Mark Bradley: Good morning, everybody. Welcome to the 21st meeting of the State, Local, Tribal and Private Sector Policy Advisory Committee, commonly 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 isoo-overview.blog.archives.gov or by going to the Federal Register. This is a public meeting. Transcript and minutes will be available within 90 days on the SLTPS-PAC Reports on Committee Activities Web page. All right, I'll now begin attendance.

DHS Vice Chair, Rich McComb. Rich are you there?

Richard McComb: Yes, I am. Good morning, Mark. Thank you.

Mark: Good morning, Rich. Happy New Year to you.

Richard: Happy New Year to you.

Mark: And DHS alternate, Ricardo Durón. Ricardo, are you there?

Ricardo Durón: Hi, guys. I'm happy to get on this thing.

Mark: Great. All right. DOE, Mark Hojnacke?

Natasha Sumter: Good morning, Mark. This is Natasha Sumter. I'm actually participating in his stead.

Mark: Okay. Sure. All right. DOE member, Tracy Kindle?

Tracy Kindle: Present. Good morning, everyone.

Mark: Good morning to you. DOE alternate, Natasha Sumter?

Natasha: That's me. Good morning.

Mark: Good morning to you. NRC member, Sabrina Atack?

Darryl Parsons: Mark, this is Darryl Parsons. Sabrina can't make it today. She is on actually a rotation elsewhere in the organization.

Mark: Okay. Thanks, Darryl, for that update and welcome to you.

Darryl: Thank you.

Mark: You're welcome. DOT remember, Sidonie Dunham?

Sidonie Dunham: I'm here. Good morning.

Mark: Good morning to you. DoD member, Michael Russo?

Michael Russo: Yes, sir. Good morning. Present.

Mark: Hi, Michael. ODNI member, Valerie Kerben?

Valerie Kerben: Hi, Mark. I'm here. Good morning.

Mark: Hi, Valerie. Welcome to you. FBI member Jake Zockert?

Jacob Zockert: Yes, sir, present.

Mark: All right. Great. FBI alternate, Scott Gerlach.

Scott Gerlach: Good morning. I'm present.

Mark: Hi, Scott. CIA member, Brian O'Neill? All right. State Department member, Kate Connor?

Kate Connor: Good morning. I'm here.

Mark: Hi, Kate. DOJ member, Glenn Bensley?

Glenn Bensley: Hey Mark, I'm here.

Mark: Hey, Glenn. DCSA member Keith Minard?

Derrick Broussard: Good morning, Mark. This is Derrick Broussard, DCSA alternate member. I'm here.

Mark: All right. Great, Derrick. All right. SLTPS Vice Chair, Private Sector, Marc Sachs.

Marcus Sachs: Hey, Mark. Good morning and Happy New Year.

Mark: Same to you, Marc. SLTPS Tribal West member Tom Woolworth. All right. Nothing from the West today. All right. SLTPS Local East member, Tom Carr. All right. SLTPS East member, Eric Tysarczyk. SLTPS Local East member, Meghann Teubner.

Meghann Teubner: Good morning, everybody. I'm here.

Mark: All right. Great, Meghann. SLTPS Local East member, Shelly Schechter. All right. SLTPS State West member, Debra Ann Winsor.

Debra Winsor: I'm present. Thank you.

Mark: Good morning. SLTPS Private Sector member, Jeffrey Imsdahl.

Jeff Imsdahl: Hey, good morning, Mark. Jeff's on.

Mark: Good morning, Jeffrey. SLTPS State member, Kevin Klein.

Kevin Klein: Present. Good morning.

Mark: Good morning to you. Speaker Marie Bernoi.

Marie Bernoi: Marie Bernoi, FBI, here. And also our new section chief, Jake Zockert, whose section will be handling this, is on the line as well.

Mark: All right. Good morning to both of you and welcome. John Costello. We'll meet him later on, and Kimberly Keravuori from the National Archives. We'll need Kimberly, too, to talk about CUI.

All right. Well, anyway, hopefully as we go on, these folks will join us. All right. If anyone else is on the call that we've not heard from, or I don't know about, please speak now for accurate roster accounting for the public record even if you're only listening.

Carolina Klink: Carolina Klink, ISOO.

Mark: Good morning, Carolina.

Steven Stern: Good morning. FBI, Steven Stern.

Mark: All right. Good morning, Steven.

John Castro: Good morning. John Castro, FBI:

Jon Cofer: DCSA, Jon Cofer.

Mark: Hi, Jon.

Larry Clark: Good morning. Larry Clark, ISOO.

Mark: Hi, Larry.

Robert Tringali: Robert Tringali, ISOO.

Mark: Hi, Robert.

Robert: Good morning.

Heather Harris Pagán: Heather Harris Pagán.

Mark: Hi, Heather.

Brian O'Neill: This is Brian O'Neill, CIA.

Mark: Okay. Hi, Brian. Anyone else?

