perfect, thank you.

Michael T.: Further questions? Alright, Bre, thank you again.

Breanna: Thank you.

Heather: Thank you. We are now moving into the portion of the meeting where we get reports from the NISPPAC Working Groups. You have already heard from Industry, along with the CSAs and CSOs, on the high level points of what was discussed during the NISA Working Group, which took place on August 18, 2026, and the clearance working group, which took place on June 24th, 2026. We have also heard from DHS. In addition to DHS, we will also hear from DOE and the NRC for their security metrics, along with DCSA for their information systems and personnel security metrics. One working group you have not heard from is the newly approved Artificial Intelligence working group. It is expected to initially be comprised of those in the NISA Working Group. They have not yet met, but updates will be provided as appropriate.

We are now going to hear from Ms. Monica Marks, the Director of the Office of Departmental Vetting and Assistance at the Department of Energy, who will be providing the metrics. Monica?

Monica Marks: Good afternoon again. Okay, so this is the past year of DOE's process and timelines. As you can see, we did have a slight increase last year based on the workforce change we had, and the lapse of appropriations, However, we have recovered, and we're now meeting all of the former IRTPA standards. So, just for this last quarter, for top secret clearances, our initiate timeline has been 6 days, where the goal currently is 14 days. The investigate timeline by DCSA was 54 days where the goal is 80 days, and the adjudicate timeline was 17 days, where the goal is 20 days, which made our average top secret onboarding for initial 77 days versus the 114-day goal.

For secret or Tier 3 level clearances, we initiated within 5 days, where the goal was 14 days, investigate 45 days where the goal was 40 days. Adjudication timeline was 17 days, where the goal was 20 days, bringing us to a 68 day total for favorable to onboard, versus the 74-day goal.

I've removed the periodic reinvestigation timelines, as we've nearly eliminated that, but in quarter four, we did complete 6 top secret PRs based on issues we

found. The initiate was 16 days. Investigate was 236 days, and the adjudicate was 281 days, bringing the total PR timeline to 533 days, but that was based on seriousness issues.

So, we've recovered from the shift in workforce and a lapse of appropriations since last summer and autumn, and we're now meeting all IRTPA goals and working towards the 2027 and 2028 PMIG goals for both secret and top secret.

This slide will be provided. It's just a monthly breakdown, so you can actually see where the times increased, and you can see what was going on across the Government at that time, and how we recovered.

So this one is for Top Secret, the next slide is the same for secret. So for continuous vetting enrollment, we currently have 120,000, just almost 121,000, national security sensitive individuals enrolled between the ODNI CE system and DCSA CV service. We also have 57% of our non-sensitive public trust individuals enrolled in DCSA's CV service. Our total CV enrollment is 124,775 people. We are currently in transition from the ODNI CE system completely to DCSA's CV service which we expect to be completed by the end of this quarter, this month.

So, for continuous evaluation, alerts for just one quarter, we had 502,385 alerts. This is broken down by the seven categories of information. We expect this to decline drastically as we transition from the ODNI CE system to DCSA CV service, as they will do our triage for us and validate the alerts, because a lot of the alerts are either not valid to our individual or don't meet an investigative threshold or it was information already known to the agency, so, we don't expect to have a half a million alerts next quarter, and if we do, we hope to have it by the second quarter of the fiscal year, once our transition is complete for our national security sensitive population. I think that's it. It is. Are there any questions?

Jennie: I have a question, please, and thank you very much for that update. You mentioned changing over to DCSA's CV service. How are you handling Rap Back enrollment? Are you also seeking prints yourself, or are you leveraging the DCSA data?

Monica: So, we've always used DCSA. So, our national security sensitive population has been fully enrolled in DCSA for over 2 years now, and we're also adding our non-sensitive public trust so, where you saw that we have 124,000 people enrolled in CE, that same population is enrolled in Rap Back. When we enroll someone in CV, we also submit them for Rap Back enrollment, and understanding that DCSA CV service is about to encompass Rap Back and it won't be a separate enrollment, we plan to still have that transition to be seamless.

