HOMELAND SECURITY EXPERTS GROUP (HSEG)

2022 HOMELAND SECURITY ENTERPRISE FORUM

PLENARY SESSION 6:

FBI: MAXIMIZING COLLABORATION AGAINST OUR MODERN THREATS

Salamander Resort & Spa

Middleburg, Virginia

Tuesday, October 25, 2022

Plenary Session 6 - FBI: Maximizing Collaboration Against our Modern Threats

MS. MOUL: Good morning. I'm Sandy Moul, Executive Director of InfraGard National Members Alliance. And I wanted to congratulate Rob Walker, Secretary Chertoff, and Congresswoman Harman again for such a groundbreaking and thought provoking forum. I didn't know how you were going to top this year after last year, but you've truly raised the bar again. So, congratulations.

Today's session is about increasing collaboration against our modern threats and features two of the FBI's most dedicated leaders, past and present, who have personified the Bureau's motto of fidelity, bravery and integrity throughout their many years of service, Deputy Director Paul Abbate and former Deputy Director John Pistole.

The FBI has long been at the forefront of partnership, collaboration and information sharing. Since the attacks of 9/11, cultural change has increased that mindset across the workforce. With the ever changing threat landscape, how's the FBI adapting to meet current and emerging threats? Well, they certainly have a well-established history to look back on. Established in 1996, InfraGard is the FBI's longest running and largest public private partnership with over 85,000 members and 77 InfraGard chapters nationwide, each affiliated with a local FBI field office.

Twenty-six years ago, the idea of InfraGard was quite ahead of its time. But in the nearly three decades since, it's been proven that collaboration between the FBI and American Business Community is not just desirable, but essential to addressing the existential threats that have made their way onto our doorstep and into our homeland.

In my role with InfraGard National Members Alliance, which represents the private sector component of the InfraGard program, I can share that this mutual commitment between the Bureau and the private sector is steeped in our desire to protect our critical infrastructure, economic interests, technology and innovation, in short, the foundation of American life. As our team has personally experienced during his tenure, Deputy Director Abbate's commitment to public private partnership via InfraGard and other programs has been nothing short of extraordinary, and for that, we are very grateful.

And now, it's my pleasure to introduce your esteemed session moderator, John Pistole, dedicated 26 years of service to the FBI, retiring as deputy director in 2010. He focused extensively on national security and counterterrorism investigations. After the tragic events of September 11th, Mr. Pistole was put in charge of the FBI's greatly expanded counterterrorism program. In this role, he contributed to the formation of terrorism policies under both the Bush and Obama administrations. After returning from the Bureau, Mr. Pistole served as the administrator of the TSA for 4.5 years. And he currently serves as president of Anderson University, his Alma Mater, and returning back to his hometown.

Ladies and gentlemen, please join me in giving a warm welcome to Mr. Pistole and Mr. Abbate.

(Applause)

MR. PISTOLE: Well, thank you for the introduction. And it's good to be with you here. And it's great to see Judge Webster here live and in person as he was the FBI Director when I joined the Bureau in 1983.

(Applause)

MR. PISTOLE: I'm just curious if any -- if you worked for Judge Webster, either at the Bureau or Agency, anybody here else? Yeah, there's a few. So, yeah, so it is good. But Deputy Director Abbate, it's great to be with you here today.

MR. ABBATE: Thanks for the --

MR. PISTOLE: Thanks for taking the time out coming out to D.C. in the busy schedule --

MR. ABBATE: Thank you.

MR. PISTOLE: -- and joining us. So, as you heard, Paul joined the FBI in the late '90s. He came in through Connecticut. He was assigned first office New York, which is it's kind of a joke in the Bureau, if you put New York at number one is that's where you want to go, you've got a really good chance that you're going to get that and he did.

MR. ABBATE: It's a guarantee.

MR. PISTOLE: Yeah. It's a guarantee.

MR. ABBATE: It is. I locked it in.