Juan Estrada: Hey, good morning. This is Juan Estrada, DHS.

Mark: Okay. Great. Anyone else?

Eric Tysarczyk: Hey, good morning. Eric Tysarczyk, from New Jersey.

Mark: Hi, Eric. All right.

Greg Pannoni: Greg Pannoni, ISOO.

Mark: Hi, Greg.

Greg: Hi, Mark.

Mark: Anyone else? I think we finally got it. Okay. All right. I want to remind government membership again of the requirement to annually file a financial disclosure report with the National Archives and Records Administration Office of the General Counsel. It's the same form of financial disclosure that's used throughout the federal government, which is OGE Form 450, which satisfies these requirements. A member of my staff should have already reached out to you asking for it. If you have any questions, just let us know.

All right. We have a few changes to the SLTPS-PAC membership. Leo Masciana has finally retired from the State Department after a long and distinguished career. Kate Connor will be replacing him formally once we get the official designation letter. Angel Catalan from the FBI is also no longer on the SLTPS-PAC. He's been replaced by Jake Zockert. Scott Gerlach remains the alternate for the FBI. There will be other SLTPS-PAC members who finish their four-year term this year. Tom Carr ends in March and Marc Sachs in July. On the federal side, Valerie Kerben, ODNI, will need a redesignation letter in March to be able to continue.

I also want to provide everyone with our agency's COVID update. We're still operating under COVID conditions. All but a few members of my staff are operating under 100% telework. We have buildings across the country that are in various stages of reopening. We will keep the SLTPS-PAC informed if there's a substantial change in ISOO's operations.

The SLTPS-PAC minutes from the last meeting were finalized and posted to the ISOO website on September 30, 2021.

All right. Getting to the heart of the meeting, we're going to now hear from Meghann Teubner on a New York City Critical Infrastructure Cybersecurity Initiative. Meghann, the floor is yours.

Meghann: Excellent. Thank you so much, and thanks everybody for the time this morning to walk through an initiative that we started here in New York City back in 2017 in recognition of the kind of growing cyber threat to critical infrastructure, to local government facilities, online facilities, and learning lessons from the kind of counterterrorism mission in New York City and across the U.S. on the need to ensure critical information sharing in a timely manner. So in 2017, the NYPD collaborated with the Manhattan District Attorney's Office, New York City Cyber Command and a nonprofit called Global Cyber Alliance here in New York to form the New York City Cyber Critical Services and Infrastructure Group, CCSI. What CCSI does is protect New York City's critical infrastructure and essential services by communicating critical cyber threat intelligence to all 17 sectors here in New York City, and that ranges from information that we in NYPD receive from our federal partners on key indicators of compromised IP addresses, threat tactics that are being used by malicious actors, whether that malicious actor is a cybercriminal or a malicious foreign state actor. So the key component of, and the driving force of, this working group or this initiative is information sharing so that all public and private sector critical infrastructure agencies have the information they need to protect their systems, because all of these systems whether they're separate, they're in some way connected, because we're all in the shared mission safe space of keeping the city safe.

Just a little background on the mission and goals and where the group is looking to head, and I should preface this by saying this initiative for the NYPD is represented by Lieutenant Gus Rodriguez, who unfortunately was not able to join us today. So I'm happy to take questions at the end of this overview. But I'm also happy to link you up directly with Lieutenant Rodriguez, who can give you more in-depth information on the day-to-day workings of CCSI and how they share that information. So the mission of CCSI is to mitigate cyber threats to critical infrastructure across all 17 sectors in New York City, including telecommunications, finance, energy, water and emergency response and that does include NYPD systems, 911 systems, et cetera. We want to increase the coordination and facilitate a mechanism to respond to cyberattacks in recognition that in some cases the agency that is currently facing some kind of cyber threat may not be the best place to address that threat at that time, and so if you have these partnerships in place, both in the public and private sector, that you can kind of use everybody's tools in the toolbox to help mitigate additional threats. CCSI currently focuses on New York City based threats, although we recognize that what is happening in other, you know, localities and to other agencies may happen here, so the end goal truly is to learn and to continue to adapt to the threat as it evolves. One of the key factors of CCSI is to foster a good public private sector partnership around cybersecurity. There are a lot of silos in cybersecurity, especially in private sector and public sector and information flow, I know it is getting a lot better, but the whole point of CCSI is to bring everybody together into a room to share information, to share best practices, and ensure that maybe one agency is familiar with a tactic that may impact another agency, so that is something that CCSI strives to ensure that everybody has access to information when they need it the most.

One of the things that the CCSI initiative did a couple of years ago is they arranged for a cyber range kind of tabletop exercise. They developed scenarios based on real use cases of cyberattacks and brought together public and private sector, sat in a room, and actually just worked through a scenario, several scenarios, to figure out gaps in information sharing to figure out where maybe we needed improvement on certain security measures, and so they continue to conduct exercises like this and think through potential threats down the line and how we can better shore up our systems, but also our partnership.