Jennie: That's great, and just a quick follow-up question with regard… we heard from DHS on using DISS/JVS just as a repository for data, so that we can share information for reciprocity. How does that stand with DOE and NRC?

Monica: So, for DOE, I cannot speak for NRC, but for DOE, we've always used CVS. And we hope that all of our data will transition from CVS to DISS/JVS. We also hope to be early adopters for all of the shared services that DCSA offers, however, we're working closely with their system developers and OCS on ensuring that the systems meet DOE's needs but we do plan to use it as, at a minimum, the repository, and continue to meet that requirement.

Jennie: Thank you.

Monica: You're welcome. Are there any other questions?

Michael T.: Alright, thanks very much.

Heather: Thank you, Monica. Next, we will hear from Mr. Michael England, Team Leader for the Security Operations Team with the Nuclear Regulatory Commission, who will be providing their update. Mike?

Michael E.: Good afternoon once again. So, first of all, let me start by saying I'm on the physical security side. I can see the personnel security side, so if I say something, please don't hold me exactly to it because I don't want to get them in any trouble. So, next slide.

Okay, so overall agency performance is trending in a positive direction. Our quarter data shows substantial reduction in processing time for both top secret and secret clearances. From FY 25 Q4 to FY 26 Q3, our total average processing time declined from 163 to 90 days for Top Secret, about a 45% improvement, and from 148 to 79 days for secret, an improvement of about 47%. The largest mover that contributed the biggest improvement is the investigation phase, which fell from 139 to 49 days for top secret, and 103 to 48 days for secret. Next slide.

As you can see, though, at the same time, our workload increased, especially in our top secret arena, and increase to 195 as compared to 107 in Q2 and 58 in Q1. We're contributing this workload dealing to the reorganization, and dealing with unexpected retirements from the agency, and bringing in new people to replace those that retired, so that bumped our workload. Next slide, please.

So as you can see, for our top secret, our processing time improved for both our top secret clearances and our secret clearances, our initial bunch, for our top secret clearances, we went to 84 days for processing a full top secret clearance, and in our secret clearances, we went down to processing in 69 days. The key takeaway from these slides is our timelines have improved materially on a quarterly basis from top secret to secret, even as our reported adjudication workload increased. Our investigation timelines increase. One of the biggest drivers that's kind of pushing our numbers back in the wrong direction, our reorganization and our hiring push. We're bringing on about 600 new people, and we know that's going to skew our timelines a little bit. So, we're trying to plan for that, and we're trying to right size our workforce to make sure we can meet this new barrier that's coming our way. Next slide. I think that's it. Thank you. Any questions?

Michael T.: Alright, thank you very much.

Heather: I apologize, Tracy. We are now going to hear from Ms. Tracy Brown, an authorizing official representative for the NISP Cybersecurity Office. Tracy?

Tracy: Thank you. Good afternoon, everyone. As Heather said earlier, I am Tracy Brown. I am an authorizing official designated representative for the NCSO office at DCSA, and I will be providing our updates.

Currently, we're overseeing a little over 4,300 systems, with an average authorization time of 58 days, and that's down from 65 days in 2025. Last month, we started transitioning our risk management framework controls from NIST 853, which is for National Security Systems, CNSSI 1253, Rev 5. As of

August 17th, we were tracking 783 systems as migrating to Rev 5. Since that time, I'm sure we have more, but I can provide the current update later. In preparation for the transition, DCSA performed several internal and Industry training sessions to support Rev 4 to Rev 5 migration, in coordination with NISA working group partners. We acknowledge the concern Industry has with the accelerated transition timeline, and we ask Industry to remember that we do have RMF tools in the bank, that we can use, industries allow to POA&M, telecontrols out with justification, present mitigation strategy to meet the intent of the controls, or risk acceptance from the customer.