MR. PISTOLE: Yeah. And so he was active doing criminal investigative work and on the SWAT team, and then went on, in summary, four to five other field offices which he led either as a supervisor or ASAC, Assistant Special Agent in Charge, or Special Agent Charge, SAC, or the Assistant Director in Charge, for example, SAC in Detroit, for Detroiters, L.A., and then WFL Washington Field Office before becoming the Executive Assistant Director of the Criminal Cyber Response and Support Services Branch of the FBI, and then the Associate Deputy Director, which is the number three person in the Bureau, before becoming almost 2 years ago being named the Deputy Director, the senior career person out of the 37,000 plus employees in the FBI, he's always the senior person, not appointed by the President.

So, it's great to have you're here. Thank you for your long service in terms of what you had been doing. What I thought I'd ask starting off, if you could just give us a kind of level set of what the Bureau is seeing these days in terms of the current threat environment, both domestically and internationally.

MR. ABBATE: Sure. I wanted to start similarly, by thanking everyone. It's -- it really is amazing to be here. And I feel privileged to share the stage with you, sir, someone who I've looked up to throughout my career into -- and particularly from this position now and aspire to be like. So, thank you for your leadership in the Bureau and beyond and to many friends and colleagues who I haven't seen for a long time. It's great to share some time with you. And then, again, to Judge Webster and his wife, Lynda, what an honor to be with you as well, sir. So, thank you for being here.

To the question. I am going to start by saying, in the work and the mission that we do and our outlook for the future, we're highly, highly optimistic. But when we look at across the threat landscape, everything that we confront each and every day as a community, counterterrorism, counterintelligence, cyber, weapons of mass destruction, I'm going to paint a bit of a dark picture here. Because I think in the last year or the last -- in recent years, what we've seen on the threat across all of those areas is really something that's becoming ever more complicated. We're seeing heightened aggression across the board on the part of adversaries. It's just incredibly complex, accelerated, increasingly unpredictable in the ways that it's coming at us in the vectors, so really, really difficult to deal with.

And I think it reflects our infinite adaptability as well. We, as a community and law enforcement and the intelligence community, are constantly working hard to meet these threats, stay ahead of them, evolve and adapt, but the adversaries are as well. And it comes down to like anything in life, it's a competition and we've got to work hard to stay ahead. And, again, I'm optimistic that we will.

So, let's go across the various disciplines. And we'll start with terrorism, in our work in countering terrorism. I think what several themes we see emerging in recent times there, one is technology and social media. We're still facing the constants of the large scale international terrorist groups like Al-Qaeda and ISIS. They haven't gone away. And I would say that, you know, based on the intelligence that we see every day, they're more intent than ever to strike us here and around the world and, you know, cause death, destruction, and harm.

But technology and the reach of social media has given them the ability to touch individuals and inspire individuals and radicalize individuals that they wouldn't have been able to just a few, you know, years ago. And that's created greater danger in the world as a result of that because now we're not just dealing with, you know, training and preparation and plotting and safe havens around the world and the deployment of operatives, but again, that reach to touch individuals here in the United States and around the world from afar and not have a direct connection with them, but cause them to seek and often commit tragically violent acts.

So, that's something that has confronted us more and more and that, you know, we've worked hard to deal with by deploying technology and leveraging that ourselves. We've also seen in the last maybe 2 to 3 years, a greater rise in the involvement of minors and juveniles in terrorism. And I think that is a reflection as well in the reach of social media and the impact in terms of radicalizing individuals at a lower age. That's becoming, you know, more and more so a real problem for us particularly with, you know, the limitations in dealing with minors, and especially at the federal level, given the constraints of our criminal justice systems. That's something we're, you know, working hard to find our way around and find solutions to. But there's no, you know, there's no easy answers there either.

We see the reemergence of what we'll call, you know, permissive operating environments or safe havens around the world. And a stark example of that is Afghanistan. You know, with the withdrawal of our military from Afghanistan, it's opened that country up to provide an area where elements of Al-Qaeda and even ISIS can operate freely and, again, have a haven where they can plot and plan to conduct operations, including here in the United States. So, we're very concerned about that as well. And at the same time, we have some degree of a loss of insight into what's going on there due to our resources being removed and the collection opportunities across the board that we would have as an extension of that.

So, the challenges within the arena of countering terrorism, I think, are greater than ever and the relentlessness of the enemy to try to strike, you know, is undeterred and I would say, greater than ever. So, those are some of the challenges in the world of terrorism, you know, on the international level. I think also cyber and technology is a part of everything. And that certainly has increased significantly just over the last few years.

