U.S. Department of Homeland Security
Homeland Security Advisory Council Public Teleconference Call
Subcommittee Progress Update
February 28, 2019

Executive Summary
2:00 p.m. to 4:00 p.m.

The open session of the Homeland Security Advisory Council (HSAC) meeting was convened on March 15th, 2016 from 2:00 p.m. to 3:30 p.m. via teleconference call. The meeting was open to members of the public under the provisions of the Federal Advisory Committee Act (FACA), P.L. 92-463 and 5 U.S.C. § 552b.

The following individuals were announced on the call:

HSAC Members:
Judge William Webster, *Chair*
Commissioner William Bratton, *Vice-Chair*
Thad Allen
Keith Alexander
Frank Cilluffo
Donald Dunbar
Paul Goldenberg
Michael Jackson
Jim Jones
Cathy Lanier
Carie Lemack
John Magaw
Jeffrey Miller
Wendy Smith-Reeve
Robert Rose
Ali Soufan
Paul Stockton
Chad Sweet
Karen Tandy

Operator:
Ladies and gentlemen, thank you for standing by. Welcome to the Homeland Security Advisory Council Meeting. During the presentation, all participants will be in a listen-only mode. If anytime during the conference you need to reach an operator, you can press star-zero. As a reminder, this conference is being recorded, Thursday, February 28, 2019.

I would now like to turn it over to Mr. Matt Hayden, Executive Director of the Council. Please go ahead, sir.

Matt Hayden (HSAC Executive Director):
Good afternoon everyone, and thank you for joining us today. My name is Matt Hayden. I'm the Executive Director of the Homeland Security Advisory Council. I'd like to welcome the HSAC members, as well as the senior leadership from the Department of Homeland Security; so specifically the Secretary Kirstjen Nielsen, and other participants on the call this afternoon.

This meeting is convened pursuant to a notice that appeared in the Federal Register on February 8, 2019.

As a way of background, the Homeland Security Advisory Council or HSAC is a federal advisory committee at the Department of Homeland Security. Under the Federal Advisory Committee Act, or FACA, these meetings are open to the public. The executive summary and meeting minutes will be posted on the DHS Website at www.dhs.gov, and the public FACA database within 90 days of today's meeting.

This council is the Secretary's go-to group of senior advisors, the kitchen cabinet so to speak. She relies on all of you to provide candid feedback and to provide a vehicle to allow any fresh ideas.

At this time, I would like to turn it over to the Chair of the HSAC, Judge William Webster.

William Webster:
Good afternoon and thank you, Matt. My name is William Webster, and I am Chairman of the Homeland Security Advisory Council, or HSAC as we call it for short. I hereby convene this meeting.

This is a public teleconference call of the Homeland Security Advisory Council, and we appreciate those members of the public, the government, and the media who have joined us.

I also would like to welcome the members of the council and the members of the subcommittees who are on the call today. I appreciate all of the hard work that the subcommittees have invested into their taskings which was established by the Secretary on October 4, 2018.

It's my pleasure to introduce Secretary Kirstjen Nielsen. She is the sixth secretary of the Department of Homeland Security. She was sworn in on December 6, 2017.

The Secretary has been engaged with the council and we look forward to continuing working with her and the department senior leadership.

On October 4, 2018, Secretary Nielsen tasked this council with four taskings; to provide the secretary and senior leadership with findings and recommendations on the following topics; CBP, families and children care panel, countering foreign influence, emerging technologies, and state, local, tribal, and territorial cybersecurity.

Thank you again to all for joining us today. Madam Secretary, the floor is yours.

Secretary Kirstjen Nielsen:
Thank you Judge Webster. Greatly appreciate the introduction. Commissioner Bratton, and fellow HSAC members, thank you always for your service, and thank you for joining the call today.

I also want to thank the members of the public who have joined us on today's call.

Before I begin, I want to quickly welcome General Keith Alexander to the council. He is no stranger to those of us on this call. We are thrilled to have him join us. He was appointed to the council this past December. And thank you general for joining us. We are - we know we will benefit from your years of experience, as well as experience from your current post at IronNet Cybersecurity. So thank you very much for joining.

So I thought what I would do is just give you few updates of major moving pieces, things that have happened. And then I'd love to just spend the time answering any questions that you might have.