DCSA continues to partner with our DIB partners, as well as their customers, to ensure that we can assist them to meet mission requirements as part of our transition plan. All new systems presented to us for authorization must meet Rev 5 compliance. Systems transition prior to our July 30th date in process under Rev 4 will continue through the process. The authorizing officials can authorize those systems up to 180 days. Right? With Industry having a mandatory requirement within the 90 days to do the administrative migration workflow. This is an administrative update records, and it does not require Industry partners to submit new authorization workflows, nor does it impact current authorization statuses, existing termination date, system details, or assigned personnel roles. What Industry would have to do now for all of their systems of record, they will need to initiate the eMASS Revision 5 migration workflow. A formal authorization workflow is only required if the system is seeking initial authorization, it's approaching its termination date, or you have a security development change that you need a new authorization decision. In support of this transition, DCSA, we published several reference materials for Industry to use, and those reference materials are found in our eMASS section under the help. We have other Industry engagements that we do meet with the NISA Working Group as requested to discuss challenges that people may experience, and we work to help, to work through those challenges.

Just a little quick update on our core program. We are 91% complete of our goal for the year. We will meet all of our goals and we have a 70% pass rate today. Questions?

Michael T.: Alright.

Leonard: I have a question on this one.

Tracy: Okay.

Leonard Moss: We wanted to present you with this NISPPAC coin. Thank you for all of your amazing support.

Tracy: Thank you.

Heather: Thank you, Tracy. We are now going to hear from Mr. Thomas Giancoli, Branch Chief, Personnel Security with DCSA for their statistics. Tom?

Thomas Giancoli: Hey, good afternoon, everyone. Quick comms check, can you hear me okay?

Heather: Yes, we can, thank you.

Thomas: Excellent. Well, good afternoon, everybody. You can go ahead to the next slide, please. I'll be providing some inventory and timeliness metrics for all DCSA products and services. There's a lot of information here, so I'm

not gonna go through every data point, but we will have some time for questions at the end.

So let's start with our investigative and adjudicative inventory, and that's on the upper left quad of the slide here. So, for the investigations program as a whole, our current inventory stands at approximately 130,000 cases again, not just for Industry, but just in general, 130,000 cases, which is a decrease of 41,000 cases, or…24% reduction for FY26. We also have approximately 34,000 issue resolution cases, and what that means is so, for our continuous vetting service that we offer, we are conducting issue resolution based off of TW 2.0 Appendix I requirements and that inventory is at about 34,000 cases that we're working through and conducting those additional investigative actions based on the policy in TW 2.0.

In terms of DOW Industry community investigation inventory of the tiered cases stands at 19,000, which is 7,000 Tier 5s and 12,000 Tier 3 cases during FY26, this inventory has decreased by 5,000. So, I'm not going to get into the specifics on why the inventory has decreased within DCSA as a whole, and specifically for Industry community, but there's a few large scale initiatives that we undertook over the last year or so that have contributed to this reduction in inventory, and one of them is the early integration of TW 2.0 standards. A few initiatives, coverage requirements that we implemented ahead of the target dates, as provided by the EAs. That was a significant contribution to the reduction in inventory. The elimination of PRs, which I've heard from a couple other departments and agencies is something I think that this is a Government-wide initiative, so elimination of PRs, and I will say, beginning in as of this July, all requests for PRs have been sunset, and I know for the Industry community, that happened, I think in FY24, so and then, expedited screening. This is a process that we've implemented to help with our closing of cases. It's a detailed process I'm not going to get into right now, but all of these initiatives have really contributed to that reduction in our inventory. I will say that, despite the inventory decreasing for FY 26 overall, there has been an uptick, within Q3, which is primarily due to the elevated request for the initial vetting, and the scenario investigation that we've received since February, and this includes Industry as well. So, we have seen a slight uptick in the requests for Q3, but overall, again, inventory's still down.

