Event Producer: Welcome and thank you for joining today's State, Local, Tribal, and Private Sector Policy Advisory Committee meeting, also known as the SLTPS-PAC. To receive all pertinent information about upcoming SLTPS-PAC meetings, please subscribe to the Information Security Oversight Office's Overview Blog at https://www.isoo-overview.blogs.archives.gov or by going to the Federal Register. All available meeting materials have been emailed to all registrants. While this is primarily an audio conference, you're welcome to join Webex with the link provided with your registration. If you have connected through Webex, please ensure you've opened the participant and chat panels by using the associated icons located at the bottom of your screen. If you require technical assistance, please send a private chat message to the event producer. Please note all audio connections are currently muted with the exception of SLTPS-PAC members, speakers, and ISOO. If you are not a member of the SLTPS-PAC and would like to ask a question or make a comment, please hit #2 to raise your hand. If your audio is through Webex today, you may click the hand icon at the bottom of your screen, or send your question to all panelists through chat. Another option is to email your questions and comments to SLTPS_PAC@nara.gov, and someone will answer your questions there. For our SLTPS-PAC members, please mute all audio connections when you're not speaking. This is a public meeting. Like previous SLTPS-PAC meetings, this will be recorded. This recording along with the transcript and minutes will be available within 90 days https://www.archives.gov/isoo/oversight-groups/sltps-pac/committee.html. Let me now turn things over to Mr. Bill Fischer, the Acting Director of ISOO, as well as the Acting Chairman of the SLTPS-PAC.

William Fischer: Good morning, everyone. Welcome to the 28th meeting of the SLTPS-PAC. I'm Bill Fischer, the Acting Director of ISOO. I'm the Director of the National Declassification Center at the National Archives in my permanent position. At this time, I do not have any news to share about when a permanent director of ISOO will be coming on board. I will now turn it over to my Designated Federal Officer, Heather Harris Pagán.

Heather Harris Pagán: Thank you Sir. I'll now begin attendance. We already know that Mr. Fischer is on the call. SLTPS-PAC Vice Chairman Richard McComb?

Richard McComb: Yes, Heather, I'm here.

Heather: Thank you Sir. Department of Energy member Natasha Sumter? DOE's alternate Tracy Kindle? DOE's other alternate Jamie Gordon?

Natasha Sumter: Good morning Heather. This is Natasha.

Heather: I'm sorry, who was that?

Natasha: Natasha just joined.

Heather: Okay, is Jamie Gordon?

Jaime Gordon: This is Jaime.

Heather: Thank you. Nuclear Regulatory Commission member Tara Inverso?

Tara Inverso: I'm here. Thank you.

Heather: Thank you. Department of Transportation member Sidonie Dunham?

Sidonie Dunham: I'm here. Thank you.

Heather: Thank you. Department of Defense member Michael Russo?

Michael Russo: Good morning Heather. Present.

Heather: Thank you Sir. Office of the Director of National Intelligence member Lisa Perez?

Lisa Perez: Good morning. I'm present.

Heather: Thank you. Central Intelligence Agency member Don?

Don: I'm here. Thanks.

Heather: Thank you. CIA's alternate Abby?

Abby: I'm here. Thank you.

Heather: Thank you. Federal Bureau of Investigations member Jacob Zockert? FBI's alternate Scott Gerlach? Department of State member Katherine Connor?

Katherine Connor: Good morning. I'm here.

Heather: Thank you. State's alternate Durrell Hicks? Department of Justice member Glenn Bensley? Defense Counterintelligence and Security Agency member Derrick Broussard? DCSA's alternate Scott Cronin?

Scott Cronin: I'm present. Thank you.

Heather: Thank you Sir. Cybersecurity and Infrastructure Security Agency member Nitin Natarajan? Vice Chair Cameron Burks?

Cameron Burks: I'm here, Heather. Thanks.

Heather: Thank you Sir. Private Sector member Jeffrey Imsdahl? State Mountain Region member Kevin Klein?

Kevin Klein: I'm here. Thank you.

Heather: Thank you Sir. State Mountain Region member Chris Palmer?

Chris Palmer: Present.

Heather: Thank you Sir. Speaker Kevin Dillon?

Kevin Dillon: Present.