Right now, NYC CCSI has 144 members, 57 organizations and 13 sectors. This includes here in New York City Con Edison, it includes CrowdStrike, Mandiant, Citibank, IBM, New York City Health and Hospitals, Northwell Health, FDNY, NYPD, New York City Cyber Command, Verizon, JPMorgan, Booz Allen, NYC Environmental Protection for water protection, so as you can see, it's kind of a range of sectors and public and private sector partners. They are looking to, hopefully in 2022, bring people together again to do another cyber range, red cell type activity to continue to kind of practice sharing information in the midst of a critical threat. We had a meeting here in New York City and brought everybody together to red zone attack and to have everybody in a room and talk through what they would be doing step by step in a scenario as something was unfolding, and this included a potential cyberattack that would have physical, real world ramifications. So again it's thinking through worst case scenarios, trying to build these partnerships before they're needed and to kind of replicate what we have in the counterterrorism, domestic violent extremism mission space of a kind of free flowing information and to bring that into the cyberspace.

So that is kind of a quick overview of CCSI. I'm happy to take some questions on how they share information. As of right now, a lot of that is done very much in an email or signal group distribution where members, you know, agree to participate. They sign up, and they have a closed and encrypted network where they share information, but again the point of me speaking today was, we've had some conversations on this call before of how to get information, critical cyber threat information, out to the widest possible audience, and appropriate audience, in recognition in some cases that, some sources and methods will always need to be protected, and to our federal partners' credit, I have been really impressed with the amount of information that is being pushed out in the cyber threat space from CISA, from FBI, with these indicators of compromise, with the potential tactics that could be used by malicious actors. What NYPD and the Manhattan DA's Office, New York City Cyber Command, and Global Cyber Alliance are trying to do is make sure that that information that is getting pushed out is getting acted upon; that there's email communications that say, here's this threat information. This is really important that we protect our critical infrastructure and open it up to questions from other partner agencies. Again, it's all about that shared mission space and shared security. So again, Lieutenant Gus Rodriguez is the lead for NYPD on this initiative. Unfortunately he couldn't join us today, but he is available for questions and willing to be

linked up with anybody. I'm happy to try to address any questions that you may have now.

Mark: Thank you, Meghann. All right. Does anybody have any questions for Meghann?

Marcus: Meghann, this is Marc Sachs, private sector.

Meghann: Hi. How are you?

Marcus: Great. Thank you. Thanks for a wonderful presentation. Do you know of other cities that are like New York and are doing similar things? And are you guys like cross-coordinating, say between you and Chicago, LA, other major cities?

Meghann: So I know those conversations have happened. I don't know how robust other cities' initiatives are and if they have been able to get them off the ground. That is one of the kind of goals for 2022-2023 that we have. And I've spoken to Lieutenant Rodriguez about it. One of the reasons why we wanted to speak on this call is to kind of push this concept out to other cities and other municipalities so that similar efforts can be developed. So I guess this is a long way of me saying, I don't have a great answer for you. We hope that this is something that we can package up and push out and encourage others to build in their own cities. So that's part of the reason why we wanted to speak today.

Marcus: Yes. I appreciate that. It's like any other police department. There's a general model, but it's always going to be tailored to the…

Meghann: Yes, exactly. What works in New York City may not necessarily be exactly what would work in another city, but it's the concept that's easy to replicate.

Marcus: Exactly. And the follow on to that, I'm sure you're aware of the Secret Service's training facility down in Hoover, Alabama, where they do forensics. I presume many of your folks have been through there? Is there value coming out of that? Is that something others should get more engaged in? And I'm just speaking, kind of promoting what the Secret Service is doing because I love what they're doing down there with training of police officers and sheriffs and others.

Meghann: Yes. You know, I'm aware of their training facility and I know that they do excellent training. I haven't participated myself so I can't speak, at an expert level as to it, but I'm happy to take that back to folks that I know here who have done it and get back to you on that.

Marcus: Yes, I appreciate that, and Mark, maybe that's something for a future meeting would be to let them brief us on the training they're doing for cyber forensics for law enforcement across the country.

Mark: I know that sounds very interesting, Marc. I agree.

Marcus: Thank you.

Mark: Anyone else have anything else for Meghann? All right. Well thank you, Meghann, for such an excellent and informative presentation. We appreciate it.

Meghann: It's my pleasure, and if anybody has follow on questions afterwards, my email is in the distro list so please don't hesitate to reach out.

Mark: Okay. Great. All right. I'm having to turn to Greg Pannoni, my deputy in ISOO, who will now address the status of action items from the July 29, 2021 meeting. Greg?

Greg: Great. Thank you, Mark. If I could, though, I just wanted to check in to see if Kimberly Keravuori has joined the call. I guess not.

