Transcript for the NISPPAC Public Meeting on March 18,2026

Michael Thomas: Morning, everybody. Welcome. In a place like this, it always feels like church. We have, I think, several dozen folks joining us here in the building, as well as many online, with many hundreds registered for the meeting, so I'm very excited to see what sort of feedback we get. Let me just start by saying I'm absolutely delighted to host you all here today in the National Archives stately McGowan Theater for a 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 here at NARA, and the Chair of the NISPPAC. Welcome both to those joining us in person, as well as those joining us online.

2026 marks the 33rd anniversary of the National Industrial Security Program Executive Order, which wedded all of us together. ISOO, Department of War, DCSA, our CSAs, our CSOs, executive branch agencies, and our many friends beyond the government. If you were looking for something to celebrate this union of purpose, you actually have a couple of choices. A 33rd anniversary is technically iron, celebrating a strong and enduring relationship, but more modern interpretations also allow for a 33 to be marked by a gemstone, an amethyst, which symbolizes peace and balance. Now, please note, this information does not constitute the solicitation of a gift, but if you're considering something to mark the occasion, please ensure that the cash value does not exceed the $20 federal limit.

But somewhere in the middle of these, amethyst and iron, strength and peace...balance. I think we strike the right tone for everything that this pack is meant to help us manage. This 33rd anniversary is not just a milestone, it's a vow renewal. And 33 years is a long time, but the roots of the work that we do with the NISP go back much deeper.

Speaking of roots, let's start with ISOO. The Information Security Oversight Office, which is part of the National Archives, was established in the 1970s to oversee America's classified national security information program. We follow in the footsteps of an earlier interagency commission that had been established under President Richard Nixon. ISOO is the referee for how the American government manages its sensitive information. We're the ones who help explain and enforce the rules: what needs to be protected, why, how, and for how long. The NISP brings to ISOO, and to all of us, a duty to pursue efficiency in the process of security, to ensure standardization and reciprocity, so that the ways we keep our people and our information and our most critical national security capabilities secure don't inadvertently impede our ability to field ever more capable tools and technologies for our national defense.

These challenges confront us every day, but they're not new. In my first NISPPAC public meeting, I talked a bit about how deep those roots actually go, all the way back to the American Revolution and George Washington's endless quest for enough guns and black powder to equip his army against the British.

But given the anniversary that's just been visited upon us a little over a month ago, perhaps today it makes sense to look back on the lessons of the Cold War that informed the drafting of the NISP executive order itself.

It's September 1959. There was hope in the air. President Eisenhower and Soviet leader Nikita Khrushchev had met at Camp David. And many felt this meeting might portend a peaceful resolution to the Cold War. But this was not to be. Often in the haze of history, these sorts of opportunities, these paths untaken, are lost without a clear or direct cause. In this case, though, we know exactly why things went down, actually, quite literally, in flames. See, about months earlier, Ike, Eisenhower.

Ike Rivers: That's okay, I'm good with you.

Michael: President Eisenhower had struck a deal to establish a secret base in Pakistan that included the use of the Peshawar Airport to launch flights for the newly developed Lockheed U-2 spy plane. This plane was, in and of itself, a product of extraordinary collaboration in government and Industry that produced remarkable new capabilities for our national defense. That's a story for another day.

On May 1st, 1960, just 15 days before the next meeting between Eisenhower and Khrushchev, the Four Powers Summit Conference in Paris, American pilot Francis Gary Powers took off from Pakistan to perform aerial reconnaissance over the Soviet Union. And you may recall that Powers was taken out mid-mission by a surface-to-air missile deep inside Soviet territory. He was immediately captured and tried and imprisoned, kicking off an international furor, and a potential path to peace was forestalled. Now, some of this history you're no doubt familiar with, but what you may not know is that there's a key piece of technology that made that Soviet strike on the U-2 possible. Their missile was equipped with a proximity fuse, which allowed it to detonate in mid-air, without a direct impact. That's how the Soviets got him. How did they get that tech? The answer is, they got it from us...through industrial espionage. The proximity fuse was stolen directly from American Industry, from Emerson Radio, in fact, better known for making Christmas lights and radios. But they had the contract to manufacture this key piece of national security technology. And the theft? Well, it actually happened a decade earlier. Perpetrated by none other than Julius and Ethel Rosenberg, best known for later stealing our nuclear secrets, and for their subsequent execution for those crimes under the Espionage Act. The proximity fuse technology made missiles 3 to 4 times more effective. During World War II, it was so secret that it was seldom even used over land for fear the Germans might recover a dud and reverse engineer it. Julius Rosenberg had been working as a defense contractor, an inspector, if you can believe it, for the U.S. Signal Corps when he pilfered the proximity fused plants. He reportedly passed them on to his Soviet handler as a Christmas present. And it proved to be the gift that kept on giving 15 years later, when that technology brought down Gary's upending international diplomacy, embarrassing Eisenhower to the point that he contemplated resignation, and, without a doubt, resulting in exceptionally grave damage to national security, as would have been

defined by President Eisenhower's November 1963 executive order on safeguarding official information in the interests of the defense of the United States. That's EO 10501. Keeping score.

The cohort of national security experts that came of age in the mid-century, including President H. W. Bush, who originated the NISP executive order. They experienced both the criticality of American Industry during World War II, as well as the thorough infiltration of government and Industry and academia by Soviet spies. The Rosenbergs are just the tip of a very large iceberg. The NISP was established in the faith that our government and the private sector could trust one another with our nation's most sensitive secrets. And the NISPPAC exists to provide the conduit for continued dialogue in this crucial conversation. Because the mechanisms for guaranteeing trust are dynamic. They have to be renewed and revitalized as the mission and threats we face of all.

This is why the work of the NISPPAC is so critical right now. We're not just updating a security manual, we're facilitating the safe passage of information between public and private sectors. We're securing America's engine of innovation. We're securing our way of life. And 33 years in, the priorities of the NISP still feel vital and necessary. Greater uniformity and reciprocity in security procedures. The elimination of duplicative or unnecessary requirements, ultimately reducing the cost of security while maintaining its rigor. These issues continue to impact virtually every executive branch agency. And at a time of dramatic government restructuring, the continuing importance of the NISP mission was acknowledged by the renewal of the NISPPAC via executive order late last year, ensuring that this principle forum for resolving the friction between government and Industry is as essential as ever.

ISOO is directly responsible, not just to all of you, but to the President, for maintaining and revitalizing the overall policy framework for the NISP, ensuring its continued effectiveness and efficiency. Over the last year, we've taken time to convene, solicit, capture, and refine the next wave of renewal for the NISP, a process that will continue as our NISPPAC members, wider Industry stakeholders, and eventually our NISPPAC working groups take on some of our thorniest security challenges. The hope is to address some of these age-old problems in some decidedly new ways. You'll hear more about that over the course of the day.

Relatedly, ISOO has also, as of this year, renewed meetings of our Federal Controlled Unclassified Information Council, which brings together a massive interagency coalition to work implementation issues, as well as to explore the intersection of this critical information management policy with the directive to apply artificial intelligence and automation to the daily work of government. We look forward to the insights that emerge from these efforts, and to presenting the consolidated recommendations for NISP policy reform, as is our formal responsibility under Executive Order 12829.

I thank you all for your participation today, and for your support of the NISPPAC as the convening point for these discussions. Thank you. Let’s begin. Heather?

Heather Harris Pagán: Thank you, Michael. Good morning everyone. I'm Heather Harris Pagán, the Designated Federal Officer for the NISPPAC. I want to thank the folks we have volunteering today to help this meeting run smoothly, so, thank you.

Information related to the NISPPAC and its public meeting is available on the ISOO website and the Federal Register. For those speaking in person, please come up to the podium for your briefings, except for the Industry briefing, where only the Spokesperson will come to the podium. You will also be responsible for advancing your slides. For those briefing on the phone, please say next slide so we know to advance them. For NISPPAC members at the table, the microphones cannot be muted or unmuted, so please do not have sidebar conversations. If you are listening in through Zoom for Gov, you may need to reset your audio settings to hear and speak. If you have connected through telephone or YouTube, please provide your name to nisppac@nara. gov for file retention as having attended the meeting. If you require technical assistance, please send an email to nisppac@nara. gov. Please note all audio connections via telephone and computer should be muted when not speaking.

For questions, and you are calling in on the telephone, please hit *9 to raise your hand, and *6 to mute and unmute yourself to ask a question. If you are on the computer, you can raise your hand, ask questions through the chat or email your questions and comments to nisppac@nara. gov and someone from our team will take care of you from there. If you are in the theater, please utilize the microphone from our esteemed colleagues Ana and Uma have. Thanks ladies.

We are planning on a 30 minute break at the halfway mark of the meeting due to the meeting length. We are having a longer meeting than we used to because we want to make sure that all the questions asked during the meeting, regardless of who is asking, are addressed during the meeting, so that would include members of the public as well. This is something we have not done in a while, and we are hopefully this will be value added to the meeting.

We have restrooms located outside the theater, along with a cafe for a snack during the break, or a meal after the meeting concludes, but please note that other than water, there are no food or drinks allowed in the theater.

In the event of an emergency, please follow members of the public outside. All available meeting materials, including today's agenda and slides, have been posted to the ISOO website and have also been emailed to all registrants. Not all speakers have slides. This is a public meeting. As with previous NISPPAC public meetings, this meeting will be recorded. This recording, along with the minutes, will be available within 90 days on the NISPPAC Reports on Committee Activities webpage.

I want to remind the government members of the committee of the requirement to file a financial disclosure report with the National Archives and Records Administration's Office of General Counsel. This must be completed prior to officially serving on the NISPPAC, and then updated and submitted on an annual basis. The same form for financial

disclosure that is used throughout the federal government, OGE Form 450, satisfies the reporting requirement.

Let's begin attendance. For the government agencies, after I say the name of your agency, please state your name. Once I have gone through the government agencies, I will then move over to Industry, and then to our individual speakers. As an aside, we will not be hearing from the Nuclear Regulatory Commission or Department of Homeland Security today. Their slides for vetting are at the end of the slideshow that was emailed to everyone.

Department of War?

Jeffrey Spinnanger: Here

Heather: Thank you Jeff. Office of the Director of National Intelligence?

Lisa Perez: Lisa Perez. Present.

Heather: Thank you Lisa. Department of Homeland Security? Department of Energy?

Theodore Banks: Ted Banks.

Heather: Thank you. Nuclear Regulatory Commission? Defense Counterintelligence and Security Agency?

Allyson Renzella: Allyson Renzella.

Heather: Thank you. Central Intelligence Agency? Department of Commerce?

Daniel Boling: Dan Boling.

Heather: Thank you Dan. Department of Justice?

Tonya Fields: Tonya Fields.

Heather: Thank you. National Aeronautics & Space Administration?

Vaughn Simon: Vaughn Simon.

Heather: Thank you. National Security Agency?

Eric Szakal: Eric Szakal.

Heather: Thank you. I appreciate it Eric. Department of the Air Force?

Andrianna Backhus: Annie Backhus.

Heather: Thank you. Department of the Army?

Laura Aghdam: Laura Aghdam.

Heather: Thank you. Department of the Navy?

Robin Nickel: Robin Nickel. Present.

Heather: Thank you. Department of State?

Kim Colón: Kim Colón.

Heather: Thank you. Now I'll move on to the Industry members:

Isaiah Rivers?

Isaiah: Present.

Heather: Thank you Ike. Jane Dinkel?

Jane Dinkel: Present.

Heather: Kathy Andrews? Chris Stolkey?

Christopher Stolkey: Present.

Heather: LaToya Coleman?

LaToya Coleman: Present.

Heather: Charlie Sowell?

Charles Sowell: Present.

Heather: Leonard Moss?

Leonard Moss: Present.

Heather: Jennie Hardy?

Jennie Hardy: Present.

Heather: Thank you. I'll take the roll call for speakers now:

William Vaughn?

William Vaughn: Present.

Heather: Thank you. Donna McLeod?

Donna McLeod: Present.

Heather: Thank you. And 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. As a reminder, 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. Ms. Breanna Palmer has replaced Richard Dejausserand as the alternate for DHS. Allyson Renzella is now the primary at DCSA, with Matthew Roche being her alternate for a short time, before Booker Bland replaced him. At the CIA, Nathan and Roger replaced Jennifer Alworth and Keleigh. At the Department of Justice, Glenn Bensley and Lori Ellison have replaced Tonya Fields as the primary and alternate, respectively. At the NSA, Eric Szakal is the new primary member. For the Air Force, John Voorhees has replaced Winston Beauchamp as the primary. For those 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 May 28, 2025. The minutes from that meeting were certified to be true and correct, and were finalized by Michael Thomas on August 13, 2025 and posted to the ISOO website on August 18, 2025.

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 requested a meeting to discuss reciprocity of training with CSAs and CSOs. This action item 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 considered to still be 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 as soon as possible on all EOs with suspected NISP implications. This item has evolved, and is currently with NISPPAC Industry. This item is considered open at this time, while ISOO continues reform efforts.

Industry requested a meeting with CSAs to discuss communication options so they are not surprised by future announcements. It is expected that this will be addressed today by ODNI. NRC is not represented during the meeting today, but will be considered open only for them, as everyone else responded.

Industry requested that ISOO convene a meeting of the CSAs to discuss CUI. This item is considered closed at this time, but will reengage at a later date.

Industry requested that Government inform Industry of any budgetary or personnel changes that will impact Authorizations to Operate. This action item is considered closed, as DCSA responded.

Industry asked DCSA to provide a status update on the facility clearance orientation handbook. This action item is considered closed, as DCSA responded.

Industry requested OUSWI&S establish a vehicle for Industry to provide NBIS requirements and feedback, and would like an initial meeting on this topic within 30 days. This item is considered closed as that has taken place.

Industry requested to be a part of the policy making process regarding the covered insider threat policy with ODNI. This item is considered closed, as that took place.

Industry requested guidance from the services on expected timelines for SCIF and SAPF compliance. This item is considered closed due to not being a requested item further.

Industry asked for a meeting with the CSO of DHS. This item is considered closed due to not being a requested item anymore.

In addition to those action items, we also have questions that were not answered during the last public meeting.

Russell Justice asked: In regards to the CUI and CMMC discussions in today's NISPPAC meeting, which was in May 2025, I am seeking clarification on CMMC and in scope cloud service providers. For example, many companies in Industry utilize SaaS solutions for security management. These include solutions like SIMs, Tru-Vetting, Security Control, Sign-In Solutions, etc. These programs allow for upload of DD-254s, which are becoming more and more often CUI. Looking through the myriad of guidance on CMMC, it appears that FEDRAMP Moderate Equivalent is still acceptable and is on the contractor utilizing the service to assess required documents and ultimately take on the risk. Additionally, if they do not deal directly with the government, are they able to receive FEDRAMP Moderate certification? Who would be their sponsor? Most are applications that sit within an approved CSP such as AWS GovCloud. If I am not making sense, it only goes to show that the guidance for CMMC, 800-171, etc. are confusing, often contradictory, and not adequately distributed to Industry Partners. Beyond the security software solutions, you have the ERP solutions like Unanet...how far down the private Industry chain does FEDRAMP or FEDRAMP equivalent reach? How can we continue to modernize and manage our contracts? Because this question is related to CMMC, it is recommended that Russell reach out to their government contract representative for clarity, so if any others have that question, please direct them there.

For the second question, Nik A asked a 32 CFR Part 117 question for the NISPOM: E-Verify offers an accepted electronic method to validate citizenship. Can DoW/DCSA speak on any consideration to update the 32 CFR part 117. 10C NISPOM rule to validate original or certified copies

of proof of citizenship to include language that supports a similar (if not the same) electronic method? This is open at this time awaiting a response from OUSWI&S or DCSA.

The third question came to us from Jennie Hardy, one of our newest NISPPAC Industry members: Can we address the plan to address Industry's concerns with the hesitance of IC adopting initiatives to modernize systems and eventually adopt the PVQ aligning with the updated investigative standards. In speaking with individual agency PERSEC leads, there seems to be no foreseeable intent to modernize. This will continue to be problematic, despite those agencies being under the same Trusted Workforce mandate. This question is still open pending a response from ODNI, but is expected to be closed during this meeting.

Our next question came from Marlene Tores, who asked if we know how many companies are compliant with CMMC? This is not something that is tracked, as Level 1 is a self attestation by a company. Level 2 and 3 are not yet required.

She also asked for an explanation of what FCI is in regards to CMMC, but we were unable to answer due to a lack of clarity.

Are there any questions or comments on the action items and questions that are still pending from the last meeting? Great.

Now, we are going to move 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: Good Morning.

Everyone: Good morning.

Isaiah: Do you know it is a great day to have a great day? Let that sink in. It's a great day to have a great day. I heard that in a little speech that my mother wrote. May she Rest in Peace. And it didn't make sense until a couple days ago. So I just wanted to introduce that to you guys today.

Mike, Mr. Thomas, thank you very much for inviting us and keeping this thing moving. On behalf of Industry NISPPAC and the MOUs, we appreciate the opportunity to participate in this very, very important dialogue.

The National Industrial Security Policy Program has always depended on one fundamental principle. And that's partnership. The protection of our nation's most sensitive information and capabilities is not the responsibility of the government alone, nor Industry alone. It is a shared mission. The strength of the NISP lies in the collaboration between government agencies and cleared Industry base, working side-by-side to safeguard the technologies, the intelligence, and the operational advantages that support our great national defense.