So quickly, as many of you know, the president did sign into law the Homeland Security Funding Bill for 2019. We were able to get an increase in the overall budget, over a billion, which brings us to about $49.4 billion to secure the homeland.

Within that money, we did receive $415 million to help us address the humanitarian crisis at the border. So that will help us with medical resources, the triage, and our ability to provide basic necessities to migrants coming across the border.

$570 million for specialized equipment, non-intrusive inspection equipment at our ports of entry so that we can scan for drugs and other illicit materials.

We did receive money for the Coast Guard Polar Security Cutter. And thanks to those on the call who have been supportive of not only the Coast Guard, but their very important mission in the Arctic.

We received new funding for the Cybersecurity and Infrastructure Security Agency. We received additional funding for computed topography machines at the airports, which as we all know is a monumental step forward in technology for our detection.

We'll have a record level of personnel in the Secret Service. And then we also had an increase in $5.4 billion for available funding for major disasters. So we're about to start the next fabrication cycle. And we will keep you posted on that.

I just got back from El Salvador last week, I'll be headed out to Honduras in a couple of weeks. I've continued my efforts both on a bilateral and multilateral strategy to engage with the Northern Triangle in Mexico to help address what we've talked about in previous calls the push factors if you will, not only making sure that we as a region strategically protects vulnerable population as soon as possible in their travel, but that we also increase security throughout the regions to combat trafficking of people, gangs and trans-national criminal organizations.

I'm happy to report that we are on track to sign the regional compact next month in Honduras that I have described to you previously. This will be the first regional contract of its kind. But it's a recognition that these challenges that we face are in fact challenges throughout the region, not just within the United States or one of the countries. So we are excited about that progress.

I just returned from California where we are continuing our conversations with the private sector and other government partners from throughout the world on careless use of the internet. We also took the opportunity to talk to our private sector partners about foreign interference, and also about child exploitation and the need for additional technological solutions to help us combat both of those.

We did announce earlier this week the first summit on tariffs and prevention that DHS will be hosting later this spring.

Also excited about this will be the next steps in our retooling our approach to counterterrorism. You've heard me say before that hate is hate and violence is violence. We are trying to ensure that we have a comprehensive approach to combat all types of terrorism that appear or threaten - appeared in the United States or threaten Americans. So more information on that to come.

Before we have that event, we will be issuing our first counterterrorism department-wide strategy. And again, the concept there is to bring all we have at DHS in an integrated fashion to really look at the new and emerging threats within the terrorist sphere.

Finally, we are - we'll shortly issue another first, which will be our first strategy to combat human trafficking, child exploitation, force labor. We work very closely with international partners and our partners within the federal government, as well as state and local partners.

But this continues to be something that plagues all of us throughout the world. So we look forward to putting additional focus on that and having a strategy to lead us forward.

And so let me stop there. There's probably a lot more that I could say, but we'd love to get to your questions, what's top of mind for you, and then we can go from there.

So Matt, perhaps if we could turn it to you for questions.

Matt Hayden:
Yes, Ma'am. Thank you, Madam Secretary.

At this time, are there any HSAC members who would like to ask a question?

Chad Sweet:
Madam Secretary, this is Chad Sweet. Congratulations again on this historic agreement in the Northern Triangle. And I know right now, you've achieved what no one else has with the principles that have been agreed.

And could you elaborate on in terms of the actual final documentation that's coming? You mentioned the rough timing. When do you anticipate the HSAC getting a briefing on that in more detail once you're able to do that?

Secretary Kirstjen Nielsen:
Yes, thank you for that. I think what I'd love to do is to give you a full briefing now. But as you know, there's some sensitivity to the international negotiations.

So probably if I could, and Matt, maybe you could help us schedule a call shortly after we sign it in Honduras, which I believe is the 27th of March, then we could schedule a call and then I could give you some details.

But in the meantime, Matt can provide you with the readout we are able to provide, and then of course the moment we sign it, we're happy to send you a summary before we do the call, so that we can make sure to keep you up to date.

The strategy currently that is we will sign this with Honduras, Guatemala and El Salvador, and then we will work with Mexico to bring them on board. I'm meeting with some of my counterparts actually later today. So we look forward to their joining the compact.