Heather: Thank you Sir. We request that everyone identify themselves by name and agency if applicable before speaking each time for the record. I want to remind government membership of the requirement to annually file a fI&Ancial disclosure report with the National Archives and Records Administration's Office of General Counsel. The same form of fI&Ancial disclosure that is used throughout the federal government, OGE Form 450, satisfies the reporting requirements. If you have any questions, let us know.

We have had a few changes to the PAC membership since the last meeting. The alternate designated federal officer, Robert Tringali, has retired. Darryl Parsons with the Nuclear Regulatory Commission has also retired. His replacement has not yet been designated in writing. Additionally, Cameron Burke was voted the vice chair among the SLTPS entities we have. We still have eight out of 12 slots that are open for membership among the SLTPS entities. If you have any nomI&Ations, please bring them to our attention. For those departed members, thank you all for the contributions over the years. We look forward to continuing the work you have done with the new representatives.

The minutes from the last meeting were fI&Alized and posted to the ISOO website on March 5, 2024. I will now address the items of interest from the February 21, 2024 SLTPS-PAC public meeting. After a complete review by DHS, it was identified that DHS's Office of Intelligence and Analysis, I&A, had enrolled cases awaiting the personnel clearance process in support of their mission, which is intelligence sharing capabilities with state and local partners. The origI&Al I&A SLTPS backlog was 215. They are now down to less than 100.

Additionally, Lee Watson from the Forge Institute posed questions regarding ODNI's role in facilitating high-side discussions and collaboration in the field. Lisa Perez from ODNI engaged with Lee, promising to engage with the appropriate ODNI office for further investigations into the standardization practices. After engaging with the appropriate ODNI office, Lisa reached out to Lee for further details. Lee expressed intent to further engage when in the area next. No specific dates are planned at this time, and it will remain open.

Does anyone have any questions? Candice, is there anyone in the queue with questions?

Event Producer: Not at this time, but as a reminder, you can press #2 on your phone to raise your hand, and if your audio is only through WebEx, you can click the hand icon at the bottom of your screen.

Heather: Thank you.

Event Producer: There is no one in queue at this time.

Heather: Thank you. At this time, we would now like to hear from the Executive Agent for the program, the Department of Homeland Security. Mr. McComb?

Rich: Good morning Heather and everyone. Just a couple of comments from me before I turn it over to Mr. Juan Estrada to give everyone here an update on the ongoings here in DHS with regard to our SLTPS program, but I would like to echo Heather's comments regarding membership from our SLTP partners. Please do let Heather know, or myself, or Mr. Estrada. We are certainly interested in filling the vacancies that we currently have on the

PAC here, so please let us know that, and we'll be happy to accommodate and let you know how that process works and walk you through that. I also would like to offer my congratulations and thanks to Mr. Burks in his new role as the SLTPS Vice Chair, so welcome aboard, Cameron.

Cameron: Thank you.

Rich: And then I would like to add, as Heather mentioned, working with the intelligence analysis partners over here in DHS and with our headquarters support staff, we're able to actually now have that backlog down to around 20 on pending clearances for action, so making good progress there. With that, I'd love to turn it over to Mr. Juan Estrada to walk through some details for the PAC here today. Juan?

Juan Estrada: Good morning, everybody. Again, this is Juan Estrada, DHS OCSO. I'm the Branch Chief of the SLTPS Management and Oversight Branch with the Compliance Standard and Training Division. As we do at most of these SLTPS meetings, we provide the group with a couple of details and statistics as far as clearances and inspections that our office completes each year.

So, as of now, DHS has approximately 7,800 SLTPS personnel with DHS-sponsored security clearances. 90% of this population have a secret clearance, and the remaining 10% have top secret clearances. One major initiative that DHS is working on is standardizing the nomI&Ation form that is used for this community. DHS is filing a new SLTPS prelimI&Ary nomI&Ation form for clearance eligibility. The goal is to have one standard form across the community to include the components. What we identified when we peeled back the onions as far as clearance nomI&Ation goes is we recognize that all the components include internal DHS whereas using multiple types of nomI&Ation forms. So, our office took the initiative to kind of come up with one form. We're piloting that right now. Some of the states are going to see that coming across their desks within the next couple of weeks. The goal is to push out that form at the beginning of fiscal year 25.