Heather: Sir, she's going to be joining around 11 o'clock. She's in a 10 o'clock meeting right now, Sir.

Greg: All right. Good. I thought she actually had to leave at 11:00. And the other thing, Mark, Valerie Kerben, who is on the line, has to break off early. So if it's okay, I'd like to ask Valerie if she has any updates to send to us now.

Mark: Yes. Of course, of course. Valerie, the floor is yours.

Valerie: Hi. Good morning. Thank you. Just for this group here, you know, we're really diligently working through, it's called Trusted Workforce 2.0. We have a lot of policy level documents that we're trying to get through the Director of National Intelligence and the Director of OPM to be signed. The whole process is to modernize and transform the way we do investigations and adjudications. There was one note that was published, the Transforming Federal Personnel Vetting Cabinet Memorandum. This was signed by the National Security Advisor on December 14th, and it was disseminated to our federal agencies, which demonstrates the administration's commitment to personnel vetting reform. This is where we're asking departments and agencies to prioritize and implement those reforms as they come along. It's going to be a real iterative process so different documents come out at different times to help agencies, you know, transition and implement in their programs. We've also asked agencies to designate senior implementation officials who will be accountable for the implementation and ensure related efforts are successful at their agencies. So, you know, like I said, we're just very busy working through all this. And as things become available and public, you know, we can all let you know. I think that's it for me. Thank you, Mark.

Mark: You're most welcome, Valerie. Does anyone have any questions for Valerie before she rings off? Okay. Thanks again, Valerie.

Valerie: Thank you.

Mark: All right, Greg. The floor is yours again.

Greg: Okay. Thank you, Mark. As Mark noted, the minutes were finalized September 30th and are on our www.archives.gov\isoo on the website there. There's also the full transcript of the last meeting as well, and the agenda is there for today's meeting.

As far as the items we had from that July 29th meeting, there were three. Today we'll hear from the FBI on the status of a process to provide its SLTPS personnel security clearance data to the Defense Counterintelligence and Security Agency, which houses the central verification database for clearances, and if possible, part of that effort was to identify non-task force officers in their system. That is the FBI system for inclusion as part of the whole data transfer of these clearance records, so that we would have that robust database of all SLTPS personnel that have been granted security clearance. So the PAC, we've focused on this issue for a couple years. The FBI has made a lot of progress in the past year. As far as I'm aware, they reported they have been engaged in the end-to-end testing of the data transfer with the CSA, and we will hear more on that in this meeting.

The next outstanding action item is still tabled due to COVID restrictions. This one had to do with ISOO hosting a meeting in our SCIF with ODNI and other entities as appropriate to examine why the Intelligence Community is unable to determine and provide the current number of SLTPS personnel that have been granted clearances and to seek a means to obtain that information, so until we're able to come back into the office and discuss this in a more secure setting, that item remains tabled. This is really related to the first item because it all pertains to the notion that's laid out in the executive order and the directive for this program that there be a robust clearance database of all individuals that have been granted clearances under this program.

The third item had to do with the Cyber Threat Information Sharing Group and the recommendations that it had put forward. The DHS vice chair did provide DHS's formal comments on those 15 recommendations, and at this time, ISOO and DHS are in discussions on the recommendations and the comments from DHS, so the chair will then determine potential ways forward and communicate them to the SLTPS-PAC membership. So do any of the members have any questions? Okay. Thank you. Mark, I'll turn it back over to you.

Mark: Okay. Thank you, Greg. I appreciate that. At this time we would now like to hear from the Executive Agent for the program, DHS, Rich or Ricardo, any updates for us?

Richard: Good morning, Mark. This is Rich McComb, the Chief Security Officer for DHS. So kind of an end of year performance reporting for fiscal year 2021. DHS, as we stated before, has approximately 9,000 SLTPS personnel with DHS sponsored clearances. Eighty-eight percent of that population is at the secret level and the remaining 12% is at the TS level, obviously the intent there being to keep it at the secret collateral level in accordance with the Executive Order.

Our compliance and governance team performed three room certifications of SLTPS locations and 18 security performance assessments during this past year. Most of those, because of COVID, were virtual in nature. These facilities included fusion centers and emergency operation centers. Forty-three percent of all the findings of these security performance assessments were administrative in nature, and were in most cases, able to be mitigated on the spot or within 30 days of the final report, so no major concerns out there with regard to compliance from an information security and personal security discipline perspective. For FY22 we have scheduled 17 SLTPS facilities that are sponsored by DHS for an assessment. We will attempt, obviously dependent upon the continued variants, Omicron variants, the impact of that to do these onsite where at all possible, but if the pandemic continues and the safety protocols and travel restrictions, et cetera, don't allow us to do that, we will continue to do those remotely as required.

A couple of public service announcements, to kind of chime in on what Valerie Kerben from ODNI mentioned here earlier on the Trusted Workforce 2.0, I don't know that in my time on here, we've mentioned this very much, but what she mentioned will apply to those who have been granted clearances by the executive branch.