And then we have begun discussions with the Southern Triangle, with Colombia, Costa Rica and Panama. We'll all be travelling in a couple of months here in April to meet with them and to get their cooperation and make sure that we can strengthen the partnership there as well, so that we truly at that point have a regional approach in the Americas.

So thank you for everyone on this call who's been supportive of this effort. We really look forward to working on these issues in a concerted way with our partners in the South.

Chad Sweet:
Thank you, Ma'am.

Matt Hayden:
And we'll take that for action. Any other questions on the line?

At this time, if there are no further questions, we'll - the Secretary has to proceed to meet with her counterparts, and we will thank you, Ma'am, for your time today, and we will proceed with the subcommittee readout.

Secretary Kirstjen Nielsen:
Matt, thank you. And I just - I want to thank everybody. I'm going to be able to stay on the phone for a little bit here. I'd love to hear some of the readouts.

The ones that I missed because of our partners who have travelled up here, I will be sure to follow up immediately. But I can't thank you all enough for your dedication working within these working groups. I really look forward to your insights and actioning what you have learned and recommended.

So thank you in advance. But Matt, I'm going to stay on as long as I can to hear some of the readouts.

Matt Hayden:
Thank you very much, Ma'am.

At this time, we'll hand it over to Karen Tandy to lead the subcommittee on CBP, families and children care.

Karen Tandy:
Thank you, Secretary Nielsen, Judge Webster, and Former Commissioner Bratton. It is a pleasure to chair this committee of now 10 members.

We expanded the committee to include a practicing pediatrician who is also a member of the UNC faculty, and is a national expert on sexual exploitation and maltreatment of children. So that brings our committee to 10.

Secretary Nielsen, you tasked us in early October specifically with conducting site visits to observe the operating environment of CBP and to study the care of individuals and children in short term custody to assess best practices for the care of children and families, also best practices of law enforcement in their interactions with this population, and then lastly to recommend changes if any to CBP policies, procedure, training involved in the custody of families and children.

So with that tasking, the committee has undertaken a substantial amount of work since October. We've had one full day of briefings, three other briefings, notably the commissioner of CBP and the head of the Border Patrol briefed the committee following the tragic death on December 8 of Jakelin Maquin.

The briefing included, with no holds barred, everything involving the timeline and steps taken. And that briefing was followed with other briefings to the committee by DHS and Customs and

Border Protection medical ops teams, as well as a congressional briefing on proposed legislation on the medical care and custody standards for our families and children.

The committee has reviewed additional materials, rather, substantial additional materials, ranging from two GAO reports, three DHS IG reports, another HHS IG report, all involving this topic, as well as the data on the flows and processes and policies regarding this topic, as well as various legal opinions, agreements, and multiple congressional hearings.

So with that, I would say probably the most important piece of the tasking has been the site visits.

So the committee of 10 by the end of this will have attended border briefings and site visits on the border to include six of the nine border sectors. And geographically, it will include all of the states that are on the Southwest border.

Notably, the committee has been on one of these border site visits, which was in December, to the San Ysidro Port of Entry; and the San Diego, El Centro, and Yuma Sectors.

And the next two site visits that are scheduled occur starting next week and the following week. Next week will be to the Rio Grande Valley sector in McAllen and Laredo, as well as to an HHS shelter in Brownsville.

The week after that, the committee will go to the El Paso sector to include HHS shelters in that sector, as well as to New Mexico, to Santa Teresa, as well as to Lordsburg.

In each one of these border visits, the committee has and will be meeting with stakeholders and NGO groups, and focusing on the tasking and the operational environment that CBP is operating in.

I would say it's too early, despite the amount of work that the committee has undertaken and the site visit thus far, it is too early to provide recommendations on policies, procedures and training.

However, from the material and briefings and the Southwest border trips to San Ysidro and the Yuma Sectors, I will say that certainly the initial observations from the bipartisan committee is that this is both a border and a humanitarian crisis. It emanates from the immigration shift from predominantly single adults to an almost 300% increase in unaccompanied children and family units that are crossing illegally between the ports of entries.

So this is squarely in the domain of the Border Patrol because it's occurring in between the ports of entries for the most part.

Also, as an initial observation, it does appear that the system, the immigration system is overwhelmed and fractured at every critical point. The indications of this include - we have

observed substantial segments of the Border Patrol enforcement agents who have been diverted from enforcement work to addressing humanitarian needs.