Okay, so we can move to timeliness now. And I will… I think I provided this during the CWG meeting in June, but it's an important consideration to understand, is that so, to align with the performance vetting… I'm sorry, Personal Vetting Performance Management Standards Implementation Guidance, so this is the PMIG, these are the timeliness metrics that are identified and established by the EAs. So to align with that, we have changed how we are reporting timeliness. It used to be the fastest 90%. Based on the PMIG, we have moved to overall average. So, again, something to consider as you're looking through the timeliness, and if you see any changes over the last year or so, that's a requirement that was in the national level policy. So, what I'll do is, I know we're kind of running short on time, and there's a few other presentations. So, I'm going to focus more on the Q3, so the current timeliness, as opposed to historical timeliness for… we'll go with the initial top secret, and then the initial secret, so T5 and T3. So, for the T5 initial investigations, FY 26 Q3, you can see the initiation timeline is 20 days, the investigation timeline is 97 days, and then the adjudication is 126 days for 243 days total. And then for our Tier 3, or secret, we have 21 days for the initiation, 59 days for the investigation, and 117 days for the adjudication,

for a total of 197 days. So that is all the information that I was going to share. I can try to answer any questions if there are some.

Michael T.: Questions?

LaToya: I have a question. The CV resolution cases, would you happen to have metrics on, how many cases you've received? I think DOE did an amazing job capturing all of their alerts that they've received, and what category they kind of fell into, and how quickly they are resolving them. Would you happen to have metrics on that?

Thomas: We are trying to obtain, more information, more data, on CV, just in general, but… but yes, we're looking to that, and I will say that, as far as Industry, TW 1.5 CV service enrollments, I believe Industry is 25% of our enrollment population, which… and again, we're still working on finalizing and confirming this information, but it's approximately 984,000 enrollments into CV, but I think what you're specifically asking is a breakdown of the alerts, potentially what area or information category of trigger may have been identified by that alert, and then what additional investigative action is required. Is that correct?

LaToya: Well, yes, and in addition to that, how long is it taking you to resolve those? Which, and that question is being driven by the concerns from Industry in regards to how long it's taking for those issues to be resolved, which is impacting us being able to get people onto mission.

Thomas: Got it, yes, I got you. We will try and get some data on that and I will say, so, we are shifting how we vet individuals from that static 5 year periodic reinvestigation to a continuous flow of information and this isn't new to anybody, I'm sure we're all familiar with this, but I say that because these individuals who are being enrolled into a CV service, I mean, just the Industry population alone, is close to a million. These are individuals who've been in service, who are trusted insiders, who are trusted individuals, who may not have interacted with the Government for a personal vetting purpose for quite some time. Not only that, but these individuals may no longer be affiliated with whatever Government service that would have required them to have that position of trust. So, I say that because that's one of the challenges that we're facing is trying to contact these individuals because we have a CV alert for an individual who may no longer be in a position of trust, or may not have been contacted or had to, I know within the policy, they're required to update their SF86 or SF85P prior to enrollment into the CV service, but that doesn't happen all the time. So, those are the challenges, but either way, we are trying to get some more data on the CV service that we offer to include the alert management issue resolution process.

LaToya: Thank you for that, and the challenges are definitely understood however, I would like to emphasize that in some scenarios, these individuals are people that have continued access, and when they are attempting to, to transition to new positions, new roles, under new programs or new MILDEPs, whatever, wherever they're going, SAPs in particular, if there's an open case, then all bets are off. The processing stops, and they are no longer considered for that role and the concern is that when that is addressed with DCSA, there's really no SLA or no timeframe that's given on when the issue can be resolved so, we're seeing quite a delay in being able to get people on because of those very reasons so that's why the question about metrics and understanding how quickly are you guys resolving these concerns, and again, I do understand the impact with being able to get in contact with people and things like that. I

would encourage you, because what we are seeing, too, is that some of those contacts are being sent directly to the individual and I'm not sure when that shifted or when that changed, you know, taking the FSO out of that equation and kind of putting them on the back end versus on the front end, but I would encourage DCSA to consider going back to what was working and put the FSO or the security officer at the beginning of that process with notification that you are trying to reach said employee instead of on the back end when it's impacting being able to get the person onto mission.

Thomas: Yeah, that's excellent feedback. And I will say, we do have a process for notification when there is a CV alert, but understood. I took notes of what you just recommended, but yeah, I appreciate that feedback. Thank you.