So the one thing that I think will be important for those here online to know in our state and local, tribal, private sector partners to know is that this model changes the U.S. government vetting from a, you know, every 5 or 10 year, in most cases here, with our folks online periodic reinvestigation to continuous vetting models. So, if you have a clearance sponsored by a partner or agency in the executive branch, you will undergo a continuous vetting model in lieu of that 5 to 10 year reinvestigation, so I think that's probably an important thing and obviously more from a communication perspective as Valerie mentioned. Likewise, for those you who may or may not know in December of 2016, the Office of the Director of National Intelligence signed Security Executive Agent Directive 3, which is Reporting Requirements for Personnel with Access to Classified Information or Who Hold Sensitive Positions. It was effective in 2017, and what SEAD 3 requires is reporting for all people across the federal government, including individuals with security clearances from departments and agencies to include contractors, subcontractors, licensees, certificate holders, grantees, experts and consultants who perform work on behalf of SLTPS entities, so as I mentioned for DHS, that will include certainly our 9,000; for other departments and agencies, obviously whatever number of folks they are sponsoring, things that are required to be reported are, you know, unofficial foreign contacts, foreign activities, unofficial personal foreign travel, arrests, charges, detentions, changes in marital status, change in name, change of cohabitation, enrollment in drug and alcohol treatment programs, financial issues and other anomalies. There are about 19 items here. Now obviously the challenge has been really, I think, reporting that. Obviously our partners, certainly from a DHS perspective, have been reporting those things. But we are piloting an automated reporting tool here in DHS that will allow our partners

who have DHS sponsored clearances to report that through a portal which will make it easier for them and for us to monitor those changes as required by the Security Executive Agent Directive, so as we pilot that, we're happy to share with our federal partners on the line here, you know, if you're interested in employing this or looking at something similar. More to follow with our DHS sponsored clearance holders as we get ready to roll out this capability. You don't have to have an email, U.S. government email, et cetera, to be able to update your status in this portal. So more to follow but I just kind of wanted to let everybody know of that requirement and how we intend to try to make that easier for folks to meet that.

That is all I have, Mark. Thanks.

Mark: Thank you, Rich. An excellent presentation and I'm glad you mentioned both those items because they are extremely important. Does anyone have any questions for Rich on this? All right. Thanks again, Rich. I appreciate it.

All right. Up next, we're going to have Jake Zockert with the FBI and his team to talk about action item one updates that Greg mentioned earlier. Jake, the floor is yours.

Jacob: Thank you, sir. Can you hear me okay?

Mark: I can, yes. Please.

Jacob: I appreciate it. So just a very brief update and then we'll kind of go around the horn with the other representatives of the FBI in case there are any other action items that I failed to discuss.

So as was mentioned earlier, we coordinated with our IT applications and data division to ensure that we sent around 11,669 records on our task force officers over into CVS, so that action is complete.

The other action item for this group was the discussion about the remaining private sector clearances that the FBI holds. We've scoured our records and identified approximately 1,245 personnel within that category, understanding those numbers will vary as people slide in and out of that program.

Where we are in the process now of transferring that information over to CVS is we are scrubbing those lists a final time to make sure that they are secure as far as the data and contact information is concerned. Once that passes through our internal reviews and is approved by executive management, the plan is to transfer those over into CVS as well. We should have a more substantive update absolutely by the next time we convene, if not far sooner. So with that brief update, Scott Gerlach, sir, is there anything that you would like to update from anything that transpired in the previous meeting that I was not in attendance?

Scott: No, sir. I think you've got it all.

Jacob: Terrific. Also on the line I have Section Chief Marie Bernoi who oversees portions of our IT team as well as, I think, Section Chief Earl Camp has joined over our security and suitability clearance section. Section Chief Bernoi, ma'am, do you have anything to add?

Marie: No. I just want to let you know that the IT team does continue to work with DCSA for the CVS feed. So we are monitoring that. We are looking at what the level of effort will be to send the remaining private sector clearances. Over.

Jacob: Thank you, ma'am. And then finally over to Section Chief Camp, sir. If you're on, do you have anything to add?

Earl Camp: I am on and I don't have anything to add. Thanks, Jake.

Jacob: Terrific, sir. With that very brief update, we will open up the floor to any questions for the FBI and concede the remaining time if there are none.

Mark: Okay. Does anybody have any questions for the Bureau? All right. Well thank you so much for that update. We really appreciate it and I'm glad to hear that this is progressing.

All right, Greg. We're in a bit of a quandary here now. We've been road running through this thing and it's what, 9:38. Kimberly is not coming on until 10 o'clock.

Heather: Mark, both John and Kimberly are on.

Mark: Okay. Great.

Heather: So go ahead and continue.