There is insufficient manpower, insufficient funding, inadequate holding, and detention facilities for this new population of families and children, delays in transportation once these families and children have been processed by the Border Patrol, delays in transportation to move them to the next stage, a strain on NGO shelters, a three to five year case backlog of asylum claims, and at the heart of all of these are the children.

Due to court decisions that have imposed 20 day limits on detention of families and children, children have become the tickets to cross the border, and they have become the tickets to release into the U.S. And as a result, our initial observation is an increase in fraudulent family relationships, and significant endangerment of children in the journey to the border and in crossing border

I think the most significant example of this, more glaring, was in the Yuma Sector. At 3:00 in the morning when we were there for our site visits, so mere hours before we appeared, there was a group of about 36 immigrants who were very near a port of entry, the San Luis port of entry. Instead, as a result of the smuggling organizations, they made a difficult 3:00 a.m. crossing of - illegal crossing of the border.

And we saw the video of that crossing. And there were children who were being forced through coiled razor wire as part of that dangerous crossing. And this is a classic example of the humanitarian need, the diversion of Border Patrol manpower to address these needs and significant endangerment of children.

What was striking, finally, in my last note - what was striking is that it was a short walk to the port of entry where there was no delay, such as been reported elsewhere - there was no delay in what could have been a safe crossing to present an asylum claim.

Thank you. That concludes the interim report of the committee.

Matt Hayden:
Thank you very much Karen. At this time, I will pause for any HSAC questions or any comments to share.

All right. At this point, hearing none. We'll rotate to the countering foreign influence subcommittee. And Ali Soufan, if you're available, we'll go ahead and start there.

Ali Soufan:
Yes. Judge Webster, Commissioner Bratton, fellow HSAC members and Secretary Nielsen, if you're still on, I am honored to provide a brief report on the progress of our counter-foreign influence subcommittee. And on behalf of all my colleagues in the subcommittee, thank you for this opportunity.

This import outlines where we are at the CFI subcommittee on delivering on the tasking by the Secretary. The taskings are basically to produce recommendations for the Homeland Security Advisory Council, and from there to the Secretary on the evolving range of foreign influence bets against the United States, and identifying additional opportunities to counter them within DHS.

As background, the tasking from the Secretary includes but not limited to three different areas; identify DHS entities, headquarters, and component level, that currently or could have capabilities to counter foreign influence, threats.

The second one is to provide recommendations on how DHS can best use its resources and authorities to actively counter foreign influence threats, as well as enhance the nation's preparedness for the support and resilience of such dangers.

And third, provide recommendations on how DHS could organize itself to prepare for and to respond to future foreign influence campaigns, in what ways the department should engage with government and non-governmental stakeholders, and on how to ensure proposed DHS activities fit into the wider U.S. government architecture for countering the foreign influence.

The recommendations - sorry, the tasking team after our September 18, 2018 HSAC meeting. And to date, our subcommittee members have held one in-person meeting and three conference calls. Throughout March and April, the subcommittee will have one additional in-person meeting and multiple conference calls.

So far, the subcommittee members had opportunities to look into different research and have in-person presentations on how foreign influence, and disinformation campaigns are being used as a tool of warfare, which does require direct act of violence, but has real potential of influence, and real potential of even disrupt society, business and politics.

At our November 14, 2018 in-person meeting, our subcommittee members have the privilege of being briefed by a number of individuals with expertise pertaining to the topic of foreign influence. Some of the main takeaways from the briefing includes one, the interconnected nature of media and digital literacy along with cyber hygiene, and how these factors into building long term resilience against foreign influence and disinformation campaigns.

Two, viewing foreign influence or disinformation through the lens of specific incident, such as the 2016 general election, does not encapsulate the whole scope of effect from such foreign influence and disinformation could be seen as a continuous, relentless assault rather than a series of targeted event-specific campaigns. It is important that the subcommittee look further into this reality.

Three, also as part of our meeting, the in-person meeting, we found out that there is no organization in the U.S. government in charge of coordinating efforts against foreign influence

such as countering misinformation, establishing the threshold, and building long-term competitiveness.

Four, when it comes to Homeland Security, DHS, the Homeland Security Investigations, HIS, has the global footprint and potentially the capacity to counter the threat of disinformation. For example, through their cybersecurity unit, but has not yet been tasked with this and lacks appropriate resources.