Jennie: And two small footnotes to that. When the work is being done, to first verify in the system of record whether an active affiliation exists, that is a part of this, and reaching out to the right people and ensuring that the work can be done to adjudicate it, but also, I'm curious if we're able to drill down into the metrics to understand the types of reports that are being worked, but to also understand the subset of issues that are coming from the Rap Back enrollments that occurred earlier on this year.

Thomas: I just took a note of that as well, thank you. So yeah, definitely some enhancements I'd say that we're working on on getting those data points and metrics for CV. That is something that I can take back and look into.

Michael T.: All right, and you're not off the hook yet, we have at least one question for you from the chat. So, let me ask you this on their behalf. Do you have any data on how many initial PCL submissions are rejected?

Thomas: I'm sorry, is that… is that a question for me?

Michael T.: You're the… you're the…

Thomas: I didn't hear the first part of that.

Michael T.: Let me, let me give it to you again. Yes, you're the man in the hot seat. This is a question from our online audience. Do you have any data on how many initial PCL submissions are rejected?

Thomas: Any more information who provided that Greg, I believe? Any more information on what it is that you're looking for as far as those PCL submissions that would be helpful, so that we can track down what data points we may need. It may be included, depending on the scope of that, it may already be included in those data points that we're looking for anyway, as CV as a whole, but anything else you can provide as far as specifically what you're looking for, as far as the data on those PCL submissions would be helpful.

LaToya: So, if I could provide some clarity, what he's asking, what the online person is asking is, do you have metrics on the rejections of those PCL cases? Like, how many are rejected?

Thomas: I, I think we do, and I need to maybe level set what population of cases that represents before I can say for sure, but yeah, we do have, as far as cases that may be rejected back to the department or agency or Industry partner. They may be rejected back for a number of reasons, but there should be some data on that, but again, so any supporting information you have, I

mean, it's…there's a lot of data. We just need to know what it is that we're looking for specifically before I can start requesting that data.

LaToya: Thank you. You have something, Annie?

Andrianna: This is Annie Backus, Department of the Air Force. This is something I think we should take back. Certainly an interest on the Government side as well for investigation requests, whether it's T3 or T5, for both Government and Industry, what is DCSA's rejection rate?

Michael T.: Great, thank you all very much. Any further questions?

Heather: Thank you, Tom. Now we will hear from Peregrine Russell-Hunter, the Director of the Defense Office of Hearings and Appeals. Perry, please come on up.

Peregrine: Alright, so I want to start out by thanking Michael and Heather for another great public meeting. Very very well run, thank you. I also want to say, for our departing members, and I see that… well, Ike, first of all, I want to say thank you for being such a great voice of Industry. You've been wonderfully vocal in all the right times from where I'm sitting. Jane and I, I have to confess, I have the honor of having worked with Jane in one capacity in her many important jobs over more than 30 years. First met Jane as a result of a DOHA hearing, because I was calling her as a witness, and she did a phenomenal job and it was also… I recall the witness prep session was in an Olive Garden. It was good. But she did a marvelous job, in that, and everything before and since, she's one of the real stars in that organization. and I just want to say thank you so much for your professionalism and partnership and vigilance and all the things you've been doing.

Jane: Thank you.

Peregrine: And then…finally, Jeff, if you're still in the room, and if you're not, then I completely understand why. I noticed that Jeff emphasized candor and transparency and, as being part of the gestalt of the NISPPAC and I want to say that, in that spirit, I'm going to do a thing I've been doing in multiple successive NISPPACs, which is to give you my phone number, which is 703-696-4751. That number rings on my desk, nobody answers it but me. The reason I do this, and I know you must all think I'm crazy for doing this, is that I get questions from working FSOs who identify real problems and the numbers I'm about to give you, by the way, for DOHA are infinitesimally small compared to the numbers that all of the previous speakers have given you, and that's because these are only the cases in the administrative process for denial or revocation, and so this is well within the 2% that require that action but at the last public NISPPAC meeting, and thanks to an innovation by Michael and Heather, these meetings are now posted on YouTube, and I had the honor of getting a phone call from a working FSO who said that he had not been present for the NISPPAC meeting, but that he had seen the NISPPAC meeting on YouTube and, so it's working and he called my number, as I had hoped, and I learned through that call about what was for him a mystery, and of course then it became a mystery for me to solve, about why it was that somebody was saying that a case had been at DOHA for 2 years that we had, in fact, never received and it turned out we were able to identify a process glitch between us and DCSA on reapplications, which in the following month, we were able to have our first-ever DOHA help desk at NCMS, which was in part due to the fact that we'd initially heard that DCSA wasn't going to have a help desk, and then they ultimately did at the last moment, but we were able to have a help desk right