From a compliance and governance program perspective, DHS has performed two new room certifications, so we have two new fusion center secure rooms, and we have completed 15 facility secure room inspections that fall under DHS purview. The schedule right now calls for 18 to be completed for fiscal year 24, so we're only three away from completing that requirement. So, whenever an individual or whenever a state requires a new room certification, they usually go through I&A and request that that room be certified by DHS. So, I&A will go out there, conduct their prelimI&Ary inspections, and then we'll go out there and certify the room. So, we had two new room certifications this year. We're currently working on the inspection schedules for FY25. We'll be pushing those inspection schedules out to the directors and the security liaisons at the beginning of the new fiscal year in October. And then last but not least, DHS initiated an administrative clearance review of its sponsored SLTPS clearance holders as an ongoing initiative to protect classified national security information.

I think last PAC we announced that we were going to roll everybody into an automated e-learning management system for I&A clearance holders. That rollout was very successful, and so when we plan on rolling out this year, we did 100 percent validation of clearance

holders that are supporting the I&A mission, and what we identified is over 750 personnel who no longer require DHS clearances. So, through the work of I&A, SLTPS, and our office, we were able to administratively or debrief individuals that no longer needed a clearance. We're going to continue to roll out that initiative next fiscal year, and anytime we do an inspection, we'll be running those reports through our ISMIS reporting system to ensure that we are identifying anybody who no longer needs a clearance.

So, those are the high-level initiatives that we're working on, DHS OCSO. Any questions for me?

Kevin: Kevin Klein, I had a question for the state and local partners. So, as far as people that are falling off the list, are you going back to the security officer at those organizations and asking them? I heard that we had to wait, so I didn't know if it's easier for us to just let you know who's dropped off.

Juan: Yeah, anytime somebody drops off, please let us know. I think there is an initiative right now to go back to you guys to ask, but if you guys have that information ahead of time, send it over to us, and we'll take care of it.

Kevin: One of the challenges was that we couldn't get the list of who's got clearances that came through us, so we might want to work on that, too.

Juan: I got you. Yes, sir. Yeah, I'll catch up with you afterwards to make sure we can support you.

Kevin: Thanks.

Juan: Alright, Heather. I think that's it for us. Thank you.

Heather: Alright. Thank you, gentlemen. Greatly appreciate that. Candice, do we have anyone in the queue for questions for DHS?

Event Producer: There are no hands raised at this time.

Heather: Thank you, ma'am. At this time, we will now introduce our speaker. Mr. Kevin Dillon, Associate Director of Strategic Relations with the Stakeholder Engagement Division at the Cybersecurity and Infrastructure Security Agency, will brief on what his office can provide SLTPS entities. Kevin?

Kevin: Hey, thanks, Heather. Appreciate the introduction, and great to be here today. As Heather said, my name is Kevin Dillon with CISA's Stakeholder Engagement Division, and I'm going to talk a little bit about some of CISA's operational priorities, some of our initiatives, and then services that are available to everyone on the call here. Cybersecurity and Infrastructure Security Agency, or CISA for short. We're the newest agency in the federal government established in 2018 to be America's cyber defense agency. We lead the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. We have a strategic plan laying out four goals really to address a lot of the challenges facing the United States.

We have three goals focusing on how the agency will work to reduce risk and build resilience, and then a fourth goal really focusing internally on the CISA agency itself. Our first goal is around cyber defense and really leading the national effort to ensure the defense and resilience of cyberspace. As I mentioned, serving as America's cyber defense agency, we lead the national effort to defend against cyber threat actors that target U.S. critical infrastructure, federal, state, local governments, private sector, and the American people. We're leaning forward on the cyber defense mission towards a collaborative, proactive risk reduction measures. Work with many partners. Part of our responsibility is help mitigating the most significant cyber risks to the country's national critical functions, both as these emerge and before incidents occurs.

Our second strategic goal is risk reduction and resilience. It's all about reducing risks and strengthening the resilience of America's critical infrastructure. We coordinate a national effort to secure and protect against these critical infrastructure risks, and this is all centered around identifying which systems and assets are truly critical to the nation, understanding why they may be vulnerable, and then taking action to manage and reduce risks to them. CISA serves as a key partner to critical infrastructure owners and operators nationwide to help reduce their risks and build security capacity to withstand new threats and disruption.

Third goal is around operational collaboration and really trying to strengthen whole-of-nation operational collaboration, information sharing. At the heart of CISA's mission is really about partnership and collaboration, working to secure cyber and physical infrastructure, always challenging ways of doing business and actively working with our government partners, industry, academic, international. Really to be action-oriented collaboration, really committed to growing and strengthening our agency's regional presence, which I'll talk about, and delivering capabilities and services to our stakeholders that need them.