Today's security environment continues to evolve rapidly. The adversaries are present. The technology's capable and determined to

exploit vulnerabilities whether they exist or not. In this environment, it's extremely important...partnership and collaborations are not simply beneficial. They are essential. Open dialogue between government and Industry allows us to anticipate the risk, shared insight, develop solutions, and strengthen the entire security ecosystem.

Equally important is the accountability. And you all hear me say that word a lot, the accountability. Partnership requires trust, and trust requires that we hold ourselves and each other to the highest standards. Industry: we must continue to demonstrate vigilance in protecting classified information and control technologies, while the government must provide clear guidance, transparency, and consistent engagement. When we hold each other accountable, we reinforce the integrity of the program and ensure that security is not just a requirement, but a shared commitment. Ultimately, the work we do through the NISP has a very real purpose. It supports the men and women who serve our great nation. Every policy we discuss, every safeguard we implement, and every partnership we strengthen contributes directly to protecting that warfighter and preserving our national security advantage. So, with that being said, Michael, Mr. Thomas, and Heather, you know, we want to thank you very much for this participation, and we do look forward to discussion ahead, and to continue the collaboration that makes this partnership so vital to the mission.

So, before I go on to the working groups and let them talk about some of the things they want to talk about, I do want to say I am so honored to sit here and say that that partnership and the collaboration between the government and Industry is alive, right? Is alive and very alive. Here's a great instance, and this is a huge win for everybody, specifically for Industry. The 2025 NDAA Section 874 established a pilot program to expand access to shared commercial infrastructures, often referred to as the classified infrastructure as a service environment. The pilot was directed by back then it was the DoD, now the DoW, to streamline access to small businesses, non-traditional defense contractors, and universities to secure facilities capable of supporting secrets and top-secret work without requiring each company to build or maintain its own classified facility. In a nutshell, now a small mom-and-pop shop does not have to get a facility clearance that is cleared at the top secret level. They can just become a NAESOC company and utilize other service provider's classified system, which decreases risk so tremendously. So, one of my first questions that I'm going to pose to DoW, and when they come up, they can kind of maybe talk about it, is the program status. Can OUSWI&S provide an update on the current implementation status of the classified infrastructure as a service pilot authorized under the FY 2025 NDAA. Specifically, which agency or organizations have begun participating in, and what milestones have been achieved to date. I do want to thank Mr. Jeff Spinnanger and DCSA, David Scott, and other leadership that was at a tremendous meeting a few months ago to really discuss this and got Industry's input. This is the first of its kind, and Industry wants just to thank the team very much for supporting this effort, as it is a tremendous win for Industry.

Also, one of the great things I think is gonna be really, really good for us coming forward is what I call it NISP 2. 0, alright? The NISP has

been around for a long time, and if you read it, it is a little bit probably outdated, and it needs to be reconstructed a little bit, so we're working with ISOO on that process. Charlie Sowell, the policy working chair, will talk a little bit more about that.

Now, before I go and pass it on to the working groups. Heather just talked about a lot of open items, okay? And you guys know how I am when it comes to accountability, right? We have to do what we need to do together to close those iteMs. It is critical now, in case you don't know, we're kind of in a war, right? If you don't think the things that we're talking about here doesn't reflect those warfighters out there, then you're wrong, so we gotta figure out how to get some of these items close, right? So, that's all I want to say. So right now, I'm just going to turn it over to LaToya Coleman, who is the chair for the clearance working group. Over to you, LaToya.

LaToya: Thank you, Ike. So among a few of the things that, were in conjunction with a few of the things that Heather brought up that are still open items, I have a few, that I would like to, kind of foot stomp on, and, some that are...or at least one or two that are, that are new.

The first, the first topic that I have is for the Department of War. So over a year ago, Industry raised a concern regarding the military department's inability to expand Industry's SCI indoctrination authority, and the inefficiencies within the SCI nomination process. Early 2025, Industry briefed the Defense Security Enterprise Advisory Group on these concerns with the understanding that Industry would receive feedback and a viable path forward. In the May 2025 public meeting, the topic was once again raised with Industry, requesting that OUSWI&S help facilitate additional discussions with the military departments to move this issue forward. As of today, there has not been any resolution, and the problem still remains the same, as it is still taking a lot of time to get Industry personnel SCI indoctrinated. So, I raise this issue again today, asking that OUSWI&S help Industry further discussion in an effort to get a resolution. For over a year, Industry has voiced concerns regarding the military department's inability to expand Industry's SCI indoctrination authority, and it has resulted in inefficiencies in the nomination. So despite these efforts that we have been making with communicating with the departments, it still is an issue, and we are asking that you guys continue to look into this and involve Industry in trying to come up with a viable solution that will work for everyone.

The next topic that I have is the adjudication timelines. We've been having really productive discussions with DCSA regarding the increase in the adjudication timelines, and in this forum, I would like DCSA to share what is causing the increase in the plan to help decrease those adjudicative timelines.

The next, topic that I have is to ODNI. Industry is requesting a status from ODNI on shared covered insider threat information policy and the key management clearance policies. Both policies have been in development for over 3 years, with what seems to be no end in sight. Industry would like to request status on these policies. I'd also like to point out that this has been a topic that was brought up in multiple other forums,

including this forum in May of 2025. And additionally, pointing out that this is also a challenge that was addressed in the MITRE FAST study that was just released over a month ago. And we are asking that ODNI please provide a status so we understand where we are with the policies, and what Industry can do to help move those forward.

We are also looking for ODNI to provide a status on TORIS. The engagement with Industry regarding that system, the operational roadmap, transparency to that roadmap, and the timelines associated with TORIS development and ultimate implementation. Thank you.

Isaiah: Thanks, Latoya. I want to go back a slide. I'd be remiss if I did not welcome two of our phenomenal leaders from Industry. So, since the last time we had our public meeting Mr. Leonard Moss from John Hopkins Applied is now a great part of the membership, and Ms. Jennie Hardy from SAIC is part of the membership now, so thank you very much. They took the place of Mr. Greg Sadler. He's sitting out in the audience, right there and Mr. Dave Tender. So, I wanted to make sure that I kept that. All right, now we're gonna jump over to Mr. Charlie Sowell of the policy working group.

Charlie: Thank you, Mr. Rivers. Before I get started on the slide, I just wanted to address one of the items from the minutes related to executive orders. As a follow-up to the minutes from the last public meeting, the item on executive orders was listed as open and assigned to Industry. Industry's request in the last meeting was for guidance on the NISP related executive orders. The NISPPAC Policy Working Group provided a list of specific orders. I must say that the request itself was interesting. Although we understand that the NISPPAC was simply looking for Industry to provide examples of executive orders that impact us, we would expect our government partners would know which ones are, from their perspective, critical to Industry and why. With that said, we do appreciate the chance to provide input. And we'll continue to provide examples through our partnership. As an example, some of the recent executive orders that have come up that clearly have an impact on Industry include Executive Order 14383, establishing an America-first arms transfer strategy from February 11th, 2026 , and Executive Order 14369, Ensuring American Space Superiority. Now, these are more recent, but some of the executive orders that Industry has been asking for government direction on go all the way back to the first day of the administration in January 2025. And to date, we still have not received any formal guidance from any of the government agencies on those executive orders, and you know, where this makes a difference. One of the earliest executive orders related to the removal of security clearances from former seniors in the intelligence community that sit on our boards, or have roles in our companies post-government employment. And so, just having guidance from the government would really help us in that. So, again, thank you for the partnership and the dialogue. We look forward to continuing to provide examples, and we're available for any questions at any time from our partners.

The main item on our slide for the policy working group is as was mentioned in the opening remarks, the NISP was formed back in . And Industry security environment, our posture, our programs, our policies

were quite different in the s and in the jargon of my kids, I'm old enough to remember the industrial security program. The threats that we faced were very different back in that day too, and although the NISP has been revised, and I commend our NISPPAC predecessors and many of our government colleagues who are here and have participated in those revisions, Industry would like to embark on what we call an AI-enabled and subject matter expert verified, review of the NISP with today's threats, and capabilities foremost at mind. We believe that through the miracle of artificial intelligence, it can help us radically reduce the butts in seats that we need to perform this review, and can let Industry give some suggestions to the government, and that's all that it would be, would be suggestions and recommendations to our government partners from everything from minor tweaks and changes to the existing program, all the way up to a completely revised and new National Industrial Security Program. So, with Mr. Thomas's assistance and guidance, we're gonna embark on that Industry part, very soon after this meeting. And based on our AI , assistance and estimates, we think we can have the recommendations done within about three and a half to four months, and again, we couldn't possibly do that without the power of AI, but we can do it with the power of AI combined with subject matter experts and our predecessors at some of the agencies that are now in Industry that led the initial NISP creation, all the way through some of the revisions. That's all I've got. Thank you.

Isaiah: Thank you, Charlie. And Mr. Thomas, make sure you hold us to that timeline, sir. I'm all about timelines. Well, we're Industry NISPPAC, we're all about timelines. I'm turning it over now to the Entity Vetting Working Group, Ms. Jane Dinkel.

Jane: Good morning and thank you. The Entity Vetting Working Group hasasks of DCSA and the USG this morning.

The first one is regarding the updated SF 328 certificate pertaining to foreign ownership, control, and influence, which was issued and released to Industry about a year ago. This was the most significant change to the NISP since the 32 CFR Part 117 was released. Industry still has questions about the content of this form and requests additional guidance. Many of the questions are broad in nature and very sweeping. They require months of coordination with multiple stakeholders within their organizations to be able to properly complete and submit this form back to DCSA...specifically question . It asks if Industry has any contracts, agreements, or understandings with any foreign person, entity, or company. That's a really, really broad statement, and you can imagine, I can't imagine the interest that DCSA would have on an unclassified consultant agreement with somebody from Costa Rica. So the ask here is for DCSA to issue guidance limiting the scope and narrowing to what is truly relevant and necessary information for them to make a FOCI determination.

The second ask that Industry has in this, in this regard is that, currently, we understand that we're only required to submit an updated SF 328 when there is a significant change to the answers or to the content. We don't have to complete the new updated form just because there's a new updated form. We understand that. But these significant changes that

were made to the form Industry asks that because they require such extensive collaboration, for DCSA to reconsider the timeline under which they require these updated forms to be submitted. I believe the 32 CFR currently states for significant changes to be reported to DCSA as soon as possible, or some other non-specific language, which really has been implemented to Industry to be 30 days. That's the agreed-upon timeline, is 30 days. Given the extensiveness of these updates that are asked for in the new form, Industry would ask that DCSA reconsider that timeline and extend it beyond 30 days. Industry could still report it to their IS rep, say, in an email, to let them know there's been a change. We're working on updating the form, but we really need a lot more than 30 days to be able to complete the form with the amount of detail that DCSA is asking for, and that really makes the form valuable.

The third ask that Industry has of DCSA today regards our academia partners. There are many cleared academias throughout the defense Industry base, and currently, their facility clearance process is the same as a commercial entity, when they are really not the same as a commercial entity. Their organization is different, they have members of their board that don't exist within Industry, and so I would ask that DCSA re-evaluate how they analyze the organizational structure of academia to reflect the uniqueness of that structure and not simply mirror Industry. We asked for a solution, partnered with the academia organization, to be able to educate and explain the differences in those organizational structures and make this content value-added. Thank you.

Isaiah: Thanks, Jane. Now we turn it over to our newest member, Mr. Leonard Moss, and we'll give an update on the NISA Working Group.

Leonard: Thank you very much, Ike, and thank you, everyone, for the warm welcome. Can you hear me? Closer? That's the first time anybody's ever told me to get louder, so. Thank you, Ike. Thank you, Mr. Thomas, and thank you, everyone, for the welcome. I just want to begin by acknowledging Mr. Greg Sadler, who's out there, who did a phenomenal job as the chair of the NISA Working Group prior to myself, he has built such a strong partnership and collaboration with DCSA, and I have to go before that and recognize Rosie also, who established that partnership that has been tremendous. So what I told them I want to do is make sure I don't break this wonderful partnership that has been created. So that's why I told Rosie and Greg they can't go too far, even though Jennie has stole Greg, but it's okay. We'll work together.

So, I have just a few topics I want to address. The first thing I want to address is...this is for all of the CSAs, right? One of the things we are talking about is that strong partnership with DCSA is wonderful, we're going to continue that because it's working really well, and I'll talk about some of the things that's working really well with DCSA that I want to foot stomp, but one of the goals that I've inherited from the working group was that they've really been trying to build a stronger collaboration with all of our other CSA partners, which we don't have, and we need to build that, because obviously we have a lot of challenges in many other areas, which we'll talk about...some of those challenges, so we really want to embark this year to strengthen the collaboration with our various CSAs, so, I'm going to be reaching out to those of you

who represent those CSAs for your assistance, and how we can do that, you know, what makes the most sense. Obviously, I know nobody wants to have any more meetings, but I think we need to have a few meetings. That way, we can work some stuff outside of this space. So that's the first topic we have.

Another topic that was brought to me very recently is this is something that the NISA Working Group has broached before, which is this Commercial Solutions for Classified program. We talked about this a little bit yesterday, Jeff. This is becoming a bigger challenge for Industry, and the reason it's becoming a bigger challenge, for those who are not familiar with this program, this is really dealing with what we call the SIPR flyaway kits. And everybody in Industry, as far as our employees, they love it, right? Because, first of all, it's cheap. It's a lot cheaper than SIPRNet, right? Secondly, it's giving them the ability to get access very quickly. The problem is, from a security practitioner standpoint, we believe that the threat to national security needs to be addressed. So, you know, we talked to DCSA, and DCSA's position is very clear. This is not under their cognizance, right? This is something that's coming out from the various parts of the Department of War. I believe it started with NSA. I think NSA created this program, and it's a great program, by the way, so I don't want to give the wrong message that it's not a great program. It's a great program, and before, it was just for, like, these very senior government officials to have these flyaway kits, because they couldn't get into the facilities to access classified network. Now it's the embedded contractors are getting access to these flyway kits, and the concern is that they're using these at their homes, right? And as a chief security officer, I don't want my folks doing SIPRNet access at their homes. I'd much rather they do it in my facility. Problem is that facility's under DCSA cognizance, DCSA is not the AO for these systeMs. So, you know, we're trying to find a solution. So I wanted to bring it to this forum, where we have all of the stakeholders to say, what's the right answer, right? Because from an Industry standpoint, I would love to be able to say, "Okay, I can put it in an unclassified space in my facility that I can control and can have oversight. "But, again, then that puts DCSA outside of the cognizance, lane. So, that's the challenge. I wanted to put that out there so we can get some solution. I don't have the solution. I have some suggestions. We have a bunch of recommendations that's come to me from various folks, and my colleague Chris can speak on them if you want to, but we have a lot of folks who have this challenge, because it's starting to become pervasive, and there's more and more of these kits are being handed out, so we really need to get our arms around it. I don't want to have another situation like what we have with Classified Cloud, where it felt like you know, we were a little late with the policy, you know, catching up with the technology, and I feel like, you know, this is another one of those situations if we don't get our arms around it. So that's one of the issues that we want to throw out there for all of you to help us with.

Another, area of focus for the NISA Working Group has been the solid-state drive mitigations. This is one that, again, has been addressed previously, but from what I've gleaned since I've taken over this role in October, it seems like we haven't really made a whole lot of

progress. I think there's been a little progress, from what I've been told.
So, the DAAG, which is awesome, just by the way, I want to put something to DAAG, we'll talk about that a little bit. The DAAG is awesome. It has made some great inroads. The ask that we have, that the NISA working group has been championing is to support mitigations of these solid-state drives short of destruction, where a mitigatable solution is available until the true end of life. This is being looked at at the DoD I&S level, at least that's what I was told, led to believe, but that was prior to the shutdown. We haven't really gotten any kind of updates or status, so we'd like to really know where is that at, what kind of progress has been made, and what can we do to help.

Okay, so the next one on my list of goodies here is for DCSA. And this is good news. This is about the DAAG. This has been taken, since I joined the working group, that has been our primary focus, has been the DAAG, because this is what it's taken. Two, three years to get the DAAG published, and it got published in October, right before the shutdown. So it was great, it was great news, everybody was happy, but the shutdown happened. So, what Industry did was we collectively got everybody together to put together, hey, what are some differences that we see from the DAPM to the DAAG? And we highlighted those differences. We provided those to DCSA, and some of those we felt were either new requirements or concerns that we had. So DCSA has been great. They've provided responses. The problem was when we provided them that original spreadsheet, we weren't very clear in what our ask was. So we've cleaned up the spreadsheet, we've given them the new spreadsheet with asks, and so we're reconciling those changes. But there was one specific one that DCSA agreed to appear to be a new requirement, and Tracy Brown actually responded just yesterday. So, you know, I'll get that out to everybody so that, you know, they're gonna address it to make sure. Because for everybody's, information, one of the things that I wanted to have on the record when we met with DCSA was that the DAAG is not a requirements document. It's a guide. The word guide is in the title, so we have to make sure, regionally, that all of the regions are, you know, behaving accordingly, that it's not a new requirements document. It's simply a guide to help make these things easier for all of us. So, that was the good news about the, the DAAG, but we're making good progress since it's been released.

And then the last topic for DCSA was eMASS, and the NIST SP 800. 53, Rev 5. DCSA committed prior to the shutdown to leverage the voice of Industry for these iteMs. Software licensings and eMASS updates, as an example, and it is an existing processing and comms vehicle that the IA portion of the agency will leverage as well, and we've seen progress there. The software licensing focusing on the challenges of licensing commercial products where internet validations are required. For those with trusted download approvals, we're in good shape as long as we're completing an Ashley review. Those without a trusted download approval should consider revisiting the item, not only for software licensing, but for COMSEC as firmware. So SIPRNet remains a bit of a linchpin, but even if provided by a classified CD, DVD, there is a high to low action that your ATOs should reflect. So, one of the things that they're asking for

is a little bit more guidance in that regard. Alright. Let me enter the home stretch here.