Other than the one in-person meeting that we had, the members of the subcommittee went through materials that were provided to us and outside research from outside DHS. And through that, we have some important findings that includes that the threat of foreign influence expands and evolves with technological advances, with the most recent threat of deep stage being an example. It is vital that we look more into this and become more familiar with the opportunities and challenges technology pose.

And the other elements that we concluded out of the research, since no actors seeking to destabilize the U.S. with the same objective, it is important to further understand each actor's goals and methods in order to give better recommendations to help advice the Secretary and devise an effective strategy for countering attempts at foreign influence.

The subcommittee is also looking in the current capabilities and resources within DHS entities, and the wider U.S. government to counter foreign influence.

Going forward as mentioned earlier, our subcommittee members are scheduled for at least one more in-person meeting and several conference calls throughout March and April.

Most research emphasizes a multi-disciplinary approach to counter any foreign influence which includes government organizations, legislations, technology advances, tech platforms, responsibility of the companies, education and civil society engagement.

As such, the CFI subcommittee members have identified several areas to partner with where we are in need of clarification in order to produce effective recommendations.

I'll give three examples for three different areas that we will continue to look into. First, legislation, second, responsibility and assignment, and third, subject matter expertise.

As when it comes to legislation, we are really interested in researching further all the different and current legislations that address the threat of foreign influence. Do these legislations include bringing in and engaging outside platforms, private actors, civil society in the CFI efforts? Are there any substantial gaps in the current legislations, responsibility and assignment? Is there any entity in the U.S. government that has capacity and has been tasked with coordinating and overseeing counter foreign influence effort across different actors? Who and what department or agencies within the government have been tasked with countering different aspects of foreign

influence and disinformation? And which government entities ultimately responsible for countering disinformation campaigns?

The last point that we are still looking into is the subject matter expertise. The CFI subcommittee members will also receive additional briefing by private sector and tech platforms.

We also reached out to some folks at Madison Avenue and Silicon Valley in order help us better understand how these platforms can be engaged in raising public awareness and building resilience against foreign influence and disinformation campaigns.

Thank you very much.

Matt Hayden:
Thank you very much as well. And at this point, is there any question from the HSAC members?

Paul Stockton:
Ali, this is Paul Stockton. That was as terrific briefing. Congratulations on the progress that the CFI team is making.

Have you considered the possibility of also including for analysis the recently revealed cyber command activities to suppress CFI campaigns at their origin, that is to cut off internet access by internet research agency as they were preparing to launch attacks against the 2018 election?

Ali Soufan:
Well Paul, thank you very much for your question, and thank you for your help and assistance on the subcommittee. I think that's something that we are definitely interested in knowing more about and we try to coordinate a brief on this with Matt and Mike to have more understanding for what's coming.

Paul Stockton:
Thank you.

Ali Soufan:
Thank you.

Matt Hayden:
Any additional questions?

Hearing none, we're going to go to the emerging technology subcommittee. I'll introduce Mr. Thad Allen and I believe Cathy Lanier as the Vice Chair is also available.

Thad Allen:
Thank you very much. This is Thad Allen. Thank you for the opportunity to brief the progress of our committee.

We're going to provide a brief overview. We have - we were given six areas to look at by the Secretary. They included UASs, 3D printing, artificial intelligence, machine learning, gene editing, robotics, and quantum computing.

With the interruption with the shutdown and other issues, we have been able to start to address the first four. We remain to be focused on robotics and quantum computing, and that will follow our work continues.

We prepared some slides for the information of the council.

I would just add the caveat, these are representation of some of the issues we're uncovering for the purpose educating the council, and not intended to be comprehensive, and that will be developed further. We have a much larger body of work that drills down significantly under these areas.

But I wanted to give an update on behalf of the committee and then offer Cathy Lanier an opportunity to add any comments she may have.

So let me first start with unmanned aerial systems. This is a very complex situation that involves everything from technologies, local tactics, the procedures to deal with threats, to evolving uses of drone technology from both the threat standpoint and an opportunity standpoint from the department.

The most significant event that's driving this was the recent FAA reauthorization that provided new authority to the Department of Homeland Security, and was under the Preventing Emerging Threats Act of 2018 as part of the FAA Reauthorization Act.