As I mentioned, it is an element of -- that's being leveraged by terrorists to expand their reach and cause greater harm. But cyber itself as a vector is of, you know, increasing concern for us as well. It's being leveraged by nation state actors, as we know, like Russia, Iran, North Korea and China to commit espionage, economic espionage, more traditional espionage, to spread disinformation and malign influence in theft as well of -- from our corporations and, you know, within that the effect -- the underlying effect on our economy.

And then, ransomware, I think is becoming increasingly dangerous. It's reached a level and hit our critical infrastructure in ways that we hadn't seen previously. And there are a number of examples of that that we're all familiar with; Colonial Pipeline, JBS foods. And there's been attacks or attempted attacks on hospitals, emergency services, and elements of our society like that that have -- we haven't seen this, but actually bring to bear a potential threat to life scenarios that can impact public safety and people's life and health. We're very concerned about that as well.

And, again, that's a competition between us and adversaries to stay ahead of that, to put up defenses and to move to a preventative state, so we can stop things from happening in advance. And then on the counterintelligence front, again, cyber is an element of that, as mentioned. But I think we have a very illustrative example -- examples of that just yesterday when the Attorney General FBI Director announced a set of indictments and criminal charges against Chinese state actors in three different cases reflects some of the things that I've already touched upon, economic espionage, but also repression and human rights violations where the physical reach of the PRC and the Chinese Communist Party is extended here to our country where they're deploying operatives to work here to threaten, to harass, and intimidate people within our country, to force them to go back to China and to limit their speech. And we're seeing that from Russia as well, Iran and others. And, again, that's only increased and heightened in the current environment.

So, increasing violent -- increasing volume, heightened aggression, and just more across the board, and a hybrid combination of all of that creates a very challenging threat picture for us to meet. But, you know, we're working hard to step up and, you know, the theme of this collaboration is front and center. Each and every day, we're working hand in hand with our law enforcement and IC partners to counter all of these threats across the board.

We sit, as you know, sir, day in and day out, we have partners from the Department of Defense, NSA, Central Intelligence Agency with us 24/7 in our building, they're part of our work that we do every day in FBI headquarters. And likewise we have individuals at -- from the working level, the highest levels deployed, you know, within the walls of our partners as well. We're working side by side to move information, stay ahead of the threats, and we're doing that at the law enforcement -- on the law enforcement stage as well.

We were just out at the International Association of Chiefs of Police conference last week in Dallas. And we, you know, had, again, a reflection of the incredible partnerships that we have there with law enforcement working hard every day to bring that together and keep the country safe and protect people. And that's the bottom line. And that's our focus each and every day.

MR. PISTOLE: Yeah. Well, thank you for that comprehensive overview. Some people may be thinking, "So, I wonder what he does in his free time?" I think you answered that question. You go to conferences and talk about the things, all the good work that the Bureau is doing.

MR. ABBATE: Once in a while.

MR. PISTOLE: So, you've had the opportunity in terms of internationally to be deployed and be the senior liaison officer, agent for the FBI in Iraq. You've been the deputy on scene commander for the Bureau in Afghanistan. You are the on-scene commander in Libya, in this place called Benghazi. How has that helped inform your view of the world and the FBI's role in promoting things that we do here that the FBI does in terms of the rule of law and other aspects of the Bureau's mission?

MR. ABBATE: It reinforces some of what we've already touched upon. I think the partnerships, first and foremost, and we've talked about, you know, interagency partnerships. Those were certainly, you know, front and center in the work that I, you know, was privileged to do in each of those countries, again, with colleagues from Department of Defense, Special Forces, the Agency, NSA, DIA, among others. That's critical, and then extending to the international partnerships. I think that's a core part of our efforts within all of this as well that we didn't touch upon. Previously our work with allies and other countries and bringing that to bear against the adversaries across all the categories we talked about is just incredibly important. We couldn't do the work effectively without that.

MR. PISTOLE: So, just to follow-up on that, you've touched on some of the foreign adversaries around North Korea, China, Russia. How has Russia's invasion of Ukraine impacted the Bureau's work, if it has? I'm not sure people would think that the FBI has any role in terms of all of that. So, maybe you can help us to understand that.