alongside DCSAs, which was super helpful, because we were solving problems together, which is really the way Government is supposed to work and so I want to say, first of all, thank you to DCSA for being such great partners, because we really do solve a lot of things on the individual case level by working together. That said, DOHA exists to provide a fair, consistent, and transparent hearing and appeal process that is independent of DCSA's investigative and adjudicative process. In fact, the Department of War's General Counsel and now the Justice Department's Office of Legal Counsel have specifically opined that the investigating entity cannot also hold hearings so that solves something that had been… I didn't really think it was an open question, but it's now been resolved. I think it's also important to know that we are able, as we begin the Industry denial revocation process, DCSA and DOHA work hand-in-glove on the issuance of the Statement of Reasons, which is the first notice to an Industry employee that there is an issue and so, our independent role in the collateral Industry contractor process begins with the legal review of that statement of reasons and at this point in this fiscal year, which is almost over, DOHA will have conducted over 1,200 legal reviews of Statement of Reasons. See, I told you those numbers were going to be super small compared to everything else you've seen but we have received almost double the draft statements of reasons in the last 5 months than we received in the first 6 months of fiscal year 2026 and we're still keeping timely, by the way, because the number had been low, and it's now increasing, which is, by the way, proof of something that both Tom and Allyson talked about, which is the mitigation strategy for the investigative inventory, and bringing that inventory down. Typically, we at DOHA, when DCSA brings their investigative inventory down, it means that they're working the harder cases, and of course, it's the harder cases that are coming to us so I can stand here and attest to the fact that what Tom and Allyson have told you is true, and that workload really is coming down, because we're seeing the cases that we should see when that happens. By the way, one of the reasons that we are still able to keep timely in our legal reviews of those statements of reasons is that we at Doha work seamlessly with DCSA in a paperless transfer and review process, so it's not like there's a box of statements of reasons, you know, coming down the BW Parkway from Fort Meade to DOHA as actually was once the case. Bless you. But it's now, it's now a… by the way, there's an old European tradition that when you sneeze when someone's telling the truth, so thank you. I wanted to stress that that ability for us to work so seamlessly with DCSA on the legal reviews and be completely paperless. I owe a debt of gratitude to now a former DCSA employee, Heather Green, who made sure that we got that done. So, I want to say just a shout out. Heather, if you're listening, thank you for that. So, the other thing that I can report is that DOHA administrative judges have just 390 cases on hand to decide, and have completed over 1,200 in fiscal year 2026, and that's, again, a lower than average workload, so we are able to keep timely that way as well and in fact, as you probably know, most now more than 90% of our hearing cases are conducted virtually over Teams, and so we are able to get to your case faster, get your case heard faster, and decided faster as a result of that. So, I wanted to close by saying, again, how much I appreciate the opportunity to speak with the NISPPAC and to be accountable to you all for what it is we're doing at the tail end of the process. Again, the numbers are small, but that doesn't matter when you're one of those numbers…when you're the person who receives a statement of reasons, and you're notified that the Government has a concern, that process has to be done with integrity and fidelity and consistency, be transparent, and also independent of the investigation. I'm proud to say that we are doing all of those things. So, with that, I'll take questions. Thank you.

Michael T.: Alright, questions for Perry?

Jennie: Hi Perry.

Peregrine: Oh, Hi.

Jennie: Can you explain, for Industry's benefit, what DOHA's part is, if any, in the revision of SEAD 4?