So the next update I have is really to talk about the, currently, we're working with ISOO and Larry, and they're looking at standing up a new AI working group, and so we're supporting that and participating, and just want to put that out there, that we think that's a really good idea, especially since Charlie wants to, you know, revise the entire NISP using AI. We think it might be good to have those professionals engaged.

Alright, and then my last topic here is on the destruction of SAP IT material. I have two last topics. Destruction of SAP IT material. One of the challenges we have with this is that there's very limited approved options available to Industry, which is obviously extremely expensive. And some of the same technologies exist, you know, when it comes to destructive capabilities. So we're asking for collaboration and better consistency within the IC and the IC has been encouraging, but we need to do the same thing in the SAP space that we're not doing. That we've been doing with the IC, so we're gonna need some assistance there. We're still receiving stove pipe direction, that conflicts, lack of tech specs, leaving it to personal decisions by individual representatives, and as you can imagine, again, costly and very challenging.

And then on the COMSEC front. DCSA committed, again, prior to the government shutdown, to leverage the voice of Industry for this as well. And that's happening. Okay. Those without trusted download, I talked about that already, but for ComSec and as firmware, updates for devices are now high-site sourced. SIPR remains a bit of a linchpin, but even if provided by a classified CDPPD, there's a high-to-low action that ATOs should reflect. I said that already. We need the ability to discuss and address this. It must be in a secure space, compounding the challenges. So we need to address that. That's what I got.

Isaiah: Thank you, Leonard. Over to Ms. Jennie Hardy, in regards to NISP Systems Working Group.

Jennie: Alright, thank you. I just want to say thank you to Mr. Thomas. Thank you to Heather, and thank you to Ike for the wonderful welcomes that you've extended to me. It is a great honor to be sitting here. And I understand the gravity of the representation and advisory role that I've taken on.

So, with regard to the systems, I want to address, primarily the NBIS suite of systeMs. We understand these systems are complex. They are rapidly changing, we're seeing rapid implementation of those changes, and those transitions can be challenging. There are added agency users to the system as well, and with those agencies come their individual needs. And so, adding to that can create quite a fog for all the various users and our needs, and how we understand the changes. Engagement with Industry is happening quite a bit, but it's often not early enough. And what we are asking for is the earliest collaboration before the testing phase, and the birth of changes, and the ideas that are going to go into these systeMs. So that we can effectively collaborate, provide advisory, to help all of our sides succeed in the implementation of these changes.

And we very much look forward to the continued collaboration that we have with DCSA and with other agencies. We need visibility into planned system development before the work begins to ensure operational requirements are understood. We request advance access to training materials when changes are happening, and we ask that when testing occurs, that we have a representative sample of Industry companies. So, we're not just talking about the large ones that kind of understand the language and what to do, we're also talking about the smaller companies as well. We want them to have a seat at the table and have input in what's happening with these systeMs. And to that end, communication is such a big part of that. So, Industry represents, conservatively, 26,000, users in these systeMs. If you take the 13,000 contractors and you add in all the user requirements and redundancies, we've got a lot of people using these systems, and not everyone is as adept as the senior security managers who speak the language well. And so we're asking for concise, predictable communication channels so that we know where to go to look for what's happening. There's so much that's happening so rapidly. We need to be able to have a clear picture of what that looks like. And along with that, the roadmap. So, right now, with regard to NBIS, we have a technical roadmap that doesn't make a lot of sense to the average person looking at it and trying to find out what changes are coming down the road. So we ask for...it's highly technical. We need a stakeholder-friendly version focused on more details, impacts, and timelines. And we would ask that that be available to all of Industry as well. And, so, with regard to that, with the NBIS suite of systems, I do also want to address NI2 and the development of that system. We are just now in the system for the DD254 workflow, what used to be known as NCCS. And we ask for the same level of early engagement with the continued development of that system. Particularly for the other functions that are in development, the 847 process, and NISS, the movement of NISS over into the new system. That's all I have. I thank you for your time.

Isaiah: Thank you, Jennie. I'm gonna turn this over to, Mr. Chris Stolkey. He'll be, giving the the updates for Physical Security Working Group in place of the wonderful Miss Kathy Andrews, who couldn't be here today. So, turn it over to you, Chris.

Christopher: Yes, but first, I'm going to start with my working group, which is the Insider Threat Working Group.

Isaiah: Is that what we're doing with me, Chris?

Christopher: I mean, I like my working group, too.

Isaiah: All right, all right. Over to you, Chris.

Christopher: Alright, to start, our working group's been hard at work. Right now, we're looking at ways we can help Industry with some of the problems we're facing within our group, and I have a couple of examples on the slides. Like, one of the challenges we have is how do we really work insider threat when our employees are often sitting at government sites, and we're not having visibility on them, we're not necessarily getting reports? So we're working together to come up with some things to share with the rest of Industry.

A good news story I'd like to share, came out last year. DCSA changed the requirements for insider threat training for program personnel, meaning specifically the people that run an insider threat program. I understand why they made the change, but it was a pretty significant change for Industry, because our training time went from about an hour to about 5 hours, so a pretty significant jump, and while that training is very good and very thorough, it also covered a lot of things that weren't necessarily required by policy. So, NISPPAC, the Insider Threat Working Group, took it upon ourselves to create a new training that did meet the requirements. And in partnership with DCSA, they reviewed it, they validated that it meets the requirements of the NISPOM, and we're happy to share that across Industry. It's right now posted on the NCMS website. If anyone has a question or would like to get access to it, certainly reach out to me.

Couple other things I'd like to share, not related to insider threat, but again, shows the partnership with DCSA. We recently reached out to DCSA with a list of inconsistencies we've been seeing across the country, right? We got together with other security professionals, and we said, hey, what are you seeing that's happening in one place and not the other? Or in some cases, the complete opposite thing happening. And I appreciate DCSA's willingness to address this. They jumped on it very quickly. They're already reaching out to various members of the NISPPAC to address these concerns, and I look forward to closing those actions out.

And then finally, contractor open storage self-approval went live as of January 2026. This is a big one. It allows Industry, if you follow the procedures, to get approval from DCSA to approve your own open storage areas. This is something we had years ago, and it was taken away, but working with DCSA, they identified that policy would allow this to happen again, and so we came up with a plan, and it is now working. Initial reports are very positive in this, and we hope it continues.

Next slide, please. So, this is where I'm going to do my best to fill in for Kathy. Kathy is the expert when we talk about physical security, and really, when we talk about physical security these days, we're talking about 705 and TEMPEST requirements. Kathy is going to, and there's some stakeholder meetings you see up there. Every time we talk to Kathy, and some in this group attendees meeting with her, she's going to another meeting, and another meeting with a stakeholder to try to make sure that Industry's voice is heard. It's challenging. As you see the first line under updates, we've had some government people leave, which hurts our ability to get the timelines done and the priorities set. We expect ICS 705-01 in Q1. With this, we accept POA&M dates to likely be changed. We say likely, because we don't know. We hear about these things, we're tracking them. We know that a risk assessment tool is currently under development. I'm going to talk a little bit more on that on the next slide, so please go there.

So, our concerns. We understand and we expect a risk-based approach and a risk tool to be used to properly figure out where the risk is when it comes to Tempest requirements. The challenge that we're seeing is that risk tool seems to be trending in the direction that makes everything

high risk. If everything's high risk, nothing is high risk. Just like if everything is a priority, nothing's a priority. We want to work with the government to make sure that that risk tool is set up appropriately so we can really identify the risk. And we say the requirements do not adequately consider the broader risk landscape within the DIB. If you were to talk to senior security leaders within the organization, and you asked them, or you told them, we're gonna give you a million extra dollars to spend on security. I suspect their first answers would be insider threat, cyber, supply chain. I don't think it would be TEMPEST requirements outside the mandate from the government. And I think we need to balance what these risks are before we go forth and spend a significant amount of money on a risk that we don't understand.

There's inconsistency in reciprocity, there's lack of uniform interpretation across all of our customers. We really need the government's help in looking at, evaluating, and promoting alternative ways to solve this TEMPEST problem. There has to be a better way than tearing out a wall and putting it back up. Not only the cost implications and supply chain implications, but there's program implications. It's not like every company has a significant amount of swing space to close a facility down, work somewhere else, and then bring it back.

We're still seeing problems with accrediting organizations. If it takes 12 to 18 months to accredit a facility, that puts Industry behind on programs. And it really doesn't balance with what we're hearing from the administration. What we're hearing from the administration is go faster, produce more. It's hard to go faster, and it's hard to produce more when you have to shut things down. Or it's harder to invest in new facilities when you have to retrofit your old facilities. We need help balancing what that risk is. And until we do, until both DoD and IC get online with the same requirements, we're gonna continue to see, or prevent, the Industry from developing strategic, timely, and cost-effective options. Thank you.

Isaiah: Thanks, Chris. That is all that we have. I do want to thank, Sir Thomas and Heather, for allowing us this opportunity to talk about some things that are very, very important to Industry. We do look forward for the rest of the engagement here to see if we can kind of walk away from this today with some of these items closed, or a good path forward. So, thank you very much.

Michael: Yeah, thank you, Ike. Thank you to everyone who offered updates from Industry. Everybody hear me? Let me say one more time, thank you to Ike, and to our friends in Industry, who all contributed their updates today. We'll have a few moments for questions if anyone here in the room or online has a question they'd like to pose to one of our Industry members. We have folks in the audience, our colleagues here, will bring a microphone down. Just raise your hand. Yes, sir.

Unknown male: Good morning. This is a physical security question, so I know you're not the primary, so hopefully, hopefully I won't surprise you, but I recall at last year's NISPPAC, I heard a verbal comment, I believe it came from ODNI, that the government's goal was to try and

reduce or eliminate the use of U.S. persons in the construction of SCIFs, and basically insisted that all U.S. citizens would be involved in the SCIF construction. Now, to be fair, it wasn't on the slide deck, it was a verbal comment that was put out, but I've been asked, by some of the clients, is that still a goal or a consideration by the government, to eliminate the use of U.S. persons in SCIF construction, restrict it just to U.S. citizens, or is that just a comment that was kind of just thrown out last time. I welcome any thoughts or input on that.

Lisa: Hi, this is Lisa Perez from ODNI. Unfortunately, that wasn't me, and I'm not sure who would have said that from ODNI, so my apologies. I'm not aware of that topic, but it is certainly something I would be happy to take back and try to get more fidelity on. Unfortunately, I don't recall that specifically being discussed.

LaToya: If I could interject, that was a comment that was made last year, and it was a comment that was made by Tessa Dutko, who presented it, to this group, on that topic, and from what my understanding was that was a consideration, is to have U.S. citizens, removing U.S. persons, but having U.S. citizens as the primary, for construction. I don't know if that has made it into this version, I'm not sure what that looks like right now, but that was discussed, and it was a consideration.

Lisa: I'm sorry, just to clarify, you said removing...that it was up for consideration to remove U.S. persons from the construction?

LaToya: It was a consideration that the construction would require that all the workers are U.S. citizens, is what the consideration was.

Lisa: Oh, okay, okay, okay, that makes more sense to me. Okay, thank you so much. Alright, I'll take that back and try to get more fidelity. Unfortunately, I don't have any, any further details to provide on that this time.

Michael: Thank you, Lisa. Any other questions in the room?

Kristen Phillips: We have two questions on the line.

Michael: Perfect. It's just gonna go to you. Thank you, Kristen. You're gonna unmute them for us?

Kristen: Samuel, go ahead. You've been unmuted. Samuel, I've given you permission to talk. Alright, let's see. We'll go to Stephanie. Stephanie, I'm asking you to unmute yourself. You've got your hand raised. Alright, I'll keep an eye on them, and we can come back if we need to. If you've got other questions online...oh, Stephanie, go ahead. Stephanie, you've unmuted yourself? Okay. One more online. Helencia, feel free to unmute yourself. Alright. I guess we don't have any callers online right now.

Michael: Yeah, thank you.

Kristen: I'll keep an eye out.

Michael: This is Michael, may I have your permission to speak?

Kristen: You go right ahead.

Michael: It's been working on my microphone. Thank you for that and thank you for the folks that were attempting to give us your questions. You can certainly put them into the chat, and if we don't address them today, we'll include them formally and address them at a later time. We did have a question, one further question in the chat about whether there is a link to the insider threat training that was mentioned. They were looking for it on the DCSA website. Anyone confirm or deny?

Christopher: It's on the NCMS website, under the NISPPAC page of the NCMS website.

Michael: NCMS website. Would you like to read the URL out?

Christopher: W...no, I would not.

Michael: So, NCMS website, under the NISPPAC.

Christopher: The president of NCMS is in the crowd today. She can probably do it.

Patricia Brokenik: So, classmgmt.com

Michael: Great. Thank you very much. And, absent any further questions, we'll move on to our update from Mr. Jeffrey Spinninger, the Director of the Information Acquisition Protection Directory for the Office of the Undersecretary of War for Intelligence and Security will give an update on behalf of the Department of War as the NISP Executive Agent.

Jeffrey: I believe that constitutes permission to speak. So someone out there should have a mute button for me. So thank you very much to our hosts at ISOO and to all assembled today. I think most of you know pretty well and have heard me say, but I'll continue to echo, this is a very important forum. And we get out of it what we put into it, which I think is definitely reflected in here. And the seven pages of notes that...thanks, Ike, that I took during the comments today, but I think that reflects the level of maturity and growth in the way in which NISPPAC is being used. I'm old enough to remember when it was used this way before, and also, to be very frank, times when it hasn't been used to this level of effect, and I think it's both to be reflective of both of those, because, as I've already said, you get out of it what you put into it. And that's not to say that it's all wine and roses, right? There's some gnashing of teeth and occasionally some friction, right? It's not happiness engineering. But it's fact-based from all sides of the ledger, and we do the best we can, you know, with those things. I think when Ike talks about integrity and accountability, I think that that's what that sounds like, and that's what this ought to look like. So, hold us to task on that. Anything that I don't get right, save for Allyson, and, you know, with that, I'll begin.

You know, Ike mentioned this, and so I will as well, right? So obviously lots going on in the world right now. You know, in the department, it's pretty busy. There's, turns out there's 7 days in the work week, and there have been for a while. And that's, you know, that's great. It's what we all sign up for, and I mean that sincerely, that's what all of us sign up for, right? So, across Industry, right, you know, steady supplies, right, the anticipation of these things, all the pieces and parts that kind of come into it, you know, and that which we get to see play out in almost near real time, you know, in the media age that we live in. So, armed with that, I just wanted to share very briefly, right, so we've had a number of places, right, so in anticipation, what, you know, what war looks like in a modern era, right, and the flash to bang, and the need for security engagement and requirements, and things that relate to stuff that's been talked about here, right, vetting. Not in a conventional sense, with only where we think about it, or as we've always thought about it in the industrial security program, but the need to be able to do this at incredible speeds and in environments that we hadn't previously thought about that because of commercial markets, and the need to be able to balance the fact that, hey, we need to be able to enable those things, but also to exert some measure of control and that's the operative word here, or security, not entirely the same, to be able to support the warfighter on the other end of that. It's complicated, but the imperative is to, one, be able to deliver options. That's what we do as security professionals, right? It's very, very infrequently about yes and no. I have...no one has ever accused me of having a tremendous amount of patience. I have even less when I hear security people use the word, no. It doesn't exist in policy, there's very little that you can prohibit, and when we feel like we're in that scenario, those are where security issues become management ones. And at the end of the day, at the top of the food chain, we all work for the same people, so if we find ourselves in that place, we're obliged to bring them up. And I think that's, you know, maybe obvious, but I think something to say as we get going here, especially when we have major combat operations ongoing. So with that, you know, to, you know, again, I've already, I've already said thanks. I'm glad that we're back together. It's been a year, almost. It's kind of crazy when you say that out loud. And I want to acknowledge up front that the pause doesn't mean that there wasn't activity. There was a shutdown that didn't really change a whole lot other than the size of our paychecks, other than level of effort didn't mean, didn't abate at all in that time period from, I would say, most of the government personnel in the in the room right now. You know, and the pace of things and the expectations from leadership within the Department of War is acute and growing, in this space, and so, over the last several months, we've taken a hard and unvarnished look at the NISP, right? And we're going to continue to do that, right? And we've done that with active voice from, certainly the represented Industry personnel here, and about 6,000 or so more of your colleagues out there in the world, and we appreciate it very much. I'll talk a little bit more about that in a minute. You know, so the one thing I wanted to say, and I meant to lift this up, I think, right, so a little bit of history here, I'm pretty sure I'm the first Department of War representative to the NISPPAC, and I think that's kind of cool, so nobody's ever going to be able to say that again, and I'm gonna ride that horse pretty far, so I like that a lot, and so I would never try to