Mark: Okay. Then I'll strike from the record what I just said. All right. We're now going to hear from Kimberly Keravuori, Regulatory and External Policy Program Manager with NARA, to give us an update on the Controlled Unclassified Information program. Kimberly, the floor is yours.

Kimberly Keravouri: Thank you, Mark. Can you all hear me? I want to make sure I actually got myself unmuted.

Mark: Yes.

Kimberly: Okay. Great. Thank you. As Mark said, this is Kimberly Keravuori. I'm working with the CUI program for NARA. And I think one of the first things we want to update this morning to you all is the status of the CUI FAR clause that's being worked on with the FAR Council. Primarily we're helping them, and it was slated as of the fall unified agenda. It was projected to be coming out for public

comment sometime this month and possibly February, but it looks more like it will be coming out for public comment more in the March/April timeframe. We're finishing up some last comment rounds within the FAR Council itself before it heads over to OMB and interagency review. So that still has to occur before it can go out for public comment as a proposed rule. But it's very, very soon. We're on the last steps. Some of them may take a little while depending on how many comments there are, but we're near the finish line. So before I move on to another topic, are there any questions about the FAR clause?

Okay. And the other topic that I was asked to cover that you all may be interested in is the revisions that we're making to the registry of the Controlled Unclassified Information. The registry lists all the categories of CUI and the authorities within each category that give rise to the information being protected at CUI. The governing items for any type of information to be protected as CUI is the underlying authority, the law, the regulation or the government-wide policy. So the listing of those on the registry is important for determining what kinds of information are covered by the category, which agencies can make use of that information as a protected category and so forth.

As agencies have begun implementing and started to really, you know, try applying the CUI requirements to their particular operations, they've started to realize that a lot of the category structures, the way they had originally envisioned dividing them up, might not be the most appropriate divisions for the purposes of the way the information gets used and shared now that they're matching the two up. So we're undergoing a large, overarching revision process to the registry list of categories. We're looking at every single one of the authorities and writing up additional information on the authorities that will include what agencies are covered by them and the scope of the information that's covered by each authority. This was also a request from agencies originally that was not permitted because of some questions about how things would be interpreted and potentially written up and so forth, but agencies have found that it's really important information for them and others. So we're going through a process where we're vetting right up through all the agencies across the Executive Branch to weigh in on to make sure that the authorities are summarized correctly and then putting additional information on the registry pages for each of the authorities.

We're also looking at streamlining the categories, potentially merging some and reorganizing them in a way that will work better with the things that the agencies are finding works more appropriately now that they're trying to match the two up with the implementation process.

And finally, we're also beginning a project on addressing specified authorities. For those who are unfamiliar, the vast bulk of the CUI is protected using a standardized set of protections and it's called CUI Basic. Those items are ones that have authorities that say the information must be protected or restricted in some manner but don't set out the requirements for doing so and so they default to the CUI basic requirements, but because many of our authorities

preexisted the CUI program, there are a number of them that specify certain requirements, many, many of which mirror or are almost identical or at least at the very same level as the CUI Basic requirements, but because they're in statute or regulation, they can't be disregarded and they are somewhat different in small ways from the CUI Basic requirements that now exist because they came about in a time when there wasn't CUI, so those will eventually all need to be revised to work with the CUI program a little more smoothly, a little better, but in the meantime they present a different set of requirements for the information that they govern. The first stage of the project to work on bringing those more into alignment with the new CUI framework is to address ones that have limited dissemination or other filing type of requirements that are kind of in a gray area that could be somewhat administrative or somewhat security related and assessing each of those to determine whether some of them can already be treated as not specified requirements and still sitting within the CUI basic guidelines. We're working on all of those now for every category of the registry and we're starting with the ones that affect the most categories in the most agencies, so all of the privacy categories, the law enforcement categories, the legal categories, immigration categories and financially related categories, including acquisitions and proprietary information, which comes from contractors typically. All of that is ongoing right now. We are working zealously with interagency working groups and then sending everything through all the agencies for their review and legal input so that it is as sound and robust as possible when we roll it out.

And finally I do want to mention for this particular group that we are also working heavily on information sharing agreements in a number of different directions. I'm sure you're all aware that federal agencies partner with a great number of state, local, tribal and private sector entities outside of contracts to share information, some of which is sensitive CUI information.

And we are also aware that the CUI requirements are not state requirements or local requirements. So there's, you know, clearly currently some disconnect between what happens with the information in the hands of the federal government and what we are allowed to do with it as we share it and what the recipients can or are willing to do with it once they receive it. So the vehicle by which much of that is going to be addressed will be various types of information sharing agreements. We're currently working on ones that relate to sharing of tribal information and actually in both directions because there's a good deal of what would be CUI that we receive from tribal organizations as well as information we provide back to them. There's a working group of agencies that work heavily with tribal organizations to address that and try to determine the scope of the agreements and how to work those out.