And it basically authorizes DHS and DOJ personnel and their missions to detect, identify, monitor and track UAS without prior consent, warn the operator of the UAS including by electromagnetic means, disrupt controls, seize control, or confiscate the UAS without prior consent and use reasonable force to disable, damage or destroy the UAS.

Within DHS, the legislation authorizes the department to protect what is called cover assets and facilities based on certain missions and criteria, and they would include Customs and Border Patrol and U.S. Coast Guard security and protection operations, including the security of facilities, aircraft and vessels whether more or less.

It also include U.S. Secret Service Protection Operations, and U.S. Federal Protective Service Protection of Government Facilities.

The statute also enables each resources to be used for national security events to support state and local territory and tribal law enforcement of entities, protection of active federal law enforcement investigations, emergency responses, and security operations.

Regarding covered assets of facilities, it must be related to the missions of the agencies I just enumerated, and must be located in the United States including territories and possessions, territorial seas and navigable waters, and identified by DHS and/or DOJ in coordination with the Department of Transportation as a high risk or potential target for unlawful UAS activity through a risk-based assessment designated by the DHS Secretary and/or the Attorney General.

Now, that is a mouthful. And even having multi-level conversations moving forward regarding the UAS threat, at the very top, it is the development and implementation of policy related to the new authorities, and that's being led by the Department of Homeland Security by the Assistant Secretary for Policy, with the support of the general council.

Ultimately, this is going to have to be distributed for implementation regarding doctrine and practices at the components of DHS that will be involved.

In regard to the committee and what we are doing, we are looking at the following areas that are provided in the slides, that were provided in advance with the briefing; including looking at UAS threats that would include interference with normal operations of commerce, traffic, construction and so forth, intelligence, surveillance and reconnaissance, weaponization, the ability to carry and dispense a wide variety of payloads, and use of UASs as smuggling conveyance.

The significant impact of these can create economic impacts, pose a physical hazard to other aircrafts, put critical assets at risk and facilitate elicit trafficking across borders.

But we intend to evolve the discussion on UASs and present our advice to the Secretary regarding control communication, policy implementation. We intend to engage the various DHS components, and provide further recommendations regarding how this might be implemented at a local level, with significant coordinating issues regarding state and local authorities.

And specifically on the northern and the southern border, you're going to have an international airspace environment which will pose complications as well. But as I said, this becomes a work in progress.

Regarding 3D printing, we're looking at areas such as the sabotage of safety critical parts where you might have malicious modification of digital build files, untraceable weapons, the ability to actually spoof biometrics and prosthetics, for instance fingerprints, what kind of threats may exist in the supply chain, and the implication of counterfeit intellectual property theft by scanning or taking design files that can replicate high value goods.

Our biggest concerns are new untraceable weapons, the ability to catastrophically disable critical systems, and loss of economic value in industry and credibility based on sabotage or counterfeit parts, and finally the overall impact of the U.S. economy by the implications of 3D printing.

Regarding artificial intelligence, we are concerned across a number of areas. And frankly, artificial intelligence and machine learning ultimately relate to advances in computation and apply to almost any threat screen we're looking at including UASs where we will need the capability and capacity and the ability to defeat mitigation systems.

Some of the areas in artificial intelligence that we're looking at include the ability to deep fake video and voice, social cohesive attacks as was discussed earlier with the issues related to the IRA, social engineering, and interactive fake voices or texts, and cyber offense and defense.

We also are looking at gene editing - and I might add up, I didn't mention earlier, we really appreciate the support of the DHS (SFRT) to provide a number of briefings for myself, Cathy Lanier and other members of the committee. And we look forward to engage in much deeper as we go forward on the remaining issues of robotics and quantum computing.

Regarding the gene editing, we are concerned that the weaponization of gene editing technologies could result in viral dissemination, biological threats, bioengineered agriculture or livestock. And that could be either an enhancement or weakness of obviously with economic benefit to this, but there also is a way to create threats through that kill chain if you will.

Human therapy and genome modification, the impact on infectious diseases. And even looking at the issue of gene exchange or the ability to take a genetic footprint and actually recreate something, or as we're calling raising the dead.

And finally, looking at how - you might encounter this in terms of threats presented by biohazards related to livestock.