out-historian the historian, but I think it's, I think it's really great, and so I just wanted to bring that forward. I think what I'm going to do here, I've got a bunch of remarks here to kind of go through, because in addition to the seven pages of notes from just a few minutes ago. These guys have fed me with some more stuff before that, but I want to address, just kind of run through real fast, because if I try to do it at the same time, I'll screw it up...there's almost 100% certainty of that. And so, kind of just working through, first and foremost, right, I appreciate the shout-outs up front that Ike made. I'll have more remarks to say on the classified infrastructure as a service pilot, the brains of the operation is over there, and Amanda McGlone, right? So this is us leaning in. And I'll end up repeating this a bit, because I repeat everything all the time, especially if I think it's important. But, right, we're confronting the fact that policy doesn't limit this, right? I appreciate what Leonard said before, and I think it's a very important lesson for all of us when he uses the cloud, he points to the cloud, and the fact of the matter is that we measure progress over a half a decade, right, of a fairly straightforward issue, where technology and policy don't align. But it is very, very important that what we learn in cloud, and what we know in classified infrastructure as a service, is that policy doesn't limit it at all, right? So policies that were written a long time ago that didn't contemplate things like the internet, or networks, or systems, those words don't exist in some of the policies, that doesn't preclude us from being able to do it. Now, having said that, there's an absence of enablement, which is difficult, and I'll acknowledge that, and so there's an absolute need for change. We'll address more of that. But as we lift these things up, I want to continue to say, we've made no change to policy, as it relates to cloud, we've made no change as it relates to policy as it relates to demonstrating the ability to deliver faster in ways that Ike described, and I'll get into in a few more. I'm not trying to get out of the iron out and revise all of the crappy policy that we have. There's a long list of it, and please, by all means, my email address is jamie.long, so, but we...and we want to know that, but two things have to be true, because one, mission happens right now. Policy processes are harder. The less control that we have over the process, the more complicated and difficult it is. And so, when I think about when Charlie talks about NISP 2.0 and others, there's some great...there's some titans in this community, people that 30 years ago, when I was just the luggage handler for other, you know, titans of this, you know, this work, and that's actually what I really did, it was, you know, to be able to talk to some of these people and these historians. But I'm going to point something out, and Charlie said this, right? So the current executive order was issued on January 6th, ironically, 1993, by President Bush, about 2 weeks before the end of his administration. That's the last page, the last chapter of the book that took 5 years to write, right? So the rewrite of the executive order was a rewrite, so the NISP did not exist in its present form, right? It does now, but the origin story of what we know today as the NISP goes to 1961. Right? And there are precursors that are even before that, that Michael could, you know, I'm sure wax very well on, right, in the history. Now, it's important to understand that history for a couple reasons. One, because the steady-state and ever-present requirement of Industry as the arsenal of the Republic, right? We, you know, we go to war with your stuff, right? Our humans and your equipment, right? So, and that's a volatile

and lethal mix, and the demand signal for that, and the no-fail aspects of that are obvious to everyone here. But that's an arduous process, and so we fully endorse that. We got a lot more work to do right now, both within the frame of the policies that they exist today. And with need to make rapid revisions where we can to move forward, because security is about empowerment to get stuff done, and I'll say it again, second time, somebody can keep a tally. Show me where the word no exists in policy. And then let's build out from there. So you're hearing no from your security officers. You know, I mean, everybody gets to the top of the food chain, right, then no becomes an answer. But for the most part, for the rank and file, of which that would be me and everybody else, you know, down the food chain from there, right, we're about...we're in the how business. We're informing risk decisions. That's our job. And if you don't know that, or...or you're not hearing that, then you need to raise that. We get into some of the other issues, I'll address that a little bit more. So I appreciate that Latoya.

As we work through on the SCI Indoc Authority. So, we've been making some headway on that. I'm going to talk a little bit about it in some detail, you know, through my remarks, but I appreciate the consistent observation. It's not quite as straightforward, right? We like to say security's commander's business, right? We have a decentralized execution model. It's kind of how we do everything in the Department of War, so we try to create a uniform set of requirements and then we need to empower the latitude necessary to execute missions across the spectrum of warfare and of Department of War operations, and that can run from the most mundane aspects of delivering goods and services at base X in Oklahoma someplace or in kinetic operations in a theater of war. The security requirements, the policies themselves are entirely the same. Including the latitude for things like access decisions. So that's not an excuse, but I think we've made a bit more progress than you alluded to, but I'll wait to hear from you, because I'm sure you will tell me if you disagree. And so, which I fully appreciate. Mostly. I'm sorry, I'm kidding.

So, you know, on the info-sharing side of this thing, again, I appreciate the shout-out, you know, and the nod to DNI. We're definitely looking for some expanding guidance. I think that's absolutely essential, but there's nothing that precludes us from engaging in that space today, and I don't want to steal any thunder that Allyson may share or others, but let me say we're leaning into this inside the department, and we're finding ways to explore what is possible today? We've had some opportunities to really kind of reach in with some specificity on specific data asks, and DCSA, again, not for me to really kind of get into, to be able to explore how we can provide data to be able to inform those programs that all draw their ties to requirements in the NISPOM, right? So I appreciate the focus on insider threat. It is, in fact, a program. But as it relates to Industry, it's requirements that are defined in the NISPOM, and so, being able to explore the limits of that and the opportunities, that's something we're doing right now. I think we'll have some more to say on that, well before the next one of these, and, we'll allow the data to be able to speak for us, because we want to be data-informed, right? This has been a very theoretical conversation for far too long, but now we've got data in motion, and that gives

everybody the opportunity to see what's potential and how we're managing risk, right? So don't talk to me about the importance of the data in terms of sharing. Show me what is it telling us to put dynamism, I practiced that, into your security programs, those in Industry, but those for which help the government manage risk in the purest sense of the term. So I'm pretty excited to be able to mention that. We're a far cry from done, right? I do think we need that uniform guidance piece of it, but nothing precludes us from leaning in, and that's exactly what we're doing. And that is a very direct mandate that came from pretty much the top of the food chain within I&S, and some of you know, know a bit of the detail there. I don't mean to be, incomplete in the answer, but we need to preserve some opportunity space as it continues to play out.

I already mentioned the NISP EO piece of it, Charlie, I think that's exactly right. I think there are some real experts out there. It occurs to me that, I see the NISPPAC Alumni Association over here, which is really fantastic. We have all of some new members here. I think that is really fantastic, you know, great, but I think about it a lot, right? So the people who understand the importance and the value of this, honestly, are all of a certain age and experience, right? But the people, the crop of the workforce, both in Industry and in government, right? You know, more directly, we're all a little bit older than that average anymore, so it's incumbent on each of us in government and Industry to make sure that the next generation of people understand what this is, why it's important, the accountability that comes from being on the record, to be able to identify issues and challenges and opportunities, right? It's not all about bad news, and then be able to kind of hold ourselves to account to be able to address those for what they are.

Jane, thank you very much for raising the 328 issue, because you brought it here. That means I can speak on it, right? So there's definitely some work to do. I will say my office has taken a very keen interest into the revisions that were issued back in May. We're focused in right now, I want to be data-informed. Right, so I will defend my job, my office is to defend of the nines, the requirements if I can, right? So, I have many of the very same questions that you have asked. We have entirely the same questions, right? So, happy to talk about that in greater detail, and if it makes sense, if we can understand the value in the data, something that they taught us a long time ago in various and sundry schools, like those essential elements of information that inform decisions in risk management, then there'll be no louder voice, and I think I can win that pretty much any room that I walk into, on that. But the opposite has to be true, right? We see great and growing need to use the 328 and the information in it to inform other decisions of importance to the government. I alluded to a little bit of that in my upfront remarks, right? We have meetings ongoing here that the NSC is calling to understand the value of this information and cross-leveling information sharing across federal agencies for substantially similar issues. There are a lot of things out there that look and smell like FOCI, as is defined in the NISP, right, and we go back to the well frequently, and some of your companies that are involved in, you know, cross-nation transactions, right, mergers, and all those kinds of things are providing some of the same information to other people, or other entities of government, right? So if we're not kind of diving in there or exploring

the limits of what that can look like, then I'm not entirely sure we're doing good government. That's active conversations right now, so, we have, we have, I guess it's April 2nd is when we're next intended to be up there, so that's continuing to move. We'll hold that as a placeholder, but I welcome the opportunity to kind of pull the thread on this. We've got great partnership with the folks that do EVs Matt here. Thank you very much. And, you know, to really kind of get down into that so we can...we can help that part of the data conversation. And I appreciate also the nod to the challenges on the academic side of things, right? We're hearing that loud and clear. I'll own this one, right? So while the policies don't specifically preclude it, I said up front, continue to say it, some of them are not written in a way that is entirely intuitive, and there are places where there are disconnects. There's some bright line language, what's written in the NISPOM today, that allow for latitude for things like exclusions and such that go forward, but there's ambiguity and inconsistency in the department's policies, those implementing policies that create today. This creates friction and drag on DCSA. That's something that my office can undertake to address. Again, we're a bit more data-informed than we were before, so it's not just the locks that we have to answer about, the president of such and such must do this, right? We owe a little bit more fidelity to the conversation, and I think we can provide that as guidance right now. We don't think we need an exception, but I reserve the right to be wrong. Because I am all the time, but right now, we're trending towards that. We just cleared that with lawyers here recently, so it's a question of who can sign it, and we're going to look to be able to put that guidance out to help to give a little bit of rudder room to DCSA, to be able to kind of get after, which is today an ambiguous challenge, I'll say. And attention from this group, and hold us to task on that as we start to see that. When the guidance comes out, you can rest assured we'll bring it here through NISPPAC and as we work with DCSA to put it to practice.

Leonard, thank you very much for bringing up the SIPR Flyaway Kit. I was pleased to hear about it yesterday. This is an incredibly solvable problem, right? This one defies logic, and I think we need to kind of be very blunt about this one, but right now, so the government does issue these devices. I'm a user, right? And it is, you know, procedural management for how we use it at home and in places that are non-traditional for where we think about classified work. This is not new to the government. We've done this for a long time, and different theaters and regimes, but it's becoming a little bit more mainstay, and I think the trend should continue to go up. There's a lot to like about it, right? That thing's a dumb terminal, right? There's no latency on it whatsoever, right, when you're done. It's kind of the best parts of what technology can bring to security requirements. I like that a lot. Now who's around you? What are your circumstances, right? Is there an Alexa in your room? All those kinds of things, you know, all awkwardly having had to be confronted, right, in the modern tech environment that is everybody's home. That's one part of the equation, but that's not the part that Leonard raised in that that's the problem for Industry today. We have sort of this head-scratching kind of interpretation that says if one part of the government issues one of these devices to a contractor, for whatever reason, that's a validated government requirement. I think anybody in the room would agree with that. So if that's a validated

government requirement, and then we sit there and say, well, hey, as it turns out, there might be some crossover where that government requirement could extend itself into an accredited location. Now, I have to be careful here, because there's an entirely different regime or limitation where SCIFs and some compartmented facilities are concerned, and that's not what we're talking about. But if we're talking at substantially the same level, a facility that has been approved for secret performance, and a device that has been approved for secret comms of some flavor, right...email, phone, whatever. Those should be a peanut butter and jelly kind of a connection right here, and if there's a policy statement that that says it cannot be done, not one related to authorization, but permission, right? I got one part of the government saying you can do that. We have a government-to-government issue, which means that we should solve this problem before this body meets next, right? And way faster than that. And so I'm happy to take that for action, because we do give them to our contractors that are embedded, you know, with government locations, and if we're creating a place where we're creating a problem, and clearly we are, we need to be able to solve that one, because the idea that instead of being able to allow that device entry into an accredited location that it's somehow better government to say, Greg, hi Greg, I want you to go out to your car and sit down, put the windows up, right, but don't come into my facility in which you could have the exact same conversation if you and I were in the room together, but you cannot do it on the device for which there is no data latency, right? I mean, I think you have to say it that way. I'm noting that every word that we say on the record, because if this sounds absurd to you, then we're all in agreement. If this makes sense to anybody in the room, please jamie.long, right there, you know, no. But I want you to reach out to me, right? Like, I don't mind being wrong, but I don't think that I am, right? Because these are important tools. We need to be embracing the technology. Our policies don't preclude the use of these technologies, and we're creating, you know, an impossible scenario for our Industry partners who are getting requirements and guidance and direction from their customers, from the people who are actually awarding the contracts and who are on the hook for performance, and then we're giving an imprecise or inconsistent answer as a function of oversight. We have an opportunity to solve this for ourselves, or I guarantee you, the managers and leaders that we all work for will solve it for us, and that feels uncomfortable, and I would just as soon avoid that. Also, because if we're going to go after vexing issues and challenging ones, let's make them, you know, consequential, not how I would define this one, but noting that we're on the record, I won't say any more about that one. And so that's also a place where, again, I wrote it down when Leonard said it, right? Policy catching up with technology. The policy doesn't preclude this, right? How we look at the policy in order to be able to get mission done and manage risk, right, not just about compliance, that's what needs to catch up, because the policy doesn't say you can't do this, right? What we're stuck with is I got, oh, we've never done it. Okay. Right? But if we have a requirement, and we can demonstrate the security in that requirement, then we are entirely empowered to solve this problem with the people in this room and, more often than not, I'm confident that's the scenario. This is one of those places. So, please put this one at the top of Heather's to-do list, and we, I think, should have, you know, good news

to report on that one long before we get back together here, whenever the heck that is.

On the solid state front, you know, Leonard, thank you for continuing to raise that. I don't want to get inside the do loop here. DCSA's done some outstanding work on this front, and I'm going to leave it to them, right, to kind of get to degrees of resolution, right? We're a far cry from the end state of this, I'll freely acknowledge that, but, you know, testament to some forward thinking and really smart risk management, opportunities here to be able to leverage, you know, the onus is ultimately on the people who own the information. Right? But putting that on a clock, you know, because we can sit here and say, hey, all else being equal, if I have a scenario where I've had some degree of spillage or whatever, you know, across substantially similar networks, right? Secret and secret, which is more often than not, you know, what our problems are. There's certainly some high to low, but it's not quite as much as is hey, we've crossed streams across networks that are approved, but at the same level, but not for the same information. I think these are headways. I would point out, you know, there was a recent package to reconstitute an executive level, so four-star level, committee overseeing CNSS issues. This has been in play for a while within the CIO. I'm not sure where it is in the signature place, so I gotta preserve some decision space, but I will note that my boss and the CIO met on this particular issue here in the last week, and we were all in complete alignment, and so I'm pretty sure that will make its way forward. Again, that which we can shine some light on, this is being one part of a much larger suite of issues in the area of national security systems and such, but this is obviously an important part, so by creating that level of that kind of a forum and that degree of what we were refer to as oversight, I think, is forward progress, and so I'm going to lift that up right now, because it covers this, and then, frankly, several of the other issues that you mentioned today, Leonard, and that continue to be on our radar here, so, we'll see how that continues to materialize. I will say, beyond the work that DCSA has done, I've made some forays in some of the other communities here to kind of see what this issue is looking like in those places, especially where we're, you know, some of those data center environments where we're not just dealing with those onesie-twosies. The one ask I would continue to have from Industry is your data tells this story, right? So we, you know, the more specific examples that you can lift for us then I think we can help to inform the scope of the problem as it continues to grow. I'm not sure that gets the visibility that necessarily needs in order to really kind of get after the core of the problem.

The destruction issue...Leonard, thank you for that. This is an opportunity...I'm not sure he's here, so that's really great. Happy to point some work out at Rob Sanborn and the CSSWG. I believe their spring conference is coming up in a couple weeks. This is one that I think is something that should be lifted there. That's not a dodge on our part here, but there are levels of complexity in the destruction side of SAP.

You know, at those places where there are inconsistencies, you're gonna have all the head sheds all in the room together at the same time. I think that can be the forum for a really kind of earnest conversation there. I don't think we have a policy prohibition. But I can tell you, you know, on a non-public forum, we do have some real probleMs. Being able to articulate that with some specificity is something that I think is best served by them, and then being able to see those places where we might be out of alignment with the kind of guidance that you're seeing from the IC, that would, I think, instruct the conversation. I think I'll be there, unless he rescinds his invitation, so hopefully we can lift that up for discussion there, Leonard, so thank you for that.

And then finally, Jennie, everything you said, I agree with, and really sounds completely reasonable. The largest single constituent of systems that you describe is Industry, right? So, like, bigger than the Army. You know, not bigger than the totality of the department, for sure, but if we think of Industry as a constituency, there's...I don't think anything you said is unreasonable. Anything that my office, or, and I'm very confident I can speak for my battle buddy, Jill Baker, on that, that we can help to assist in that, we're happy to support that as it continues to come in. When we get down into the eachs of...across each of the various, you know, systems that are there, and the current and future requirements. So please, keep us posted on that.

Chris, we already talked about the one part of the insider threat. I really appreciate what you shared on the training side of this thing, right? So the department...Secretary on down, there's been lots of public conversation on training, and there's too much of it. It's inconsequential, you know, and it's incredibly costly. So the difference between 5 hours and 1 hour of training is not measured in just the time alone. That's dollars and cents, and we want to be able to be able to understand that. Again, if somebody can articulate the benefit of the 5 hours of training in measurable ways, then you'll have no stronger advocate than my office, and again, I can kind of...there's no daylight between Jill and I on this issue. Although I'm happy to say that she's responsible for insider threat, but we need to be able to do what makes sense. I do have a question, though. And so, in the revised training you all put out, which is substantially smaller, is there any friction in terms of the acceptance of that training as the annual, as the requirement?

Christopher: Not yet, and that's thanks to our partners with DCSA. With the training is a letter from DCSA that says it's validated to meet the requirements of the NISPOM.

Jeff: That's excellent. So we want to keep a kind of a sharp eye on that. I'm aware that sometimes there's unevenness across the CSAs as it relates to your training and whatever else, and so, again, I see those more...those need to be floated up into those governance and that managerial side because that's not really a security issue, it's a management one, so I'm glad to know that.