Peregrine: I wish I could tell you. I will say that, I have been consistently involved, on behalf of DOHA and the Office of General Counsel and the Department generally, in the updating of the adjudicative guidelines for now almost 30 years, certainly, certainly 25. This is the first time in the history of my time doing this, and given, you know, who we are at DOHA, we see a lot of cases, and just as I was able to say, yep, we can attest that the investigative workload is coming down, because we're seeing the cases, we should see when that happens. I can also say that we have been able to contribute to SEAD 4 revisions because of what we see and you all in Industry, of course can and should as well, because of what you see, because of, in your workforces, you're seeing trends. It was interesting, though, one of the slides about the continuous vetting hits, was quite informative, because you see the enormous number, for example, that are financial, that are credit reports and public records is up there, but then criminal, it turns out, is super low. Those are all things we learn because we have these meetings, we have these discussions and, and I can tell you that recent revisions to SEAD 4, that became effective in, you know, now 9 years ago, were, in large part, informed by our shared experiences in adjudicating and hearing cases, applying the guidelines and of course, the DOHA Appeal Board is the one place in all of Government where you can see published decisions that where we show our work that show how the adjudicative guidelines are applied to real cases, and of course, we anonymize them, so nobody… you can't tell who it is, but you can tell what was done, and so there are now about 38,000 cases on the DOHA website, dating back to November 1st of 1996, which is when we first started doing that to comply with the electronic FOIA amendments, by the way, and so we have able to track the trends, and we definitely, have some comments to offer, should that become possible, so, not yet, but still hopeful.

Michael T.: So, Perry, going to the chat, our colleague Lisa Perez from ODNI had a question for you. She says going back to the legal opinion that you referenced, where and why did the question originate, and what led to the endeavor that resulted in the opinion?

Peregrine: Okay, so…there is a provision in Executive Order 12968, which makes it clear that the investigating entity cannot also hold the opportunity to appear personally, or what I've been in shorthand calling a hearing. The reason for that, and I'm going to paraphrase Honorable Matthews, our General Counsel, who said, you know, the investigator shouldn't be judge, jury, and executioner. There needs to be some administrative separation. And so that's been well understood for fully 30 years now. What was less well understood was how thinly that interpretive salami was going to get sliced and so, the question was raised within the department. The General Counsel answered it, and as the Chief Legal Officer of the Department, the Honorable Earl Matthews gets to answer that question. Additional questions were asked, and therefore, the Office of Legal Counsel at the Department of Justice was consulted. And yes, I am using the passive voice.

Michael T.: Noted. I'm still clinging to, well,your salami reference in terms of it being sliced thin.

Peregrine: But I think, sort of, lurking within your question is, the question of scope, and the OLC opinion is, and by the way, we published that on our website, you know, because the General Counsel ordered us to. You will see that it only applies to the Department of War, it does not apply more broadly. So it is… because what happens… by the way, the Office of Legal Counsel is a wonderful thing. You get to ask them questions, and they will answer, and then your agency gets to apply them and so, in this case, because it was the Department of War that asked the Department of War, it got the answer, and the answer only applies to the Department of War.

Michael T.: Thank you very much. Any further questions for Perry? Alright. Thank you, Thank you very much. Gang? You did it. We're now at the time of the meeting where if there's any additional new business that anyone would like to bring forward, floor's up.

Christopher: I got something. If you didn't indulge me for a moment. So, I'm about to do something I don't like to do, especially in public, and say something nice about Ike. So, as our spokesperson, he got to stand up there, say nice things about Jane, nice things about Jeff, so I thought it was appropriate that we make up some nice things to say about you. So if you don't know, as spokesperson one of his many jobs is to reach out to people that have been nominated and gone through the election process to be on the NISPPAC and so, a couple years ago, he gives me a call, and I answer it, say, hello, no, hello, no, how you doing? His question immediately, are you ready to go to work? Are you ready to go to work? I'm like, you're not even gonna say hello? That's all he wanted to know, because that's all he cared about. And man, he wasn't kidding. There's an expectation if you're on the NISPPAC, that you're out there, you are working hard just for Industry, our customers, and most importantly, the warfighter and he absolutely leads by example from that. Whether it's meetings, calls, everything. He's there all the time, which can get annoying sometimes, too, but there's no doubting his dedication. There's a lot of things to like about him, some things that'll drive you crazy, but there's a lot of things to like. The thing that I appreciated most, and I think many in the group do, is his willingness to listen. Even if he doesn't agree, he wants to better understand and it made us better, it made our group better, made our relationship better, and we appreciate you. It made you successful, made us successful, and thanks for letting us be part of your family.