MR. ABBATE: We do have a role in that. And I think it's part of the whole, but I think it's important. We actually, many may know this, but we were, you know, in partnership with other U.S. Government components. We're already very active and engaged in Ukraine. We have a legal Attache Office there that's well staffed. We were working very collaboratively with, you know, Ukrainian law enforcement and intel partners, with a particular focus on countering the cyber threat, which had, even prior to the Russian's invasion, had been coming at Ukraine, specifically from Russia over a number of years. And, you know, there had been a lot of damaging attacks from the cyber perspective even leading up to the invasion.

So, we were working hand in hand to, you know, share intelligence, to help them, to reinforce them, do training, send resources to help bolster their defenses along with other, again, U.S. Government partners. So, it's been more challenging now. We had to, as with other U.S. government personnel, move out, you know, the country for a period of time during the initial invasion. But we never gave up on that partnership and the support we along with others are providing to the to Ukraine.

And I think some of the biggest takeaways there. This is a reaffirmation of the importance and the role that the private sector plays. The private sector had really stepped up in regards to helping to provide intelligence and information on cyber to the Ukrainian Government to help put it into position to best protect itself. I can't stress that enough. And we already knew that. We already knew the importance of the private sector and really had doubled down on that, you know, for the Bureau reflected in our Office of Private Sector, in the work that we've done to continue to build those relationships and that trust, but it's really on display there. Without that, we wouldn't be seeing the resilience that has been sustained by Ukraine in terms of countering cyber because the fact is, even though we haven't seen hugely damaging effects, most of it has been, you know, physical ground war.

Ukraine did prepare and plan based on lessons learned from the past, with support predominantly from the private sector, but from other countries as well including the U.S. and made themselves very resilient and put -- and has continued to put up very good cyber defenses relative to what the Russian military government is throwing at them.

MR. PISTOLE: So, one of the key aspects of this conference and all the homeland security aspects, the Bureau works with DHS components across the board in so many ways. Yesterday we've heard from Ken Wainstein, the undersecretary for I&A, who's of course a DOJ, former U.S. attorney and the Chief of Staff for Director Mueller. Perhaps share with the group in terms of some of those interactions with DIH (phonetic) components, whether the operational components like TSA or CBP or any of the others, of course, FEMA, Secret Service, of all of these things that are part of the operations, if you will, in addition to all the other activities that DHS does. Maybe just talk a little bit about that from your perspective.

MR. ABBATE: DHS?

MR. PISTOLE: DHS.

MR. ABBATE: Yeah. I could spend a long time at that. We've got exceptional partnerships with DHS overall and with the components individually. Just a few you mentioned, CBP, just incredible work that's being done with CBP. The intelligence that -- I think this is underappreciated as well and I'm going to, you know, a huge credit goes to CBP. The intelligence that is being collected at our borders, ports and points of entry everyday by CBP is immense, and it's hugely valuable. And I think there's been a greater appreciation of that. Over time, we really tapped into that.

So, you know, traditionally it was leveraged more so in the criminal, traditional criminal world, but in post 9/11, countering terrorism as well, where we've seen that expand a lot is in counterintelligence. We're relying on partners and CBP to help us, not just take information that's passively collected and operationalize it, but we're working with them proactively to go out and do things that we've never done before to put us ahead of the game. And that's been extraordinarily helpful in the work that we do all around.

So, CBP, Secret Service, we have an incredible collaboration with Secret Service, especially in cyber, and especially on criminal cyber. We work hand in hand with them, you know, across all of our field offices within the cyber task forces. And that -- the efforts that we've done jointly on training and operationally, I think, have advanced our, you know, expertise and experience within countering cyber threats significantly. So, great credit goes to Secret Service as well on that.

Big picture, DHS, you mentioned Ken, you know, he's a great friend, and it's awesome that he's back in government now, leading intelligence and analysis. You know, we're talking, you know, all the time in terms of what are we seeing out there on the threat? You know, and what adjustments can we make within our respective agencies and across the departments to better meet the threat? So, that's a fantastic collaboration, you know, at the leadership level, and then down into the teams as well. And that's reflected importantly in the, you know, the products, the intelligence products that we're turning out to the private sector, to state and local partners as well to better inform them and to bring awareness to the threat that, you know, that we'll work together on as well.