Our fourth goal is more internally focused agency unifications, what it's called, really just driving kind of a one CISA approach through integrated capabilities in our workforce. Really just all about creating that one team behind our shared mission, just being the most efficient agency that we can be.

So, shifting over to just some of the services and capabilities, I want to mention our CISA regional presence. CISA has 10 CISA regions aligned to the same thing as like FEMA's, and really they're all about directly supporting local government, critical infrastructure owners, operators with risk mitigation solutions, capabilities, services, et cetera. An example of some of the things that they can provide for you, cyber and physical vulnerability assessments, things like architecture review and design, subject matter expertise, incident response support, exercise planning and support, that you help around national special security events. Each region has a regional director and then has, depending on the size of the region, may have multiple protective security advisors, cybersecurity advisors, emergency communications coordinators, chemical security experts, election security. So, each region has a cadre of those staff that can conduct in person, et cetera, conversations and meetings to sort of start a path for you and talk about CISA services and capabilities. The regional staff across the country support all 56 states and territories, and again, really there to help you with capabilities through a wide range of initiatives.

Another campaign we have going on, I'll talk about a couple campaigns and then finish up with services. You all may be familiar with CISA's Secure by Design campaign. We launched that in 2023, and this is all about urging software manufacturers to really revamp how they design and develop product software to create a future where technology products are safe for customers out of the box. In 2024, we're moving from awareness into industry action and turning those principles into progress by creating a Secure by Design alert series where we publish blogs and starting to reframe the conversation to focus more on the software manufacturers and what they can do to really implement that Secure by Design. CISA has a Secure by Design pledge. We have a little bit over 150 technology companies that have signed onto that pledge, and it has a number of actions for them, and we'll be checking in with them and looking for them to publicly state how they're implementing the actions there. Really trying to get folks to kind of move away from words like vulnerability when discussing cyber incidents and start using more terms like product defect, coding error, to really make it clear that software manufacturers can do more around fixing these defects to prevent cyber incidents. We really think kind of reframing this conversation is really important because these manufacturers can start to implement safer software and really understand the mechanisms to do so. So, as we continue to push the Secure by Design message, CISA had a Secure by Design white paper a year ago, initially came out with 10 U.S. and international partners, and then roughly six months later, we had seven additional partners join us to publish an updated version of that titled The Balance of Cybersecurity Risk Principles and Approaches for Secure by Design Software. To learn more about this initiative, go to cisa.gov/securebydesign. You can see all of the papers that we publish, the blogs, alerts, et cetera. So, it's a good resource there on cisa.gov.

Another campaign I want to highlight is our Secure Our World, our evergreen cybersecurity awareness campaign. We launched that in September of 2023 and launched a public service announcement, really kind of a fun way of doing it, really just all about bringing awareness to the public, about being safe online, really focused on four key messages. Then we had a second PSA we launched in May of this year 2024. Each PSA focuses on four key messages, recognizing and reporting phishing, using strong passwords and a password manager, leveraging multi-factor authentication wherever, whenever it's possible, and then updating software and leveraging automatic updates whenever, wherever possible. So, that campaign, again, will continue. That's our umbrella cybersecurity awareness campaign. As we start to look towards October and Cybersecurity Awareness Month, we'll have some additional videos really honing in on each of those four behaviors I mentioned, all being a similar style and sort of, you know, kind of same characters just to kind of bring that brand recognition forward. Same thing on cisa.gov/secureourworld. You can find a number of resources that are available. You can use them as is. We have tip sheets for each of the four behaviors. Those are translated into a number of different languages. So, you know, if you wanted to have your own campaign or create some of your own social media, you can leverage the materials that we have. We've got toolkits up on there. We'll be doing a lot of social media around October, Cybersecurity Awareness Month. We post on CISA social media every Tuesday, something framed around Secure Our World, so, we're very active in that space. You may have even maybe heard it on the radio or TV, things like that. We've got some ad buys going on for that piece.

So, I'll jump over to CISA services, you know, services and tools that are available to you now. Again, many of the, you can find all the details on cisa.gov, but CISA offers a number of no-cost resources and tools, which I'll highlight a few of those things like cyber hygiene, vulnerability scanning, we've got our cybersecurity performance goals. But really, we kind of always suggest folks start with the kind of top three services that we offer, really kind of foundational actions to really help you start building a program if you're kind of just starting.