And Chris, again, on behalf of Kathy, yep, I think that's great, all the things you said, I believe there's a meeting upcoming with NISPPAC

Industry and DNI, I think it's Friday, right? Lisa's on the call, right? So I guess, like, that's about the, I think that's.

Lisa: Yes, we have a meeting Friday.

Jeff: Yeah, I think that's great. We were happy to see the invite for that. We certainly have a lot of equity in it, both from understanding the risk side of it, but there's really two different risks, right? There's certainly the risks to mission, right, you know, that are the underpinning reason why we have these kinds of facilities. But for the department, who is by far, by far, the bill payer for this, right? Understanding, you know, we owe very much the same thing that Chris articulated today to our leadership. And we want to be able to do what makes sense, right? We are, you know, but we need to be able to understand that in brass tacks while mission gets done, right? And so I think you, you know, just to foot stomp what you said there, I think is great. So, with that, I can skip through a bunch of this stuff, right? But I just didn't want to miss any of those things, because I think they're very important.

A couple things I do want to kind of call out. The one, and I'm going to give credit to LaToya, because Ike's leaving anyway, and so, and that is for mentioning the FAST study. I believe both of them mentioned it. You know, we, cannot say thank you enough to Industry, you know, for the outstanding lean-in for this, right? You know. This is kind of a once-in-a-generational thing. You know, to me, it's a precursor to what Charlie and what NISPPAC Industry are thinking in terms of a NISP 2.0 kind of a construct. Lots of details that are going to be needed there, but understanding where we are, I think is incredibly important. Lots of opinion, you know, that are out there, 6500 thing, right? Yep, it's been surfaced that these are...there's a lot of opinion there. That's true. But it's objectively measured by data scientists, and I think that that gives us, at minimum, a barometer reading to understand where we are, and then be able to overlay that with the expectations that we hear in our leadership now and that we can anticipate in future leadership, you know, next year and 10 years from now. Because what we do, right, has that kind of staying power. I point back to 61 or earlier, right? The core mechanics of that are unchanged. They're not going to change, they're not going to change in whatever NISP 2.0 looks like, right? But being able to understand that, and where the tension is, right, that's the first...that's, to me, may be the critical step, because while we want to think about the EO, then it's Plinko, right? Through regulatory process, right? Regulatory process gets us down to policy, and when I overlay that, even if I start with 1993, the CFR, I don't even remember 98, I think, right? So, from 93 to 98, gets us a new CFR, and we danced on the overprint and all the rest of that kind of stuff in the early parts of the 2000s, some of you remember that, and we issued the NISPOM only 27 years later, right? So, like, and so we can't be limited by that as we start to think about it, because this is a very dynamic set of requirements. But I wanted to say thank you for that. The FAST study, you know, helps us to understand delays and inefficiencies that we are experiencing, they're not the exception, they are the rule.

And so, I meant to lead with this up front, right? So, lots of time. I'm not a big fan of time as a measure of a security program, but we have to be mindful of it. Obviously, but the one thing I wanted to say up front here, and this is, I think, credit to Matt Roche, but the only timeline that matters is the time from contract award to delivery, right? To full performance and delivery. And this is something that we have to do much, much, much more acutely across all the various regimes that kind of sit with under NISP, right? Meaning that when a contract is awarded, when can a company perform all the expectations across that contract, right? That's a conversation in eligibility, facilities and otherwise, systems and otherwise. It's a function of access, and then, you know, those things, right, all of those impediments have to be laid bare in order to be able to do something about that. Now, that's not where the conversation should end, however. That's really where it begins, because actual security performance then happens after those things happen as well, right? That's where we really want to be. I want to be in the oversight business. I want to be able, in the active management of security requirements, while performance happens. And too much of the conversation today is all on the front end. It's actually the prologue, excuse me, before we get to the first part of the story, and we're seeing this in uncomfortable ways. About the only thing we can do right now is to be able to overlay the costs associated with that, right? Actual dollars and cents costs associated with that. And that's us calling a little bit of fire on our own position, and that's collective. But that gets that kind of attention and speaks in the language, you know, dollars and cents kind of a language, really kind of helps to lend light a fire under opportunity. We're seeing that play out right now.

If I just skip ahead a little bit, when I look at it on the SCI indoc piece of thing. And I did say there's a little bit of light here, but the million hours or so that INSA estimated a couple years ago, in terms of loss, we did a version of this in testament to Annie and some entrepreneurial engagement within the Department of the Air Force to really kind of understand, as-a-service capability, really, and I wouldn't want to, you know, waste time in the description of it, but to be able to lean into this and see a reduction in timelines. And so, in just one initiative...I appreciate we want to do something maybe at the Air Force level, but I'll echo what I said earlier, right? We have decentralized execution processes, because that's how we manage and execute just about everything in the department. So an element across the DAF where they're doing this body of work, and they've seen a substantial reduction. I wrote down what Annie was gracious enough to share with my office here recently, but a 60-80% reduction of processing time, which recovers about $ million a year in one, you know, one part of the Air Force where SCI requirements are of a pretty steady state part of the requirements for contract performance is concerned. So what are we doing right now? Our job, our office is raising that up. And we're lifting that out. We want to try to be advocates for a greater expansion in the pilot. Which is the way, if we can find the resourcing for doing that, and I'm committed to look for those, to be able to assist and continue to partner with the Air Force as they showcase the ability to normalize that. And then we're able to do that, then you're showing offsets. We can go back to people who would then pay the bill in the Air

Force or other places and say, hey, if I avoided $100 million of people reading a newspaper, because, of course, that's after a contract is awarded, and after eligibility has been established, which means that that's all billable, even if you're reading a paper, then I think then we're being able to shine a light on something that's not a security process, it's an administrative one, and there's an important distinction there, because we can solve those, you know, through awareness and then directed management. And so I think that's where we find ourselves today. So, LaToya, to your point, that's not a solution to the problem, and it's not entirely the same as saying, yep, we're gonna go in and we're gonna tell...we're gonna use some iron pen here and tell everybody to delegate the authorization processes to Industry, which is permitted, but what's also permitted is that we allow the units and organizations across the department to manage risk as they see it, and so we have to be able to do both of those in equal measure, and then continue to pay attention on it. So we're not solving the problem, but I also don't think we're a bit further down the road. We need to do more of this. I'm hopeful to be able to find those funds here, and then maybe at a future opportunity would be great to...I'll put Annie on the spot here, so she can showcase what this looks like from a component level. And then, you know, out to the others that are out there, right, so the mil depts and others, to be able to pick up on these initiatives, so that we're then defending that independence of execution but with a measure of oversight that helps us to get after a problem that is clearly evident, because when I do the math, if I accept, you know, rough order of magnitude of INSA, we're talking hundreds of millions, so, much, much higher. If I accept the numbers that the DAF gave us within one part of the Air Force, and then I do a little bit of Cookie Monster math across the broader department, then we might be moving from hundreds of millions to billions pretty fast, and this is an important and essential opportunity.

So, let's see, touched on FOCI, leadership, yeah, so hey, lots, lots going on at DCSA, I was asked to mention that, so I did. So, commercial classified infrastructure service, couple things I wanted to continue to footstom. Again, echoing some of what Ike was...had said, and Leonard and others raised up. You know, Dave's not here, right, but DISA is, so Roger, thank you, so we...this has been an incredible partnership. It has continued to move forward. It's one of those places where and, knowing we're on the record, right, but, you know, we had some congressional lean-in on this, right? We helped to assist what that looks like, but I think it's great, because it puts us on notice, and it gives us opportunity to move forward. And so, you know, Amanda, through some, you know, some real great brokering of relationships. Leonard, I can't remember if it was Leonard or Ike, as he wanted to know who it is that we're working for. It's not really mine to deliver here. We've got good partnerships across the components, right? So we're working with components that have contracts for these kinds of services now, and in working with those military components, there are some commercial providers who see this as a bona fide capability across a large, you know, maybe not fully serviced constituency that exists today in Industry. And so we'll continue to do that, right, and by shining a light on it here, I think we really did have a breakthrough a week or so ago in terms of kind of laying out not just the facility side of it,

right, the physical infrastructure, but more importantly, on the information systems side of it, which is, today, those things all end up having in sequence, and that sequence creates a crazy timeline that can measure without exaggeration into the year's length. If we're talking SCI performance, it's not unreasonable to estimate that's a 48 month timeline, and that's after a defined requirement from the government. That is just not acceptable by any measure. But there's been some progress right here across a couple of these operating locations that are in service to government requirements, you know, in contracts. I'll leave it to others to tell those in greater detail, and some of them will become more apparent as performance begins to make its way out there. I think there's better opportunity to let that happen organically. Our job is to continue to put, I think reasonable, but I'm the one speaking timelines to these things, so that we're able to continue to maintain a cadence. I will say that we're doing that now. We're meeting about every other week and it's an end-to-end thing. It begins with the facility clearance and all the attendant pieces and parts that DCSA does, but it continues up through the security continuum into those compartmented areas, both for where the IC is related to and, of course, department special access.

And I think I see our academia already did that one, EO, I agree. Oh yeah, CUI, last one. Because why not end with that? Hey, so we, you know, appreciate where we are on this, you know, we wanted, like, to see this form. I used to not be a big fan of CUI coming up in NISPPAC, but I've kind of reversed course on that. I appreciate that some of the open tasks that were discussed in the early on were closed, and that's fine, but I'm going to continue to ask ISOO as the executive agent to continue to please help driving clarity, consistency, and resolution across government. We got a lot to do inside the department. I'll own that, 100%. On behalf of Devin Casey, who we stole from ISOO, which we're glad of, but we need...we still have a lot to do at the executive level, and so I would ask you all to please continue to do that. One of the questions that was asked early on, I did want to address, I was pleased to meet with the department's acting CISO yesterday, and I just want to put out there, related to CMMC, the Department of War CIO is currently standing up a CMMC listening session. There'll be a series of these things upcoming. The first one is going to be hosted by the Defense Cybercrime Center, which I think is fantastic, because it creates work for my friend Les Bernys, which I'm happy for. But more than that, because it's an intersection of where most of the DIPCS program lives today. So, the timeline, the scheduling of that hasn't landed yet, but it will be soon. I apologize for the uncertainty. As soon as we're able to put some fidelity of that, that's literally this morning, that came in, then, rest assured, we will put that out there, and we'll be a present company will be on hand to assist in that. I just wanted to lay that out for the group. Alright, happy to answer any questions.

Michael: All right, thank you, Jeff, very much. And, does anyone have any questions for Jeff here in the room?

LaToya: Jeff, you know I couldn't let you leave without asking a few questions. So I thank you for addressing that there is work happening, and I look forward to hearing more about that work and the data

associated with, making that concern, or gaining a resolution to that concern. So I look forward to hearing more about that. The next comment that I have is regarding CUI. I was reluctant to say this on record, but I am surprised that it's closed, because there is still a concern within Industry as it pertains to CUI and the lack of consistency and proper guidance regarding CUI. So it was very much surprising to me to hear that it was closed, and I would like, to ask that that not be closed, and that it remain an open item until we get to some point of, at a minimum, consistency, with how it is implemented across government to help Industry be able to, to meet the requirements that are set forth.

The last thing that I had for you specifically, Jeff, is not so much of a kudos, but more of a question regarding the MITRE FAST study. Thank you, MITRE. Thank you for, for, for, you know, pulling all of that together. That was a major feat, and provided, what was approximately 200, almost 200 pages of very good data, to drive some, hopefully, great progression in government and Industry. But my question for you is, what are the next steps regarding the recommendations that were, that were put into the MITRE study, and will there be, timelines associated with those, and transparency associated with what you are addressing and what you will not be addressing?

Jeff: So, hey, thank you for that. So let me work backwards on your answers. Number one, yes to the transparency piece entirely. So the biggest next steps here, right, so MITRE and the study got, is done, and we beat the clock related to one other thing that I didn't mention, which was, you know, we're pending a GAO report that should be issued here shortly. Weeks, not months, you know, from now, right? So we've received the draft, we've got recommendations, right? So those of you familiar with this understand that there's a measure of formality in the reviewing of drafts, in the response, so that it will go out. The FAST...I will say, one, at the macro, right, you know, GAO tends to stay kind of at a little bit of a higher level in its assessments, where there's a heck of a lot of detail, part of the record, within FAST, I will say they are entirely in alignment with one another. And so, as we start to build remediations, right, to be able to kind of address things, we're looking to kind of clump them together. Some of that's, you know, discussions that we're looking to have inside the department right now. We've invited kind of at a working level to this point, engagement from the military departments in particular and others. I will say, that remains aspirational, right? We're gonna put a little more formality to that here pretty quickly. I had some discussions with that with Army leadership literally this morning, so that will continue to play. My goal here, and again, in the interest of transparency, is that that will align to those outcomes and the deliverables that the department will owe in response to the GAO report. So those will be entirely complimentary. The timelines for those kinds of things, and the awareness of that are measurable, and it plays out entirely in public, right? Everything that you'll see orients around to GAO. What that does for us is it gives us a small measure of efficiency, so we're not doing substantially similar things in two different regimes. We're just going to lay one over the other, and they go, yep, GAO, everything you said. Hey, by the way, here's this 209 pages, right, so, of material that largely reinforce everything that you saw right here, and here's how we're getting after

that. There will be absolute opportunity for engagement. We're looking forward to this. We know that you all have won for all the contributions the Industry made into the data that really encompasses the bulk of that report, you have a lot of interest in, and I'm sure, ideas as it relates to what the remediation should look like also. And so, whichever one or several working groups that that should fit within, you know, we require only the invitation and maybe about a week's notice to be able to bring that forward, because I think that creates more work for Amanda McGlone, which I'm a big fan of, the work, not, not really Amanda, but so we want to be able to...so I think that that becomes incredible. One thing that also relates to that, because these things, again, we're looking at a little more parallel processing, and I failed to mention one other thing, which is the department's manual for the NISP, right? So 5220.32 Volumes 1 and 2, right, are about to go out to coordination, into...I mentioned this yesterday in the DCSA forum, should be within the next week or so, that's, we'll say a week or so, right? So we're aiming for this Friday. We're going to submit it to the folks who do that work for us by this week. There's almost always some back and forth because of well, just, there's always some back and forth, and so...but it will go out. As soon as it does, we will get it here through Heather and company to NISPPAC. One of the things that was lifted yesterday was, like, hey, you prefer to have less than, like, more than, like, hey, here's a week. So the coordination pipeline will be open. The first thing that most components do when they get an issuance is they ask for an extension. We're not going to do any of that, right? So, but what we'll tell you is it's generally open for about a month or so. We'll kind of give you the same time period. And I'll lift up for you and anybody in Industry, right, we hold no allegiance to the words, except for when you want to make a change, tell us why, right? Something stinks, or it's ugly, or it doesn't...this is bad, or that's wrong, or how could you be so stupid? All fine, I hear it all the time, but if you give us inputs that are constructive, right? If you change this, this is how we're able to do that, then we're able to kind of bring all that together and then bear it in. So you'll see those things then, hopefully you see the linear progression in that, right? So we have the GAO report comprehensive, excuse me, we have the FAST comprehensive. We have the GAO macro substantially similar, and then we're on a glide path to put out new policy, related to what NISP implementation should look like, right? So if that feels like a linear thing to me, if you disagree, then, well, tell me later, but yeah, so, like, that's how we're...that's how we're playing that out. So I...I can pledge that piece of it. There's 170-some-odd different recommendations in there. We're not looking to address those one at a time. We're going to chunk a lot of them together. We think Classified as a Service addresses probably upwards of 70% of aspects of them, right? So that, like, that's kind of where this needs to be. That's what it's intended to be for. It's a tool, it's data, right? As you said. How we use that data in those pieces and parts, that's a partnership, and that needs to be done as collaboratively as possible.

Michael: Question?

Isaiah: No, Latoya got it. She answered my question.

She, she asked him that question.

Michael: Charlie?

Charlie: Yeah, so, Mr. Spinninger, thank you for your comments, and I think one of the big takeaways that Industry will keep in mind as we put this NISP 2.0 thing in place is the speed of policy. I remember from ODNI, once the switch came between security executive agent directives being able to be directly issued from the DNI to the OIRA process, wow. So, point well taken, and the impact that that has on the government. All the things that you have to do to coordinate something like that, so...so definitely, considered. I would just say that as long as your leadership philosophy is at play, where no is a...is not in the policy, we're great. The challenge becomes when there's a change in that leadership or a change in the philosophy. And so Industry constantly strives for the policy to embody the philosophy, and that's where we're trying to go with this, so...so thanks for your partnership.

Jeff: Yeah, thank you for that. I think that's exactly right, right? Look, leaders, you know, everybody comes in on a clock, right? The policy is intended to be more steady state than that, and in fact, it is, right? So as we're approaching 40 years of the, I don't want to do the math, but closing it, whatever the heck it is, a long time since this was written. It's intended to be enabling of those places, and in fact, it is, right? And I can make a very strong argument for that. That's not to say that it's doesn't create, you know, like a relearning, which puts latency into things, because the leadership does change. So I completely agree that I think the revision aspects of what you're aiming for are exactly...we need to do that while we continue to do what we're doing right now. And I will say, I will say the leadership direction that we have from within the org chart, which right now is conveniently entirely the same, where I&S and DCSA are concerned, is unambiguous, and, Tara, Ms. Jones, speaks very specifically about, right, faster than possible, and at first, you're like, well, that doesn't make any sense at all, until you're like, well, I better not slow down and ask about that, because we're trying to meet the pace. There's opportunity in that, and we're looking forward to seizing it.