So, and then CISA, you know, again, on cyber, a relatively newer component, but the work that we're doing together with CISA on the cyber threat is, you know, of the greatest importance as well, particularly with critical -- protecting critical infrastructure in the lead role that DHS and CISA has in that. So, we're working hand in hand there as well to keep everybody informed ahead of the threat, and then deal with things that come at us and on the occasion that they actually hit us as well.

MR. PISTOLE: So, following up on that, two other questions before we will go to a polling question to get your input as to what you believe the FBI's priority should be in terms of dealing with threats. So, we'll see that in a few minutes here. I'll give you both questions and if you want to weave them together, but one of the things the Bureau has been criticized for in the past has not been very good at sharing, whether it's intel or actual information or evidence in some cases with state, local, and tribal law enforcement. And so if you could talk a little bit about that?

And then the other side of that coin is the private sector and how the private sector can and does inform the Bureau in terms of work, and how the Bureau can work with the private sector to help accomplish the mission of the FBI and the 10 priorities.

MR. ABBATE: Sure. This is something that is an enduring challenge. It's something that we think about and focus on day in and day out. And even with all of that, and we've built an, you know, from your days, and many of you, we've built an incredible apparatus across government to focus on sharing information intelligence in the most robust way possible to make sure that there are no gaps or seams and that nothing is missed. And in spite of all of that, we know, you know, sadly, in certain instances, that things are still missed. Things don't get past. Mistakes are made.

We can never -- we've always got to learn from those mistakes. We've got to take the lessons and apply them. And you can put as many policies and processes in place to underpin all of this which we have. You can do the exchanges of personnel redundantly as we have. But I think it comes down to relationships in learning. And you've got to stay focused each and every day. And what we talk about in the Bureau is, particularly when a mistake is made, and we have the lesson learned, you know, what do you have? It's a question of commonsense and judgment at the most basic level. What do you have and who needs it, and then getting it to them with urgency. And that's an absolute requirement when its threat related information, and especially when it bears on harm to human life. That's the bottom line.

So, we -- we're constantly reinforcing that. We're constantly talking about it. It's the way we've built, extended the -- what you put in place with, you know, Director Mueller and other colleagues at the time. We still get together, this is for the Bureau, we still get together each and every morning early, though it's a little bit later than when you were there. We now get together at 8:00 a.m.

MR. PISTOLE: The day's half over. Come on, 8:00?

MR. ABBATE: I know. I knew you'd be disappointed.

MR. PISTOLE: Yeah. I'm glad to hear that actually, so.

MR. ABBATE: But we still get together each and every morning. And I think this is really important. This reflects the discipline and the focus it takes because people still say to me, "Hey, can we take a day off? You know, can we just do Monday, Wednesday, Friday? Like why do we have to get together every morning every day?" And then actually we get together at the end of the day too.

MR. PISTOLE: Yes.

MR. ABBATE: We still get together with Director Wray at the end of the day, with the team. And I do -- I close out with the team as well. I think that's really important because it reinforces everything that we do. We're talking about the threats, the intel, the issues facing us. We're ensuring that the right people have that information within the FBI, within the field, which is the frontline where the work is done, and then within other agencies as well who need that information to best protect our country and everyone. And we can never go away from that. I don't care what anyone says.

And, again, that comes down to relationships and it comes down to discipline and it comes down to focus. And you mentioned before, you know, experience overseas. I think one thing in countering terrorism, but this applies to everything, we can never be complacent. We have to fight that every day. And I think there's a natural pull toward that, it's human nature. But we have to reach down deep to avoid complacency each and every day and everything that we do in this business because it is about life and/or death.

And we also have to use our imaginations effectively to think about not just what happened in the past, but what are the possibilities in the future and how are those adversaries, the people that want to harm is going to come at us and try to get ahead of that, so bottom line.