First one we say is really connecting with your regional cybersecurity advisors I talked about. Again, these folks are assigned to all of our 10 regional offices. Regions are depending on the state that you go into. So, again, cisa.gov/regions, you can find all of the breakdowns, see which region you would fit in, and then the contact information for any of those folks.

But then the second piece, we'd always say, signing up for that cyber hygiene vulnerability scanning service. Even if you have a robust vulnerability management program in place already, this can complement that. It is, you know, it could be, you know, no cost to you, easy to sign up, and it's going to be scanning your externally facing addresses on a weekly basis, which you'll get a report, so, we're really, encouraging, we're trying to get a greater uptake of that service. It scales widely, meaning if the entire audience here signs up, you know, there's plenty of room for that, and the capability that can be done really easily. If you have cisa.gov, you find that service, it's a simple email to request it, and they'll get you set up and running within about two weeks at most. So, very easy to sign up for.

Another area we have is our cybersecurity performance goals. We have an assessment around this and a checklist, but these are really a common set of practices that, you know, all organizations should be looking to implement and kickstart their cybersecurity efforts. So, this is from small and medium-sized businesses up to large organizations, helps prioritize investment for essential actions that have high impact outcomes. We've even mapped these services to a link we have called free cybersecurity tools and services, so that if there's a capability we have linked to, some of those are CISA services, some of, you know, external partners that have provide free capabilities, we link to those things. You can say if you don't have a capability in there, there's many times there's a link to a free tool or service that either CISA or one of the partners that we have is captured there. There's things like CISA Exercises. We can do things like tabletop exercises, can send sort of pre-canned materials around those. You could do on your own or bring in CISA exercise subject matter expertise to facilitate things. There's a couple of different ways to manage that.

The final one I would mention, we also have our cybersecurity evaluation tool. CSET is the acronym, and this is a, you know, standalone desktop application really all about guiding owners and operators through a process of evaluating their either operational technology environments or their IT environments. We have a newer module in there called a ransomware readiness assessment, just essentially a self-assessment based on a set of recommended practices just to, you know, understand how well you are to equip to defend against or recover from a ransomware incident. So, good capability there.

And then on CISA.gov, last one I'll mention, is you can sign up for alerts and advisories. So, we're sending out industrial control system alerts, vulnerability summaries, product alerts, things like that.

It's a pretty active alert system. You know, you likely get two to three emails a week. So, kind of in closing as a final resource, we always direct you to that CISA.gov website. The website is really organized by service and tools, you know, really makes it easy to find, you know, basically a one-stop shop to help you find all the resources that you need. You know, so we always suggest take a look around there, look at the resources, look at the regional capabilities that we have. All that information is there and stays really active and updated on a regular basis. Really appreciate you all having me on here on the call today. Happy to stay around and take any questions, but thanks for the time. Back to you, Heather.

Heather: Thank you Sir. Are there any questions for Kevin? Candice, how about the queue? How's that looking?

Event Producer: We did not have any questions. Someone raising their hand. Someone's question did get posted in chat. I'm going to send that to you now.

Heather: Okay. Thank you. Okay. We have a question that says, "AI large language models, LLMs, may present a significant challenge to the classification system due to their ability to infer sensitive information beyond the classification level of their training data. To tackle this issue, a collaborative team, including scientists from a national laboratory, Yoshua Bengio, and researchers from the University of Illinois Urbana-Champaign (UIUC) is conducting red team experiments. These efforts provide crucial insights for policymakers and could play a vital role in developing robust safeguards for classified information.
We're looking for your expertise to help shape our research direction. Would any stakeholders be interested in advising on potential experiments in helping define the scope of this project? If so, please reach out to me. My email is heather.harrispagan@nara.gov.
Thank you, Candice. Are there any other questions?

Event Producer: There's no one in queue.

Heather: All right. Thank you. We are now at the point of the meeting where we ask for SLTPS members to present any new business they may have. Does anyone have anything? Do any members of the public have any questions or remarks before we close out today's meeting?

Event Producer: Just as a reminder, you can press #2 on your phone or click the hand icon on WebEx.

Heather: Alright. Our next SLTPS-PAC is scheduled for January 8, 2025. Meeting adjourned.