Michael: That's great, and one...one, further question for you from the chat. Jeff, we had, let's see...Mary Deffenbeck asked, about the listing sessions that you referenced on CUI, and what the audience for those would be.

Jeff: So it's definitely Industry. Well, so for CMMC, right, those are the listening sessions that CIO is putting out, right? So, you know, you can't really think, you know, one layer below the surface of CMMC, particularly as we get into two and beyond, is a conversation on CUI. So we'll definitely be there, you know, and as an act of a supporting role as is necessary, but they shared today that those are...the timeline hasn't been established yet. He just shared that, you know, the first one will be at the Defense Cybercrime Center, be hosted by them. I think that is...I was really happy to read that today, or hear that today. As

it materializes, we'll definitely get that out there, but active voice is here, don't tell me all the things, but don't stop the conversation about what's wrong, or inefficient, or complicated, or whatever, right? Let's think in terms of acting, because the cybersecurity piece of this, on those unclassified systems that feed all of the classified performance, right, there's a real problem there, and we need to get after that. While we help to work and consider the complications of regulatory policy.

Michael: Thank you. And I'll note that we have a variety of questions that have come in on the chat, and some of those are better directed to some of our later speakers, so we're tracking them, and we'll pose them as the relevant speaker is up for their update, alright? Pass it over to Heather for our next speaker.

Heather: Thank you, sir. We'll now hear from Ms. Allyson Renzella, the Senior Policy Advisor for Industrial Security at DCSA. Allison, come on up.

Allyson: Good afternoon, everyone. Can you hear me? I'm glad to be with you today. This is my first meeting as the DCSA representative, so it's good to see everyone in person. I've attended a lot of these over the years, but this is my first one as the official representative, so, thanks for having me, and it's good to be here.

I wanted to start off highlighting a few recent initiatives, that we think demonstrate how collaboration and coordination with our stakeholders, both from Industry and government, are driving outcomes. So I want to highlight a few of those, what we think and hope are success stories. First of all, as we mentioned several times, I want to highlight our commitment to the transformation needed to modernize the NISP. Over the past few months, we've been working with all the stakeholders to design an IT solution that will allow access to secret-level systems at classified infrastructure-as-a-service sites, excuse me, as needed to support faster, more agile, and more secure NISP operations. I am pleased to announce that we have developed and are executing a plan that balances security with simplicity and agility, using no on-site data storage, enabling Industry connectivity to classify communications equipment that has traditionally been rare. This has, in the past, resulted in workarounds and delays to contract performance, without that access. So this supports access to both existing networks and new cloud environments, all under a single authorization. To those of you who participated in this development process, and it is a work in process, we can't thank you enough for your innovative thinking and your commitment to, making this, what I think is going to be a successful outcome. Another example I'd like to highlight, we also, want to thank Industry for successful coordination on a couple other recent initiatives. As mentioned before, we have implemented the DCSA Assessment and Authorization Guide, the DAAG. It is a work in progress, so we appreciate the continued feedback from Industry to refine it and improve it. And that does include guidance. Again, guidance, not requirements, guidance on spills regarding solid-state drives. So we have included some options in there for Industry. You can request, from the information owner or your government customer, you know, some

potential pathways, rather than just automatic destruction. So we appreciate that, and then also, as was discussed earlier, thanks to Industry for their steadfastness and, helping us to enable self-certification for open storage areas. We are hearing that this is a success. It was always allowed in policy. I think just it got removed from the NISPOM, so people construed that as it was no longer allowed, but that was not the case. We felt it was appropriate that it's in government policy, that this is allowed. So, thank you for bearing with us as we work through that, and I'm glad to hear that it's working well. I want to provide a few updates, on where we are with clearances. We hear you on the adjudicative timelines. We acknowledge that those have been going up. I'm gonna allow my colleague, Ms. Donna McCloud, to talk about that a little more during the clearance working group updates later in the meeting, but as far as facility clearances, the timelines are continuing to trend downward. As of last week, we have between 350 and 360 total of cases, but those timelines are going down, and then from the system side of the house, I wanted to give a few updates on the National Industrial Security System, Increment 2, NI2. The goal of NI2 is to streamline industrial security processes by incorporating existing and emerging workflows into a unified cloud environment. This will include incorporating the NISP contract classification system, formerly known as NCCS, the FOCI expansion effort, and current NISP functions. By automating data integration from various government, public, and commercial sources, NI2 will hopefully enable efficiency, reduce costs, and facilitate information sharing across the department. On January 30th, DCSA officially launched the NI2 increment, which replaced NISS. This is the NISP-specific piece that was launched. We acknowledged there were some hiccups, but we are working through that, and just as of, last week, March 12th, we released an update. This release resolved the Legacy 254 upload issues and several post-launch and backlog issues. Hopefully users didn't even notice the release, there was no downtime and the impact was limited to possibility of an expired session, or the need to refresh their web browser. This fix, the summary of fixes in this release, it was focused on introducing a complete workflow for legacy 254 uploads, and correcting critical bugs affecting contract account manager users. Those Contract Account Manager users fixes, resolved the document upload issue. It fixed a bug preventing some pending account managers from being correctly prompted to upload their appointment letter, and sought to address an issue in the core task service that was incorrectly blocking some 254s from moving forward in the system.

Next, I want to talk about the FCL Handbook. That is a work in progress, but I also want to thank Industry. We know there was a short turnaround time, so we thank you for your valuable feedback. We did incorporate that. It's in draft. It's still being coordinated internally. We don't have a specific date for a release, but we know it's a priority. This is an important tool to reduce rework and rejections of sponsorship packages, and just give more clarity to new entrance into the program, so, it is a very important tool that we're trying to get done as quickly as possible.

We heard you on the NISP inconsistency issues. We thank NISPPAC Industry for providing that very detailed, specific list. We know this is nothing new, we're working to address it and we want to just emphasize the fact that we are striving for consistency in process. There may not always be the same outcome based on the specifics of the circumstances, but this is what risk-based decisions look like. So that is the goal, is that we want consistency in process, so we'll keep you informed, and when you do identify issues, let us know, but I would suggest we need specifics to best address the issues. You can use your NISPPAC reps, as you have done quite effectively, you can also go through your industrial security representative, the field office chief, or the regional directors, and they will bring those issues to our office to address.

Okay, switching gears, when I talk about Trusted Workforce, as we affectionately call it the TWIG, the Trusted Workforce Implementation Group, that group has been stood up and the goal is to execute ideal future state Trusted Workforce 2.0 business model, building a prioritized plan to transform personnel vetting and iteratively deliver value through Trusted Workforce 2.0 products and shared services. The TWIG is regularly engaging with customer agencies and key members of Industry to provide an overview of the end-to-end future state personnel vetting process model and collecting feedback from customers. Some highlights of recent accomplishments include, delivering an online status tracker for new applicants via the eApp automated email. Individuals can now view real-time status of their e-application from initiation to submission and it shows the average number of days within each phase specific to the respective case type. We've also rolled out the PVQ, the personnel event questionnaire, at the end of February to 2500 users for immediate use for their 5-year updates, and are currently executing limited engagements with select Industry partners to transition to the PVQ for the 5-year renewal. Also, many of you are tracking Rap Back initiatives. The government went through this ourselves not too long ago, but we are now focusing on Industry partners, getting them enrolled in Rap Back. That is the record of arrest and prosecution back. It's a service provided by FBI that enables real-time notification of changes to an individual's criminal record and it uses the automated fingerprint identification system, and retains fingerprints for comparison against other fingerprints in the FBI database. So why is this important? It's important for continuous monitoring. It facilitates continuous monitoring, ensuring that cleared personnel remain trustworthy throughout their eligibility. It offers increased security, it enables quick identification of potential security risks posed by cleared individuals, allowing swift action time and cost savings. It is significantly more efficient than conducting repeated, full-scale background investigations from scratch. So, there is a phased rollout for Industry planned. Phase 1 is the Rap Back Ready population. That's the current focus. This applies to individuals with fingerprints already on file with DCSA. Those are from May 2018 to the present. There's no cost to Industry for this phase. Required action, so Industry partners must distribute two FBI advisement forms to their cleared population informally acknowledge the distribution to DCSA. This initiates the enrollment process.

Phase 2 is Rap Back available population. This applies to personnel who do not have fingerprints with DCSA, but have them on file with the FBI for other purposes, and that goes back from June 2010. There is no cost, and there is no action required from Industry. This phase will begin after Phase 1 is complete, and I will say we are actively working to reciprocally receive any fingerprints that are on file from maybe other agencies or previous positions, we are working to identify that to really try to minimize the impact to Industry and then Phase 3 is everybody else. So this applies to all other personnel who do not have fingerprints on file with either DCSA or the FBI. For the cost piece, we recognize there is a cost. We are working to minimize any costs in evaluating potential avenues for maybe other providers to determine if they can support Industry participants at no direct cost. We recognize the labor costs associated with that, but we are trying to keep it to a minimum. Timeline, we will provide advance notice before this phase begins to allow for budgeting and planning.

All right, and everyone's favorite topic, NBIS. So some general updates. We've successfully released several key updates, these include the eApp cloud migration that happened in December. A single email system for NBIS eApp account activations, Phase 3 of the CVS to DISS migration and a subject reset capability, which went live on January 6th. We want to extend a special thanks to our NISPPAC Industry partners, from the NBIS-DISS sub-working group, who were instrumental in assisting with testing throughout these rollouts. Your dedication was invaluable, and the feedback was crucial. Some updates on specific features and capability rollouts. I know some of you are tracking, we recently rolled out the Individual Engagement Portal, or the IEP. It's a suite of capabilities that support collection of personnel vetting data from individuals, customer service-focused functionalities, and they facilitate interactions between the facility security officer and individuals subject to personnel vetting. This happened very recently, just a couple weeks ago. It provides individuals with direct access to their application status to improve transparency, enhance efficiency, and support Trusted Workforce 2.0 goals. We understand the Industry has some concerns with how this could impact their internal processes, and if they will be made aware of their cleared employees reporting activities. So we will continue to work with you on a potential path forward, and how that will work for Industry going forward. Finally, related to NBIS, Central Verification System, or CVS, to DISS, Joint Verification System Onboarding. The goal is to establish DISS/JVS as the single modernized entry point for all federal agencies and Industry, replacing CVS. This includes a complete migration of all data and agencies from CVS to JVS.

Phase 4. excuse me, up for data migration is expected to be complete by the end of this month, by the end of March. We will begin onboarding federal agencies and ISP agencies into DISS in Q3 of FY26. The good news is for Industry is that you are already established in DISS/JVS and will not need to go through the onboarding process. We will continue to communicate updates to Industry through the NISPPAC.

And then I want to address some questions that we got from Industry directly. We received a question, What is the projected date to communicate to Industry how and when the transition from NBIS to DISS

will happen, when training will be available, and how long will Industry have to make the transition? The delivery date for initiation, review, and authorization capabilities within DISS/JVS is expected in June. The DCSA team is building capabilities within DISS/JVS for testing and early adoption, for Industry to prepare. We have close contact and a great partnership with NISPPAC to ensure this information is properly communicated.

And then the last question from Industry, NBIS engagement and operational roadmap transparency. While communication and engagement regarding NBIS has significantly improved, challenges remain around the visibility of operational plans, timelines, and early involvement for Industry stakeholders and system development. Is there a timeline for an NBIS operational roadmap, including timelines and milestones, so the Industry has time to prepare? We have developed an internal prototype for the operational roadmap that is under internal review this week. Our goal is to share and demo the prototype with NISPPAC before the end of March. And with that, that concludes my remarks, pending any questions.

Michael: There are definitely questions. This time, let's start with our friends who are joining us online. So you did reference the coming FCL handbook and so we had a question about pending guidance there from Doug Cameron. Seems like you, if you address that, we know guidance is coming. He also asked a question, and forgive me, I'm going to paraphrase these because they're quite long, to sort of review and discuss the control protection for marking requirements for DISS information and guidance that all information for DISS should be controlled or protected as CUI concerns about the ability to share based on that marking.

Allyson: I may have to defer to my personnel vetting counterparts and our CUI team. I do not want to speak out of turn. I'll have to take that one back.

Michael: Sure, of course, and all these questions will remain a part of the record. I've got one more for you before we turn to the room, if anyone's got a burning question. Gretchen Alspaugh asked "will there be a community-wide directive to use NI2 for DD254s. Some services use it and others don't, which makes it difficult for Industry."

Allson: Sure. So, speaking from my time up at OUSWI&S, working for Mr. Spinnager, and we have put out lots of guidance memos, it's in policy. I know there is a FAR overhaul that is taking place, has taken place. So some of the language in the FAR, I believe, has been modified, but as far as I'm tracking, it is still a requirement to use the system, and it is a requirement for policy, and like I said, we've put out memos stating the same as well, so that has not changed. We recognize there's been some challenges with getting the system to full implementation, to support our users' needs, so that is an ongoing effort, but, we remain committed to that. People need to be using that system.

Michael: Great. Joseph Whipp asked in the chat, "could you please go into greater detail or readdress comments, about timelines and what candidates can see in eApp? Are they able to see where they are in the process? Can they log back in after their SF86 has been submitted?"

Allyson: I'm sorry, I cannot see who is online. Is anyone online from DCSA, from Trusted Workforce Group, that could potentially answer that, or otherwise, I will take it back. I don't want to put anyone on the spot.

Heather: We'll take it back unless they immediately raise their hand, and then we can't hear them.

Allyson: It seemed like we were having sound issues earlier, so we'll just take it back.

Michael: And any further questions? Thank you very much.

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

Lisa: Hi. I was gonna say good morning, but good afternoon, everyone. So there was a pending question from a prior meeting that ODNI addressed Industry's concerns with hesitance of the intelligence community adopting initiatives to modernize systems, and of course, to eventually adopt the PVQ, aligning with updated investigative standards. The person who had submitted the question said in speaking with individual agency PERSEC leads, there seems to be no feasible intent to modernize. I'm happy to say that we have spoken on TORISs before, but I'll speak on it again today, providing, of course, a status update and of course, address, I think there was a request for, with regard to TORIS, to discuss engagement with Industry and operational roadmap transparency, and of course, timelines. So, ODNI is developing a system known as TORIS, to align with the Trusted Workforce 2.0 strategies, and of course, to address increased demand for expanded transparency between agencies related to personnel mobility. So, the system is known as TORIS, as I said, and it stands for Transparency of Reciprocity Information System. TORIS will aid in the timely exchange of personnel vetting data among IC agencies, and that will enable greater visibility into the information that's needed in order to support the transfer of trust determinations for personnel. TORIS is a system comprised of six main pillars of effort that will improve the efficiency and reliability of sharing this information. I do have limited information to share at this time, since we are in the early stages of TORIS planning and development still, but I will share whatever I do have for now. So the six pillars include trusted workforce information exchange identified as TWIE, and a foundational service that facilitates the exchange of data. And then, of course, we have the IC Personnel Vetting Questionnaire, the PVQ, the one and the same as DCSA's. The PVQ, as you are already aware, is the form that's replacing the, the current personnel vetting standard form, such as SF86 and this will be the same form being launched by DCSA through Embass's eApp. We'll essentially have a copy of eApp on the high side,

and or for those who are engaging with the IC. So this will ensure the easier exchange of the form, right, when a person transitions between the IC and non-IC agencies that happen to use DCSA services. The next pillar is called Passport. So the passport displays the current snapshot of an individual's personnel vetting status for the purpose of completing a security, such as, the transfer of trust between the agencies, as I described earlier. Then Trusted Workforce Records Gateway is another pillar. I don't have any specific details on that right now. The IC Forms/E-interview Engine, this, will be sort of a delivery system, that may submit forms to an individual to complete that are outside of the PVQ, for instance, the SF714, the financial disclosure form that's used for personnel vetting for some individuals. And then the last pillar is people systems integration. For that one, I don't have any specific details, at least not yet. So in the past, we've been asked about engagement with Industry. As we move forward in the planning and development of TORIS, we have already begun such an exchange when the last meeting with NISPPAC reps on the topic was in February, and we did that meeting to gain understanding of the pain points that exist for Industry, so that we may give consideration during planning and development in order to improve on the processes surrounding mobility of contractors within the IC and of course for the implementation of these new systeMs. We look forward to continuing engagement like that, which, took place back in February, so I don't know yet when our capabilities team will be able to meet again, but that's certainly one of the things on our list for a near-future engagement. The timelines associated with TORIS are in the midst of consideration at this time, so I don't have that to share, but hopefully by the time we have our next public meeting, we will have long since been able to share such information. But again, we'll reiterate it at that next meeting, if it has already gone public, but just want to let you know I don't have it to share today.