MR. PISTOLE: So, in my early days of my career, I was fortunate to be assigned to the New York Office, my second office. I did not put my hand up for that, but no cost of living differentials and everything. And I remember the realtor laughing at me. He said, "They can't send you here making $28,000." I said, "Well, they did." And so here we are back in the day. But I was assigned to a joint Organized Crime Task Force and there's no way we could have accomplished what we did in the Federal System, Federal Courts, but for the involvement of the NYPD on the task force.

So, obviously, the JTTFs have greatly expanded since 9/11. But there's all types of task forces, again with state and locals and other federal agencies, some of which are represented here. Maybe just touch on that, and then the private sector.

MR. ABBATE: Sure. And as you noted before, it's -- we're upon the 40th anniversary --

MR. PISTOLE: Yeah.

MR. ABBATE: -- of the first Joint Terrorism Task Force in New York City. So, that's a pretty momentous occasion. But that model has really been adopted and taken across the other disciplines and into the other programs just in recent years, recognizing how effective it's been at bringing everyone together, again, breaking down those barriers and obstacles, allowing the sharing of intelligence and the work together out on the frontline.

We now have -- much like we do with the JTTFs, we now have cyber task force in each of the 56 field offices and beyond that, bring together, you know, the cyber experts, agents, analysts, and then incorporate state and local officers, detectives as well, and then other federal partners. You know, we wouldn't be able to effectively do the work in countering the cyber threat without that. And then even going beyond that, on counterintelligence, we now have counterintelligence task forces in each and every field office as well that incorporate all of those partners as well.

So, the model, which has proven so effective and successful over the years on meeting the terrorism threat has been adopted into the other programs and it's being just as effectively used there as well.

MR. PISTOLE: Yeah. Good. And then private partnerships, private companies that work with the Bureau to accomplish roles, maybe just touch on that briefly.

MR. ABBATE: Yeah. We have, as you know, an office of private sector which reflects our commitment to that partnership. And, again, I go back to what we've seen in recent experience. And now it has been proven, the Ukraine example. The private sector holds, you know, owns the bulk of the infrastructure and critical infrastructure within our country and beyond. So, they're on the frontline in terms of receiving the threat. And then also by virtue of that, they have the information and the intelligence that's reflected in that. And it's got to be a two way street there as well.

So, we've worked hard within that to build the private public collaboration. We've gotten many representative, associations, and groups that drive that from DSAC, InfraGard, some whom the leaders of that who are great friends are here as well. We know how important that is. And I think that's earlier in its evolution, actually, in many ways than the inter-governmental and even international relationships. But we're working hard to catch that up. And I think a lot of progress has been made. Some of the issues and challenges that I've heard raised, you know, over the last decade, earlier on, I don't hear as much now. I think we've really leaned forward, you know, at least from the FBI standpoint. We're really pushing as we have done within government share, you know, share information intelligence to (inaudible), lean forward, you know, reach beyond. And we've got to keep that in focus as well. And that comes down to, again, building the -- building relationships with private sector partners, and then building the trust and credibility with each other, and then having -- it's got to be mutual.

Again, it's a two way street. We each from government and from the private sector have something to offer each other. And we can't, you know, achieve the highest levels of what we're trying to accomplish without coming together and being open with each other in that way.

MR. PISTOLE: Yeah. So, let's go to our poll question. As we're looking at that, one of the things I picked up on is, how much things have improved at the Bureau in the last 10 years or so? No correlation, of course, to my departure, but it is good. So, here are the questions. The one question, what do you believe should be the FBI's top priority for the next, not the top three, not top five, Bureau has got 10 priorities, but what do you see? And then we'll go to -- we'll have time for some brief questions from the audience, I believe.

UNIDENTIFIED SPEAKER: John, while -- while the poll results are coming in.

MR. PISTOLE: Yes.

UNIDENTIFIED SPEAKER: -- if I can go ahead and pose, I know we're running short on time here.

MR. PISTOLE: Yes.

UNIDENTIFIED SPEAKER: Deputy Director Abbate, we have a virtual audience who's attended and I want to keep them engaged.

MR. ABBATE: Got it.

UNIDENTIFIED SPEAKER: I'm going to weave two questions together here. One asks how are nation states specifically operating to turn Americans against one another with the goal of distraction, implosion, internal aggression, et cetera? And then the follow up, the corollary to that is, how are they using our Internet of Things against us, our smart speakers, et cetera? Is that a factor from the cyber side that you guys are seeing?