LaToya: Don't give Ike the mic.

Isaiah: Well. Oh. I'm not afraid, you know, they say men, you know, we shouldn't cry. Listen, man, I'm an emotional individual. My mother was an emotional individual. I'm compassionate about this, you all got compassion, but I'm really compassionate and emotional because the feeling that I get from Chris and the rest are genuine. I know fake, right? I know fake. I'm a New Yorker, I'm a hustler, right? So I know when I see something that's fake. And the genuineness between everybody in here and in Industry has been real, and I appreciate that but before I go, I'm gonna leave you with something, that, the group probably didn't know I was gonna say, and I didn't know I was gonna say, but I'm gonna say it anyway. A couple of years ago, Industry NISPPAC, we sat around a table, and we talked about how we can give back to the community and when we say give back to the community, we're talking about the DIB, the Defense Industrial Base, those security professionals out there that do the

work day in and day out, right? Most of us are seniors, right? We get to have the oversight, but those individuals, what are we giving back to them, right? What is Industry NISPPAC giving back to the community and so, over the summer, well, early on this summer, we got together, the group got together, and we said, hey, let's create a NISPPAC Industry Award for Security and Excellence for Industrial Security Professionals. So I'm here to announce today that in 2027, we will be passing out that award to some lucky representative. Industry NISPPAC talked it over with ISOO, Mike and Heather, and they loved the idea, and so we have a NISPPAC award working group. I chaired the working group, but the working group is for all former NISPPAC members, and some of them are here now. Greg Sadler's on the working group. Tracy Durkin is on the working group. Derek Jones is on the working group. Quinton Wilkes is on the working group. Heather Sims is on the working group. Michelle Lambiasi is on the working group. Rosie Borrero Jones is on the working group. Cheryl Stone is on the working group and old school Tom Langer is on the working group, right and so these are all former NISPPAC members that are on this particular working group, and we're so honored that we can give something back, right and so when you talk about legacies and what you leave on the table, right, we just want Industry to know that we understand their pain, we understand their victories and we just want to do something to give back. I want to give a big shout out to Ms. Trish. She's the president of the NCMS, and she's our Industry NISPPAC MOU and she's gonna allow the NCMS a venue for us to actually, pass out that particular award, but this is not a DCSA centric Award. This is for the entire DIB, right? And so we're gonna be reaching out to…the chair of NDIA, the chair of ISWG, for those individuals that maybe not go to NCMS, but maybe just go to NDIA and we're gonna find them and take that award to them. So there's gonna be more information coming about that, but this group, this body right here cares about Industry and about the Government, but we love the Industry, and we want to give back so I want to thank the group for taking the vision that we had a few years ago, and then just putting it out there on the surface now. So thank you, everybody. I appreciate y'all.

Michael T.: Does anybody else have anything nice to say about Ike?

Audience: No.

Michael T.: I didn’t think so. Well, in closing, I have two things to share. One is that our next meeting will be right back here on March 17th. Got a lot of work to do between now and then, a lot of questions to answer and I'd be remiss if we didn't close in thanking one more time Jane and Ike not just for their service to NISPPAC, but for their service to this country. Both of them had long and distinguished careers in different aspects of public service and we are very very grateful for that, as well as for the work that you've done.

Isaiah: Mike, by the way, I missed Jane. Jane is also on that working group, because we're both, as of 1 October, we'll be both former NISPPAC Industry members.

Jane: I tried to get out and they keep pulling me back in.

Michael T.: Thank you, everyone, and thank you to the ISOO staff who facilitated this meeting today. So many of them were here amongst you, doing different jobs that are outside of the regular portfolio. Most of all, thanks to Heather Pagán for bringing us all together.