Let's see...Industry requested a meeting with CSAs to discuss communication options, so they're not surprised by future announcements. ODNI would support meeting CSAs to discuss optimization of communication efforts, to keep Industry informed, and of course, such a matter is important to ODNI, such as in our development of TORIS, engaging NISPPAC representatives to exchange perspectives and gain greater understanding of problems we're trying to solve as it relates to improving mobility of Industry. Again, whatever the other topics are, I know in the past there have been discussions on executive orders or new policies coming out as well. They're just seeking not to be surprised. So starting discussions, within the IC on reciprocity of training for Industry was another topic we were asked to speak on today. The ODNI has begun engagement with training POCs within ODNI and other IC agencies to gain a greater understanding of efforts that may already be underway that will support reducing redundant training time for contractors. An intelligence community directive is in place, which covers the reciprocity of mandatory training, ICD 613. So the policy was intended to increase workforce productivity by eliminating training redundancies while meeting statutory and regulatory training requirements. This policy directed the development of IC core training for derivative classification, Privacy Act, personnel identity information, counterintelligence and insider threat training. The IC agencies are able, of course, to supplement the core content requirements with agency

element-specific training that may inform of such things, as specific agency policies and POCs relevant to training topics, or if within whatever that training is, they provide, like, reporting tools. If the agency has their specific tools, then, right, it would provide that sort of information as well. So where the core content requirements have been met through another IC elements course, the agency-specific course may be taken separately, so satisfying the additional agency-specific training requirement. So clarifying that there would be this core part of the training, and then there'd be this other piece that could be attached to the IC training that somehow you would be able to do that agency-specific piece that's added on. So ODNI would like to engage further with NISPPAC representatives, because I'd really like to gain a perspective of Industry on other training topics they believe could benefit from IC core training development, that I may be able to go back to these groups to recommend to the training POCs involved in the IC core training policies, or those who handle the IC cores training policies and training development. So, maybe we could speak something more on that Friday, if there's an opportunity in the meeting we have coming, with some NISPPAC reps, but if not, we can certainly find another opportunity for engagement.

And then, the last thing I think I was asked to speak on was to provide a status for insider threat policy for covered employees and what's referred to as the overhead billet policy. So the covered insider threat policy has reached, for the most part, final language, but has been caught up in a consideration over the appropriate policy document type, due to the fact that the policy direction as directed, would come from the DNI and her role as DNI, as well as her role as SecEA. So there was a bit of back and forth trying to sort that out between lawyers. Glad to say we have resolved that here internally, and have reached consensus and so the policy is submitted back into the system and in the final stages of consideration before the DNI reviews it for signature. It is my hope that by the next public meeting, I'll be in a position to say that the policy was issued months before, but I do not currently have a specific plan date for its issuance, but again, we are in the last stages.

Then the policy on submitting applications for access to classified information for certain personnel, was drafted and submitted for internal agency coordination as of last summer originally, for which we have steadily worked to progress the policy. So I'm happy to say that all of the cross-coordination is completed within ODNI, and we are in the final stages of consideration before the DNI reviews for signature. I think it's one notch ahead of the other policy, but we're very much near the end of the finish line. All of the disagreements, discussions, and coordination and re-evaluations have all taken place. So hopefully, again, by the next meeting, I'll be able to say months past, we have issued it. And, I think then I'll open it up for questions.

Isaiah: Hi, Lisa, this is Ike.

Lisa: Hi!

Isaiah: Hi! Is there a reason why we gotta wait till September, October, before those approved. Industry is just really not

understanding. I know we had a lot of change with leadership and administration. We're talking 3 plus years that we've been waiting for these policies and Industry companies...they are struggling because, you know, they can't make decisions without proper guidance, and legal gets involved, etc, etc. So...is there a chance we may hear about some good news that it's been approved and out on the streets before September or October? Over.

Lisa: Yes, I feel confident of that. Like I said, we're in the very last stages. I'm saying that by the next meeting, I hope to be able to say months past, we had actually issued it. But I don't have a date to say, like, I can't say the DNI guarantees to have signed it by April 15th. It is in the very last stages. When documents get to that point, right, it's a prioritization of world events and whatever else is happening at the time. So, sort of, a date where we think something might occur might shift based on those priority events that happen.

Isaiah: Okay, thank you.

Lisa: Yes, sir.

Michael: We did have a question in the chat on TORIS, but I think you gave a great explanation of that meets the mail there. Any other questions in the room?

LaToya: Yeah, I actually have a question. This is LaToya with Industry.

Lisa: Hi, LaToya.

LaToya: Hey Lisa. So you mentioned the training reciprocity, and we appreciate the efforts that you guys have made within the IC elements to try to reduce the training hours amongst the IC. But my question for you is, has there been any effort made outside of the IC to incorporate, potential reciprocity with DoD, or, I'm sorry, DoW?

Lisa: I don't have the policy with me, but I do recall the policy, deferred to, at least, like, for specifically, but am I really focus on military members, and I'm sorry, I don't remember the specific details. But that in the instances of that, it would defer to the DoW policy. But I cannot recall off the top of my head what it said with regard to Industry on that topic. So I'll have to dig into that one more and see, but I'm not 100% sure, I'm sorry, because it's not my normal area of expertise, but I will take that back to that group, and I would love to also have more conversations with Industry on, you know, is there other training, that I might take back to them and ask them to consider?

LaToya: Thank you. My second question for you, is regarding TORIS and PVQ. You mentioned that the PVQ is going to be incorporated into TORIS, so it's kind of a two-part question, with question one being are we looking at every agency to be incorporated into TORIS? And what agencies or have all of the IC elements adopted the PVQ?

Lisa: The expectation is that all agencies across the federal government will adopt the PVQ so, I don't see any pushback from that particularly at

this time, but as we put all of that into TORIS and begin to onboard agencies for the use of TORIS, that will become more clear, if there's for any reason pushback but as far as the policies go and the requirements go, the PVQ should be adopted, the PVQ that's being developed for EAP.

LaToya: The IC elements are...you're saying, yes, that the IC elements are adopting the PVQ for use?

Lisa: No, I'm saying that's what the policy requirement is.

LaToya: Which it's very different, because I'm asking that question because we've experienced in Industry where that has not been the case. It was not used across all the agencies, so I wanted to make sure that I was, clear on that question so that Industry understands what to expect, as it pertains to what could happen with the PBQ. Thank you so much.

Lisa: Yeah. Thank you, ma'am. We have been having discussions with the IC agencies. I don't know where everyone is at 100% on all of those, but we, certainly, I think it's been more an education piece for the agencies to understand what will be the PVQ and TORIS, just as it is the same, right, for Industry. Everyone's learning, and we're also, of course, in the process of planning and developing. So much like with Industry, right, we're trying to find out what pain points are, what problems can we solve as we move forward, so that we're just not, you know, designing it on what we think would work. So the same is so for the IC agencies. So as we continue, you know, I feel confident everyone will be in a position to adopt it. You know, how long that process will be, I don't know yet.

LaToya: Thank you, Lisa.

Lisa: Thank you.

Jennie: Lisa, this is Jennie Hardy, Industry. A question about TORIS, and first of all, thank you for your engagement with us on the NISPPAC thus far. We are excited to continue to move forward with you. With regard to the ICs, has there been engagement with the ICs, as there has been engagement with Industry in the discussions about the development of TORIS?

Lisa: Yes.

Michael: Straight to the point, right?

Lisa: Sorry. Yes, we've had those discussions.

Michael: She should be a politician.

Jennie: Is it all of the ICs? Or is only some and not others? Because the concern from Industry is if this is going to be used as the system that's like shared services. We would want to see, ideally, adoption by all, which is tough and not having adoption or buy-in by all would

be...would be difficult working with disjointed systems and forms and processes.

Lisa: Yeah, so there are some smaller elements of the IC, is that maybe what you're thinking?

Michael: All right, Lisa, thanks very much, and thanks, everyone, for your question.

Lisa: Okay, thank you.

Heather: Next, we'll hear from Ms. Jamie Gordon with Program Planning and Management in the Office of Security with the Department of Energy, who will be providing their update. Jamie?

Jaime: Hi, how are you guys doing today? Can you actually hear me? I tried to speak up earlier during roll call, but it wouldn't go through.

Heather: Yes, we can hear you, thank you.

Jaime: Okay, great, thank you. So, hello, everyone. It is good to be here today. The DOE was asked to speak to solid state drive sanitization procedures. We do have procedures for various types of sanitation scenarios, and we are willing to work with any Industry partner to ensure appropriate procedures are followed based on the type of contamination and or sanitization. So, if there are specific questions, please get those to us so we can get that specific information to you on how to provide that, just to do those procedures.

As for CUI, and as stated earlier, NARA has just sent out new information regarding updates to the CUI processes, so due to the continued unique requirements for certain types of CUI that really do make standardization difficult, and the fact that these new updates have come out, DOE is going to have to review these updates and provide additional guidance through the NISPPAC as we move forward on this. And that is it for the DOE updates, unless there's any questions.

Michael: Any questions for our colleagues at DOE? Alright, thank you very much for the update.

Jaime: Thank you very much.

Heather: Thanks, Jamie. We're now going to take a 30 minute break. NISPPAC members and speakers can make their way to the green room behind the stage for some light refreshments, and we'll be back in 30 minutes. Thank you.

Heather: 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 NHSA Working Group, which took place on January 14, 2026, and the Clearance Working Group, which took place on January 21st, 2026. We will also hear from the Department of Energy for their security clearance metrics, along with DCSA for their information systems

and personnel security metrics. As a reminder, DHS and NRC security clearance metrics are located at the end of the slide deck that was emailed to all registrants and online. We are now going to hear from Ms. Monica Marks, Director of the Office of Departmental Vetting and Assistance within the Office of Environment, Health, Safety, and Security at the Department of Energy will be providing their metrics. Monica? Monica, we can't hear you if you're speaking.

Jaime: Hi, this is Jamie. I'm gonna go ahead and cover down on Monica's briefing. She's having problems getting her mic to work.

Heather: Great, thank you, Jamie.

Jaime: So, let me make sure I've got these pulled up. Do we have slides, or no?

Heather: We do not.

Jaime: We do not? Okay. So, I'll just go ahead and go through this. The quarterly DOE timelines for the average days for the fastest 90% of the reporting clearances decisions made for last, fiscal year, for quarter...first quarter is, for Top Secret, we had roughly about 4 days to initiate, about 108 days to investigate, and around 29 days to adjudicate. For secret, we had around 6 days for initiating, 71 days for investigating, and 16 days for adjudicating. For top secret PRs. We did take a little bit longer for the adjudication period, simply because they're periodic reinvestigations, and we go through continuous vetting, so it takes longer for the adjudication period, but it averaged around 19 days for initiation...I'm sorry, 184 days for investigations, and around 150 days for adjudication. And for secret PRs, it was roughly around 13 days for initiation, 109 days for investigation, and about 172 for adjudication. We did average around 2700, for top secret investigations, 410 for secret investigations, 44 for top secret PRs, and 6 for secret PRs. To break those down into the actual individual, months, between November and December, we had roughly 1800 to 1900 investigations, and those were averaging about 1 or 2 days to initiate around 114 investigations. December was a little bit faster, I think, because we had so many less, around 96 days to investigate. And in November, we had 26 days for investigation and 16 days for adjudication. So, for T3s, it was actually a lot faster. We had around 6 days for investigations, to initiate in November, and we had around 5 days to initiate in December, roughly 69 days in November for investigation and 17 days for adjudication, and September was 73 for investigation and 17 for adjudication. For PRs, obviously, again, the adjudication investigation days were a little bit longer, so for the T5Rs, November, we had about 5 days for initiation, 155 days for investigation, and 164 days for adjudication and in December, we had roughly 21 days to initiate, 171 days to investigate, and 195 days for adjudication. And lastly, we had our T3Rs, which we really didn't have any that we initiated or did any in December, but in November, we had about 4 days to initiate, 90 days to investigate, and 91 days to adjudicate. So the majority of the last quarter was roughly...I think that the longest we took to adjudicate or do the entire process was 387 days for a couple. Other than that, we've been managing to get most of our investigations done within 300 to 150

days... or something like that, so. Are there any questions for me, regarding stats?

Michael: Any questions here in the room? We have a couple in the chat.

All right, we have a couple for you here. Wendy Bowie in the chat asks if you can define what initiate means? Is that the point that things are initiated after the e-app is transmitted through NBIS?

Jaime: Correct. It takes that long to get through that particular system.

Michael: Got it. Okay, great, thank you. And then Greg Pannoni asks in chat, if DOE is routinely conducting PR investigations.

Jaime: Not routinely, no, that it's all dependent on, continuous vetting. So, if there is any information that comes up that's questionable, then we will be conducting the PRs for that, but it just basically is based on the continuous vetting, not through routine PRs.

Michael: Any further questions?

Heather: We do have one more. Dean Miller asked if we could get those stats in writing or provide a URL to where we can find those stats. I will include the slides in the minutes, at the report for the committee page for the NISPPAC, it will be there within 90 days. And, Dean, if you want to send me an email, I can send them to you once the meeting concludes.

Jaime: Thank you, Heather.

Michael: And LaToya?

LaToya: I have a question. This is Latoya Coleman, Industry. I wanted to ask, related to what you just said, you, you mentioned that you are only doing an update when there is a CV alert that triggers an update? Is that what...just for clarity?

Jaime: Yes, that is what I have been told. I will verify that with our personnel security individuals to make sure that I'm not answering that inaccurately, but yes, it's through the continuous vetting process.

LaToya: Okay, yeah, if we could get clarity on that, that would be great. Thank you.

Michael: I think you should go with Latoya Industries, pretty solid.

Heather: Alright.

Michael: Thank you very much.

Heather: We're now going to hear from Mr. William Vaughn, the Deputy for the NISP Cyber Security Office at DCSA. William?

William: All right, good afternoon, and thank you all for the opportunity to provide an update of the cybersecurity activities of the National Industrial Security Program Cybersecurity Office, and for the continued partnership between government and Industry represented here today. As many of you in this room know, the defense industrial base is more digitally interconnected than at any point in history. Classified information systems now operate across complex enterprise networks, cloud environments, and globally distributed supply chains. So this evolution has expanded capability across the industrial base, but has also increased the need for strong, consistent cybersecurity oversight across the NISP. So the mission of our office is to ensure that the classified information systems supporting national defense remain secure, resilient, and capable of operating in today's evolving threat environment. So this morning, or this afternoon, I'll briefly address three areas. First, the current cybersecurity environment within the NISP. Second, several key initiatives that are currently underway. And finally, the direction we are heading as we continue modernizing cybersecurity oversight across the DIB. Now, the NISP currently supports approximately 4,550 classified information systeMs. Now, that is a great reduction, from what you're probably used to hearing, which normally is about 5,000 to 6,000 systeMs. And the reason for that is with the partnership with the Defense Industrial Base, we were able to go into eMASS and eradicate duplicate entries and things of that nature. So, we have it now down to what we believe is the accurate count. So, it's 4,550 classified information systeMs. So, great work on the part of Leonard Moss and the NISA Working Group helping us with these efforts. These systems represent a critical component of the nation's defense technology ecosystem and support missions across the defense and intelligence community. So thus far, in fiscal year 2026, we have authorized 548 systems, with 66 processed as of yesterday. During this time, we also had 119 authorizations that required extensions, including 10 this month, to ensure that we have continual operation. So, there will be times that if we as an agency are unable to get to a specific site, we do not want to hamper your operation, so we have the authority to grant extensions, so we've done that to make sure that we don't have any interruptions. Across the enterprise, the average time required for DCSA to complete the assessment authorization workflow currently stands at 64 days, which is well below our mandated 90-day timeframe. And again, this only includes once we have the appropriate package, right, everything is straight, and now that we have it, it's not returned back to the Defense Industrial Base. So, on average, we're turning those in 64 days. All right, now for initiative number one, our eMASS modernization and Rarefied transition. So, one of the most significant events currently underway is the modernization of eMASS, which supports our enterprise authorization activities across the NISP. So, earlier this year, we deployed 5.14, which was a high-impact release that introduced significant updates to the platform, including improvements to the authorization workflows and enhancements to the plan of action and milestones. Now, this week, to address some minor issues identified during that deployment, we fielded a low-impact follow-up called 5.14-1, and of course, the notes for those updates can be found, when you log into the eMASS website. So, looking ahead, the next major HIPAC in release is going to be version 5.15, which is currently expected at the end of April. This release is going to introduce several enhancements to the platform, including improved

workflow management, stronger controls for POA&Ms and other NISP security controls, and this is in coordination with the NISA Working Group. These updates also support the transition to the Rev 5, which current planning targets full implementation. And the good news story here is that we were able to complete all the overlays early last week. So, what that means, for everyone is this: Now that we have completed our requirements for DISA, now DISA can start working on the actual implementation in the software. It's to note that, unfortunately, we are limited in the amount of updates that we can do in the fiscal year due to contractual obligations. But another thing is, a good news story is that we were able to negotiate with DISA a reciprocity agreement, which means that if anyone else who uses the eMASS system has had that type of release that we're looking to implement, we can have reciprocity, which means that that doesn't count against our contract requirements for the number of things that we can implement in that particular year.

Second initiative is the Cyber Operational Readiness Assessments, also known as the CORA. So these CORA assessments provide direct evaluation of the cybersecurity posture across classified SIPRNet circuits and support broader department priorities to strengthen the security of the DoDIN included implementations of zero trust principles and outlined in Executive Order 14028, which is improving the nation's security.

So, a key aspect of operational readiness is also having a clear, approved plan for incidents like data spillage. So, I was asked to address that, so I will now. So, to that end, it's important to note that the sanitization for spillage must be approved as part of your incident response plan. So the data owner provides approval and concurrence of allowable methods in accordance with CNSSI 1001, Section 4-8, if the customer requires destruction, then follow NSA provided guidance. The data owner customer may allow mitigation or accept risk within the spillage cleanup procedures.

The fiscal year 2026 CORA Assessment Schedule has been released. It is located on the DCDC portal. DCDC is the Department of War Cyber Defense Command, and the execution is currently underway, so to ensure appropriate risk visibility across the enterprise, all circuits that have not been previously, achieved a moderate, low, or very low risk will receive a priority for inspection during this fiscal year. So what that means is everybody who has not passed a CORA in the last two years, you will get inspected before this fiscal year ends. Currently, we are approximately halfway against our annual business plan goal.