And we also have international ones that are being looked at and addressed. And we are also working on ones for the broader state and local private sector partner sharing situations, so those will be forthcoming. We're working on these in a number of different directions and each of them has their own quirks that have to be taken into account. There is a lot of variety between agencies as

to the types of information they share and the types of partners and the capabilities of protecting the information, so we just wanted to let you know that that is being worked on, and we will probably come back and ask for your input and involvement when we get to a certain stage in the development of those.

Thank you. Any questions? Great. I turn the floor back over to you, Mark, I guess.

Mark: I appreciate it, Kimberly. Thank you for such a thorough briefing and also giving us an update on the elusive FAR clause. But we're glad to hear that maybe it sounds like you're running that thing down. All right. We're now at the point of the meeting where we ask for SLTPS-PAC members to present any new business they may have. All right?

Greg: Mark?

Mark: Yes, sir.

Greg: We actually have John Costello, I believe, is on the line from the Chief of Staff Office of National Cyber Director at the Executive Office of the President.

Mark: You're right. We switched. Okay. John, I offer my sincere apologies. All right. We're now going to hear from John Costello, Chief of Staff of the Office of the National Cyber Director at the Executive Office of the President, to provide an overview of what their office does. John, the floor is yours.

John Costello: Hey, good morning, folks. First of all I want to extend a thank you to you guys and certainly a warm welcome to State, Local, Tribal and Private Sector Policy Advisory Committee. I really appreciate you guys taking the time to have us come and brief. My remarks will be generally pretty short. I really wanted to talk about just the Office of the National Cyber Director in general. It's a new component in the White House with a Senate confirmed head, the National Cyber Director. Those are precious, you know, few positions within the Executive Office of the President. I think it's happened five times in the course of U.S. history. We're certainly proud to be the fifth one.

So I wanted to tell you guys a little bit more about like, you know, our origins, what we're doing and ultimately where we're going to go and who we're partnering with in doing that.

So we were created in the 2021 National Defense Authorization Act based off of a recommendation from the Cyberspace Solarium Commission. The purpose of this office is to drive federal coherence and craft under the direction of the President, a vision for U.S. defensive cybersecurity, pulling together all the elements of the U.S. government and the Executive Office of the President into a single, cohesive effort.

As many of you may have noticed or may not have noticed, the senior most official in the White House in charge of cyber has shifted in priority and has shifted in levels between administrations and across administrations, and I think this is a strong signal from Congress and the American people that given the level and scope and scale of cyber instance that we see every year, both in departments and agencies and in private sector critical infrastructure in our state and local partners, this needs to be an enduring, consistent and high level priority of any administration, irrespective of party or otherwise.

So Congress has created that office to make sure that it remains so and remains so over time. So, Chris Inglis, who is the first National Cyber Director, came onboard in July. And it was him in an office. That is where the office started.

We've grown in leaps and bounds since then. We're about 25 people with an expectation to triple and quadruple that by the end of the fiscal year in the calendar year, respectfully. That is a quantum leap and light speed growth when it comes to building a federal office, especially in the White House. That's something we're really excited about.

One thing I do want to talk about is sort of how we're organizing ourselves and what really we focus on. So we really have four enduring priorities and principles. Number one is federal coherence.

The national cybersecurity mission and federal cybersecurity mission has grown organically within departments and agency authorities over time. And each one are - right now we have a division of effort and division of labor between departments and agencies and what they tackle and who they work with.

Despite everyone's best intentions over time, that's grown a little chaotic. It's growing complex. And one thing that we're looking at is the key principle for everything we do is making sure that all of this coheres in an understandable and easily communicated way to the private sector, to state and local, other governments and frankly within our own federal enterprise.

Number two is private sector public private partnership, And I mean that from private sector in the U.S. government and the U.S. government and state, local, tribal and territorial entities.

You know, the U.S. government, state and local and private sector partners, none of us can do this alone. We know we have to work together to be able to contribute to the entire whole.

Our risk is shared so we have to take a shared approach but that doesn't mean the division of labor. It means a true collaboration where we share each other's information. We share each other's agency as we move forward.

Third is reconciling resources to aspirations. Accountability, making sure that we have a clear understanding of risk and that our dollars flow to where that risk needs to be ultimately mitigated.

This is a big deal. One thing that we were given as part of our authorities is Budget Review Authority, which is very rare in the White House. And that gives us a platform from which we review department and agency budgets and make recommendations that can align to overall strategic goals.

Last is present and future resilience. We know that the level of cyber instance reflecting critical infrastructure of all kinds, state and local and private sector is unacceptably high right now. We definitely need to take steps in the short-term in the interim to reduce that risk. But long-term we ultimately need to shape the technology ecosystem on which we all rely.

That's looking at the people. It's looking at the processes. It's looking at the technology, all the things that make up that ecosystem and making sure they're more sustainable and secure in the long-term.