MR. ABBATE: On the first piece, we know there's been numerous examples, some of which, you know, we've brought criminal charges in regard to where nation states; Russia, China, Iran, North Korea, I'll call them out, again, are, you know, leveraging the internet, social media to spread disinformation and malign influence in order to affect the thinking of, you know, the U.S. population in our society.

So, you know, we've worked -- we understand that now. And we work hard again with partners. Example of our work is the foreign influence task force, where we're looking out to identify efforts by adversaries to conduct that type of activity, and call it out or work with, you know, private sector companies in social media and technology to give them the information. This is example of the public private partnership. We're sharing information over time now much more so when we have it to inform private sector action based on their terms of service, and rules to not those bad actors off of the platforms and take that out of -- out of play.

On the Internet of Things, that's certainly something that we're focused on how that could potentially be weaponized. There's a lot of concern about that. I wouldn't say, you know, that we've seen a lot of reflections at this point of it actually happening on a -- on a large scale. We are concerned. One thought I have within that though is what we call ubiquitous technical surveillance.

So, that's, you know, use of leveraging of technology against us by foreign adversaries, like the ones I mentioned. And when it comes down to conducting our operations, investigations and things like that, we're always on the look at -- lookout for that because I think there is the risk and it's been demonstrated that adversaries can tap into devices, in your place of work, in your home, though. You know, obviously, in the workplace, we have security guard, you know, protocols and stuff around that to prevent that from happening. But it's something we have seen attempts to leverage that or actually instances where it has been used against us. And we are very concerned about the further expansion of that and the weaponization of other devices across the board.

MR. PISTOLE: Questions from the audience? Maybe one or two brief ones, I think. Anything? There's one back there. If you could identify yourself, please?

MS. MARTINEZ: Hi, this is Didi Martinez with NBC News. I had a question. It was brought up briefly in the session yesterday about DBEs, and particularly January 6th, how social media has created the landscape where people are their own cyber sleuths. We saw people submitting tips, some of them false, some of them turned out to be legitimate.

Can you talk a little bit more about kind of the FBI's role when it comes to strategy and, you know, disseminate between this massive information dump online and following up and also debunking, I guess, like false tips? Thank you.

MR. ABBATE: We --

MR. PISTOLE: I'm glad you've got that one.

MR. ABBATE: Look, I think the thing here is we have to be disciplined in the work that we do and keep our focus and it's all about the facts. So, you know, we have a national tip line that we run out of our CJIS Campus in West Virginia. It's called our public access line. We get -- I'm always stunned by this, but we get nearly over 4,000 calls per day. It's a huge volume. This is individuals from the public phoning in or sending in e-tips.

So, it's a massive amount of information for the teams which are in the hundreds out there to sort through day in and day out and discern what's an actual threat and what isn't. But they're trained and they have developed an expertise in that and they're very effective of going through that, you know, leveraging the information that we have and combining it with other things. They're very good at assessing, you know, callers and, you know, what's coming across on the line.

It's a combination of a lot of skills to boil it down to what really matters because at the end of the day, we can't afford to miss anything when it comes to preventing violence. And they do that very effectively. And, you know, we have -- one of the things I always think about, I wish the public knew more is how many, I'll call them success stories, but there are so many instances that have occurred out there where we've received calls, and we've been able to act rapidly and get the information out to our field offices or state and local partners and intercede and prevent somebody from committing an act of violence in a lot of different forms and in a lot of different levels.

I don't think the public is aware of that, as I wish they were, you know. It's just -- again, I think that's a reflection of the volume, but it goes back to discipline and the facts. We're not into policing thought or ideology. We're focused on, is it a threat of violence? Is there potential violence associated with the complaint, or the call that's coming in? And then getting in front of that and then moving that information out quickly to those on the frontline, who are going to action it and get in the way of, you know, preventing something bad from happening. And we're doing that all day, every day with our partners, and we've done it very effectively, but we can never lose focus or take our foot off the gas. That's the bottom line.

MR. PISTOLE: Well, I think we've run out of time unfortunately. So, let's give a warm thank you to Deputy Director Paul Abbate.

(Applause)

\* \* \* \* \*