And the third initiative is the ISSP Training Academy, which is the Information Systems Security Professional Training Academy. This academy is designed to strengthen the capabilities of personnel responsible for cybersecurity oversight across the classified systems supporting the DIB. So, we released Phase 1, which established the foundational training through an e-learning platform to support personnel across the enterprise. Phase 2 will expand the academy through instruction and practical coursework focused on consistency, technical proficiency, and standardized execution in cybersecurity oversight activities and this is one of the things that we're doing to address the findings of the MITRE FAST study. So, as of last week, our office recently approved the

curriculum, so all the curriculum that, was going to teach the people, that is done, so now we are entering the same thing as the eMASS, we're in the design phase, so we're waiting on the vendor to put all their updates inside the e-learning platform. So, I will have updates, in the tentative IMS, for the NISA Working Group during the next quarter, for both the ISSP Training Academy and the eMASS.

So, for the future, as we look ahead, the cybersecurity mission supporting the NISP will continue to focus on strengthening protection of classified systems while enabling the speed of innovation required across the DIB. Recent analysis, including the findings for the MITRE FAST study on acquisition security transformation, reinforces the importance of modernizing cybersecurity oversight to better align with today's digital operating environment. Our goal is to ensure that cybersecurity within the NISP continues ivolving to protect national security and it's important to remember where our office sits in the grand scheme of things. So, we are, most often, the assessment and authorization arm of higher-level entities, right? So if your facility is involved in classified information as a service, Golden Dome, or Expedited SIPRNet circuits, understand that the requirements for I&S, the CIO Office, the CISO, DCDC, and DISA must first be met before DCSA can engage. So, once those requirements are met, my office and Mr. Scott, we stand ready to support the authorization assessment processes. So, through continued monetization, operational oversight and strong partnership with government and Industry, we remain focused on ensuring that the NISP continues to protect the nation's most sensitive information while supporting the innovation and capability delivered by the DIB. So, standing by for your questions.

Michael: Thank you so much. Questions here in the room? Great, I think we're all clear. All clear on the chat as well. All right. Perfect reefing rules. Got it.

Heather: Thank you, William. We're now going to hear from Ms. Donna McCloud, the Senior Policy Advisor for Personnel Security with DCSA. Donna?

Donna: Thank you. I am here this afternoon to give the metrics update on behalf of personal vetting, and that will include investigation and adjudication. So our metrics as of February 21st, 2026, our investigation, our inventory is 104,000 cases, which is a decrease of 7,000 cases, or 40% during FY26 and this total of investigative work, the 104,000 I mentioned, includes everything for investigation, to include initial, CV, and the issue resolution that we do for CV.

For the DoW industrial community, the investigation inventory for tiered cases stand at 13.5K cases, marking a decrease of over 10,000 cases, or 43% for the FY and a 20% decrease over the past 12 months and, also to further break that down for Industry, that gives us about 4.9K in the Tier 5 investigations, and 8.6K for our Tier 3 investigations.

And so, as I had mentioned before, in different working groups and engagements within Industry, we've reported on the various inventory reduction, operational changes that we made to help draw down the

investigation inventory. We talked about the collaboration that we've done with the FBI to reduce the name check backlog, implementation of some of the Trusted Workforce 2.0 standards that we're able to decrease some of the times that we did for investigation, and also expand and expedited review of investigation. All of that helped to draw down the investigation. The timeliness for Industry, our T5 timeliness for FY26, Q1, 19 days for initiation, 140 days for investigation, and 68 days for adjudication, which comes to a total of 227 days total end-to-end. For T3 initials for FY26, Q1, 19 days for initiation, 71 days for investigation, and 66 days for adjudication, which is a total of 156 days total end-to-end. So as I talk about the decrease in what's happening on the investigation side. That means, on our adjudication side, the inventory is just increasing. So that's the reason for the increase in adjudication, because we're drawing down the investigation inventory. So, as of February 21, adjudication inventory for T5, 3,000 cases for T5s and 9,000 for T3s. So, again, trust decision has experienced an increased trust decision the adjudication. We have experienced an increase in due to the focus of the AHCBs, CV investigations that they're doing, incident reports, and closed and tiered investigation inventory. So all these actions caused the increase in what we see for adjudication. So our trust decision is working through an initiative to draw down the inventory, to quickly close new cases, not requiring additional issue resolution and anticipates a significant impact on timeliness next quarter. We appreciate everyone's patience as we work through the historical highs in the inventory due to many initiatives within Personnel Vetting. And, any questions about the metrics?

Michael: I feel good about it. Any questions from the audience?

Donna: And one thing I wanted to follow up with, there was a question early on about the individual engagement portal and what does it look like? I was able to phone a friend and get some information on that, because I had not seen it myself and so I actually have a visual of what they look like. I can't show it now, but I was told that this information is shared through the NISPPAC, and there is a fact sheet that goes along with this, so we will make sure that our liaison communicate with NISPPAC and give you that information.

Michael: Okay, great, thank you. And we have, do have one question from the chat. You know, Greg Pannoni can't leave us without a...so I'm gonna, I'm gonna do his question justice here. Recently, I saw an article indicating that the latest Trusted Workforce 2.0 quarterly Progress Report was released and indicated inter alia that reform efforts would tackle updating meaningful performance metrics. One of those was a metric for rejection metrics. With that in mind, will DCSA begin reporting on PCL applicant rejection rates?

Donna: So, what I will say is I do not know the exact answer to that, and I don't want to misstate it, but I will say that what DCSA will report on what the metrics are required per trusted workforce investigator standards, and what we need to do for Trusted Workforce, but we can go back and see exactly what it has, if anything is in there for that.

Michael: Great. Thank you very much.

Donna: Thank you.

Allyson: If I may, so don't get scared, Donna. I don't have a question. I just want to say something. For those of you who don't know, this is Donna's last NISPPAC. She is retiring in July. So, just want to say thank you, Donna.

Isaiah: Since you have been a great partner to Industry NISPPAC, so you've been a great partner to everybody, but on behalf of Industry NISPPAC, we would like to give you our Industry NISPPAC Challenge Coin.

Donna: Oh, thank you, appreciate it.

Heather: Thank you Donna. It's really been fantastic working with you. Good luck to you in retirement. We're now going to hear from Mr. Perry Russell Hunter, the Director of Defense Office of Hearings and Appeals. Perry, please come on up.

Perry: Thank you. Good afternoon. Michael, Heather, NISPPAC members, public. I want to thank you for the opportunity to be here. The Defense Office of Hearings and Appeals plays an important role, albeit a small one, because...you may not realize this, but 98% of clearance applications or reinvestigations result in a favorable determination. So, the number of rejections, Greg, if you're listening, is relatively small. And it's always been relatively small, and it always will be relatively small, but getting to those is the important work. And so...I want to start out by saying that DOHA, if you don't know, is independent of DCSA. We report to the General Counsel of the Department of War and we provide consistent and a transparent process that allows individuals to be heard in Industry, to be heard before denial or revocation can take place. Now, in some very rare instances, there may be suspensions of eligibility, but the overwhelming majority of folks who appear before DOHA are getting their day in court before a denial or revocation, not after. And that's really important. In fact, it's so important that with the 2024 NDAA, Congress, at least the Senate side, indicated that they thought that those protections should be available to service members and civilians within the department. And, while that did not make it into law, what did make it into law was a conference report that said that we in the department should be striving to give service members and civilians the protections that you all in Industry have enjoyed for 65 years now. And so we're working on that. In fact, Jeff said something really poignant, to me at least. Jeff has a way with words. But he said something this morning about the accountability of being on the record. Well, I know he was talking about the NISPPAC, and this public meeting forum that's so important to hold all of us accountable, but it also applies to what we do at DOHA because we hold on the record proceedings. So there's no guesswork as to what has happened. We call witnesses, and they're subject to cross-examination and confrontation. That's something that President Eisenhower was wise enough to realize was warranted for Industry back in 1960. And that followed a number of unfair hearings that had happened in the period between 1947 and 1959, which the Supreme Court, in a case called Green v. McElroy, put an end

to. If you saw the movie Oppenheimer, you probably saw a sample of what those 1947 to 1959 hearings looked like. Individuals maybe could have a lawyer, maybe not. They could have a lawyer, the lawyer wasn't allowed to speak, they didn't get a chance to see the evidence against them. All that changed for Industry, thanks to President Eisenhower and all of that is, I think, about to change for service members and civilians, and I'm very proud of that as well. Now, that being said, you're probably wondering how we're doing. So DOHA is timely on our legal reviews, of the statements of reasons that go out to members of Industry whose clearances are being challenged. Now, why does that matter? Well, it matters because the statement of reasons is the initial step, it's the initial procedural protection for a cleared contractor. And so, the idea that we want to make sure that, before we make somebody worry about losing their job, we're going to make sure that we have it right. We have it right factually, and that we have it right legally and so, I'm happy to report that 95% of our statements of reasons legal reviews are being done in under 45 days. And that's important because it means that, you all in Industry, know where you stand at the earliest possible moment. We reviewed, in the past calendar year, over 1,100 statements of reasons, 1,024 to be exact. And, among those numbers, we actually rejected 90 that were either factually wrong or legally wrong. So that there's, when you talk about accountability, accountability at DOHA works both ways. We hold the individual accountable, but we also hold the stages in government before us accountable and that matters as well. So, with that said, I've already mentioned a Supreme Court case that turns out to be very important to this process. There is, of course, another pair that are more recent, the Lucia case and the Arthrex case. The Lucia case, Lucia v. Securities and Exchange Commission, the Supreme Court said that if you're going to be making important decisions that affect the public, you need to be appointed by the agency head. So, while that wasn't clear, it applied to DOHA administrative judges and the clearance process. Along came a case a few years later, the Arthrex case, and the Arthrex decision made it abundantly clear that if we're making these kinds of decisions, especially after the issuance of the Statement of Reasons, that the individual needs to be appointed. And so, all of the DOHA administrative judges that decide cases involving Industry contractors have been appointed by the Secretary of War. So that is, an important protection because there is, not just public accountability, but political accountability as well. Now, that being said, I have enjoyed the independence of a career working with the Defense Office of Hearings and Appeals, where if someone tries to influence a case, I have one thing to say to them. We're holding a hearing. You're welcome to come testify. That's what fairness really looks like. So, Jeff, I want to thank you, because when I came up here, when I first came to this meeting, I had some other ways of trying to describe what DOHA does, but the accountability of being on the record is probably better than anything I could have thought of, so, thank you and, Michael, Heather, thank you very much for letting me be here. I will take any questions. Oh, oh, wait, one more. If you might think of a question later...My number is 703-696-4751. It rings on my desk. I answer it. Please feel free to call.

Isaiah: He really does. He does.

Jeff: Perry, when you first came to this meeting, your hair was brown. Accountable, right? Yeah.

Michael: So, if anyone has any questions that they would like to dial Perry directly on, you're welcomed to.

Perry: Thank you. By the way, I just want to say kudos to Heather. Heather runs a great meeting. During the break, she saw that I was sitting way up, way back there. She's interested in time, she goes, no, sit right there, so...

Michael: Thank you very much. Well, in the spirit of kudos, we're getting close to the end here, but I want to take some time to thank Heather, of course, who you all know well, all of our participants here on stage in the room, our amazing AV team at NARA that has helped this video go flawlessly, including...and also, Kristen, our voice from above, who's ushered people in the chat has been doing all sorts of things behind the scenes that you're not seeing. You may have interacted with one of three remarkable young women who have joined us here at ISOO for their semester in Washington, or grad school program, so we're really lucky to have Ana, Uma, and Bariha here supporting us. They are all of a generation that is mortified by public attendance. With that said, with the kudos out of the way, this is the window of time we've addressed all of our old business. And now is the time for any NISPPAC members may choose to present any new business, unresolved grievances, or other matters before we separate for the day. Does anybody have any final new business they'd like to propose?

Isaiah: So, I have one go back. Yes, sir. Yes, sir. This is to Jeff, Mr. Spinninger for VOW. It's in regards to NCCS and NI2. So, Jeff, where Industry's probably kind of afraid if you don't implement an end date to agencies with that, we're gonna always have some challenges. So, not to put you on the spot, but we're kind of looking for you to kind of put an end date.

Jeff: Yeah, so, well, thank you for that, right? So, there's a couple things that are happening at the same time, right? One of which is we're sort of addressing an issue that's been in play for a long time, right? Said more directly, the FAR has been around for a while in terms of what this requirement looks like and to be very frank, the department, and we'll just say at the department level, has been a little bit inconsistent as it relates to the system side of this thing, right? So, laying the case for and then creating a requirement for the system piece of this was done a long time ago, and we've kind of had the hew and cry, which is, you know, I think something that we have to be able to acknowledge and so right now, what that brings us to is, as we have been beating the drum, you know, in two different camps here. One, the security aspects of the underlying form, right? For sure. But the fact that it's an acquisition requirement is a part of the equation. And let me be very blunt about that, right? So across 46 Department of War components, right, there are 46 different ways in which the department organizes acquisitions and security requirements. Some of them are a little bit more straightforward, and we've seen some real progress there. Some of them aren't, right? Inside the department, we also had a bit of

an uneven requirements process, and where people then said, hey, based on uneven, you know, requirements, or my requirement didn't get in there, or whatever else, we're just gonna pick our marbles and go home until we get those right. And that describes a couple years of the issue. So for all of that time, right, we've been able to speak up through what we call the Defense Security Enterprise, and, you know, present here now. So, Latoya Industry, briefed it earlier, right? So, you know, mentioned it, right, through our governance, have lifted this up, but we've done the same thing on the acquisition side of this thing. So, we're still under the phase of that which gets measured, gets attention and so we've been measuring what the usage and the performance metrics look like as a function of users, right? Still hold now a little bit where DCSA is concerned so that they can be able to showcase what they use the data for, right? That remains a little bit aspirational at this moment, to be very frank because that brings us right back to the very first part of the equation, which is we're back to having a systems challenge again, right? We had a bunch of things, and life, and some other stuff. Right? We had all kinds of hue and cry, because while the FAR was changed, Allyson, I appreciate mentioning this, right, it was reordered, none of the words changed, right? So this created a bunch of panic, and so we kind of needed to kind of quell all of that. But at this stage of the game, where we find ourselves, is we need to give a little bit of runway to our partners at DCSA because there is a big systems component of this, and kind of borrowed from what you mentioned earlier, making sure that Industry is as much a participant as that as possible. I think is where we find ourselves today, because I think...I don't know this yet, but I think most of the contracts that are awarded where classified performance are required are subcontracts, right? So making sure that that interchange can happen when it's kind of, frankly, Industry direct to the system is something that I'm not sure we've paid much attention to, and all of the banging on the doors across the acquisition side or the security side of the department don't address that. So I think that's where we find ourselves right now. It's rolled up into the larger constructs and conversations related to NI2 and we're gonna give a little bit of space for that. There's a lot going on there. So, what I'd ask for is the continued attention of this body, right, put it number 2 below, whatever we were talking about earlier, a couple things, and then let's keep looking at this through the working groups over the course of the next several months, because I think you're going to see some...on the program management side of DCSA, some real, I'll call them points on the board, that we'll be able to then give greater fidelity to your question, which has basically been unchanged for a long time. Nothing else will move us a little bit further down.

Isaiah: Thank you,

Jeff: Sir.

Isaiah: And then last, I want to give a kudos to ODNI. From a SEAD 4 perspective. I'm not sure if any of you know, but SEAD 4 is in the revision stage right now, and Industry NISPPAC is a player in that, so we wanted to ensure that we highlighted that partnership between ODNI and Industry NISPPAC in regards to being involved early and often when it comes to SEAD 4. So, thank you.

Jennie: Ike, I have one go back on...on the NI2. We would ask that there be an emphasis on prioritization of training of the system, so Industry finds that those who are in the system, working with customers who are new to use the system, there's confusion on both sides with...with how to use it, and Particularly now that it's transitioned into the DD254 workflow within NI2, a lot of things have been simplified, and we would ask that that training be, either revised or reissued to those groups, so they can better...they'll use it if they understand it.

Jeff: That's a great point. Thank you for that.

Michael: Thank you so much. Two other notes, I want to make from...a couple notes I want to make from the chat before we adjourn. First, if we didn't get your questions. I'm sorry, did I cut somebody? Oh, thanks. Sorry, is that better? Hello, everyone. From the chat, if there are questions that we didn't address directly, we certainly have captured those, and we'll look to provide responses. Some folks had some thorough multi-part questions that are just not practical to address in a meeting like this one. We also had a couple of submissions relating to CUI. I want to acknowledge that those came in. Again, they were multi-part, some including documents and attachments. So...we'll take those on board, we'll take a look at them, but they're not things that we can address in the body of the meeting. The other thing that's blowing up the chat are congratulations for Donna, and that seems like a really good note to end on.

As a reminder, our future NISPPAC meetings will be listed in the Federal Register 30 days in advance, as well as posted on the ISOO website. Our next meeting is scheduled right now for September 2nd, barring...what could happen? What could happen? And, last thing I'd like to do is take the privilege to thank my entire ISOO staff, many of whom you haven't seen, but have been supporting our work today, including Carolina and Larry, along with Heather. So thank you very much, gang, for making this possible. We're a small but mighty team, and we do our best to support you. Thank you all for your participation and support of this process. And with that, we're adjourned.