So that's what our major principles are. But what is the scope of our work? Really, we've got six, you know, broad lines of effort, things that we are going to focus on as we build up. I'm not going to take too long in describing these. A lot of them are fairly self-evident.

Number one is federal cybersecurity. As many of you may know, the Chief Information Security Officer Chris DeRusha in October was appointed as our deputy for federal cybersecurity, working with OMB and working with the departments and agencies, making sure their enterprise cybersecurity is squared away and good to go.

Number two is national cybersecurity as distinct from federal. This is everything else. How do we ensure that the private sector and state and local are getting what they need and are in the loop in new and emerging incidents and vulnerabilities and are well prepared to make sure that they can rapidly respond to recover when they are affected by (unintelligible).

Supply chain technology security, we do have to look at the products, software, hardware, devices and services that make up our ecosystem and their supply chains to make sure that they're free from undue foreign influence, free from major vulnerabilities and are being designed and produced with the highest levels of security in mind.

Cyber planning and operations, so a big part of our mandate is forging a unified effort across departments and agencies to ensure that we have a common understanding of the threat, a common response and a common plan as incidents happen.

Every federal department agency and private sector partners that we work with all understand their roles. And we can transition seamlessly into crisis response mode when an unfortunate incident occurs.

Workforce training and education is our fifth line of effort. There's a major talent gap across all sectors and across all levels and across all enterprises right now when it comes to cybersecurity. And it's something that we know that's seen as an intractable problem, something that's deeply hard to solve, something that we know we need to take on.

That means trying to bolster the force within the federal government, increase training opportunities, expand pipelines, put in retraining programs. We know this is going to be a difficult line of work, but certainly an essential and important one.

Last but not least, it's budget review and assessment. As I mentioned, reviewing departments and agency budgets while certainly not edge of your seat, exciting work, it is absolutely critical.

If you want to know what someone's strategic priorities are, you look at their budget and we know that strategy has to follow. Strategy has to follow through into money otherwise strategy is largely irrelevant. So we're building a mechanism to ensure that is the case.

So that is a fairly broad overview of the Office of the National Cyber Director. Given the time, you know, I don't want to drone on for too long but happy to take any questions you guys may have about, you know, what we do, some of the things that we have going on and certainly who we're working with. So with that, I'll kick it around.

Mark: Does anyone have any questions for John on this new and exciting initiative?

Marcus: Yes. Marc Sachs here, private sector. John, thank you very, very much. I appreciate that. What are the opportunities for the private sector to help? And I realize the focus is largely on government, which is appropriate.

But, as you know, the vast amount of expertise and talent is out across the fruited plain and we would all love to help our government. Is there a front door I can point people to or is something coming soon that we could help with?

John: Certainly. So we are standing up a stakeholder engagement office for just that purpose. We want to make sure that we are open. We have an open relationship with the private sector and state and local but certainly the private sector. So, we're building an office for that purpose.

As you may know from a records perspective and from a management perspective and from an ethical perspective, it does take a certain level of staffing to make sure that these relationships and interactions with the private

sector can be efficient. And efficiency is necessary to be able to do it at a scale that we want to be able to do it. So we're building an office for that purpose.

You can reach out to us at press@ncd.eop.gov or engagements@ncd.eop.gov and one of our stakeholder engagement folks will respond and certainly sit down, and we'd love to hear from you.

Marcus: I appreciate that. I know there's a lot of people that are absolutely willing to help. And there's a good track record as you might be aware over the last 20, 25 years. So thank you. I appreciate that.

John: Yes, yes. Excellent. Thanks. It's a great question.

Mark: Does anyone have any other questions for John?

Sidonie: John, this is Sidonie from DOC. I really liked your briefing. What did you say your first effort was? I know your second was national cyber supply chain but what was your first effort again?

John: The first line of effort was federal cybersecurity.

Sidonie: Thank you.

John: Yes.

Sidonie: Thank you.

Mark: Okay. Anyone else for John? All right, John, thank you so much. Again I apologize for not being able to read my talking points but anyway.

John: No worries.

Mark: Good. Great briefing, and we appreciate your time to come over and talk to us this morning.

John: Excellent. Thanks, folks. You guys have a wonderful afternoon.

Mark: Thank you, John. All right. Now, we're now at the point of the meeting where we ask for SLTPS-PAC members to present any new business they may have. All right. Open floor. Anyone? All right. Hearing none, new business. All right. Do any other committee members have any questions or remarks before we close out today's meeting? All right. Hearing none, all right. Our next SLTPS-PAC is scheduled for June 15, 2022. We are hoping, and I've said this now for two years, to have the next SLTPS-PAC meeting in person, but we will also plan for having to be 100% virtual. As a reminder, SLTPS-PAC meeting announcements are posted in the Federal Register approximately 30 days before the meeting along with being posted to the ISOO blog. All right. With that, I'm going to

adjourn the meeting and thank you all for attending and please stay safe. Thank you.