There's much more information out there. This is supposed to be an overview, provide you kind of a sample of some of the issues we're running into.

What we're trying to do, is a little bit of a challenge, is to constrain what we're doing on what's most important and not try and boil the ocean if you will.

But we have made the decision that the number one threats we need to deal with right now are UASs and we're putting our focus on that with the recent FAA reauthorization - given that authorization extends to DHS components. And that is our most pressing work we do right now.

I will follow up with an updated briefing, and we'll be addressing our robotics and quantum computing at our next opportunity.

I'd like to stop there and ask Cathy Lanier if she would like to add anything.

Cathy Lanier:
Thank you Thad.

The only thing I'd like to add is having opportunities to be both part of this strategic group, but also operational with some of the changes encountering UAS, following the reauthorization act, there really is a sense of urgency in terms of developing what Thad outlined is the doctrine, command and control, communications that will go along with what science and technology are doing in research, but also a sense of urgency to putting what technologies are available in the hands of the right people to provide that protection that are needed.

So there's a real, real sense of urgency as we work through this progress. And I think we'll elaborate a little bit more on that in our final report. But that's really all I have to add. Thank you again.

Thad Allen:
And we're ready for any questions.

Matt Hayden:
All right. Any questions from the HSAC?

Hearing none, thank you very much, Thad and Cathy. That was a great overview of progress and great work.

Switching now to the state local, tribal and territorial cybersecurity subcommittee. I'd like to introduce Mr. Paul Goldernberg and the Vice-Chair Paul - I'm sorry, Frank Cilluffo.

Paul Goldenberg:
Thank you Matt. Thank you to Secretary Nielsen, Judge Webster, Commissioner Bratton and especially to Frank Cilluffo and with a lot of help from Bob Rose and other - and just more recently who just joined us was General Alexander who really I had the opportunity to have a quite enlightening conversation with yesterday with regard to securing the election process. And we'll be hearing more from General, I believe and from the group in that vein.

Most of you all know that local governments across the United States are very much the focal point of service delivery to our homes and our businesses. And the fact that local governments, state and local governments are largely responsible for providing everything from utility services; water, power, public transportation, public health services, schools, emergency response functions, and extremely critical. And now as we hear coming under attack are fire and policing services, cyberattack.

Residents use and interact with these services on a daily basis, really making the reliability and availability of these services more critical to the wellbeing of not only our state and local, but to greater society as well.

Our local governments increasingly are relying on information technology, IT, and communication systems to improve the delivery of the services to the residents. These IT systems and the internet that have allowed governments to communicate with their constituents

in a much more efficient matter. They're providing direct access to a range of online services now more than ever, and support delivery of municipal services like water and power.

Additionally, many of the local governments today are leveraging the, we all know is the IoT, the internet of things, the technologies. And now we hear every day more so about smart city solutions to improve the efficiencies and the physical city infrastructures. And these trends are becoming more and more reliant on a cyber-connected service than ever before, enabling the cities and the counties across the United States to really become more innovative, improve the efficiencies, and open up new economic opportunities. And that's all the good news.

The real challenge for state and locals, they're disparate, there's over 3,000 of them across the United States, some that have very sophisticated IT systems and some - and many unfortunately that do not.

The increase in dependence on cyber and communication systems has introduced newer opportunities as we all know for these cyber threat actors, and great cyber and physical connectedness is also meant the cyber incident could generate an impact on physical infrastructure, potentially threatening the public health and safety, particularly if the infrastructure manages the lifeline functions or systems with a great potential to cause harm across the board.

Local governments as we all know are moving toward the digital environment, which means that the governments are now collecting more than ever and retaining large amounts of our personal identity, our personal identification, and other sensitive data online. And we know that state actors, as well as those that are working in the basements are seeking to obtain.

So with that, local government now faces unprecedented and evolving challenges in protecting their public safety, protecting the data, and ensuring the integrity of their networks against cyber threats both physical and other. So the challenges had been real tough for the state and locals.

Our tasking from the Secretary was pretty clear. The cybersecurity subcommittee was tasked to examine the DHS cybersecurity engagement with the state local partners. And subcommittee was tasked to provide recommendations for improving the DHS support to these stakeholders in order for them to better protect themselves and better understand the threats against them.

So we really had three primary taskings; how does DHS efficiently and effectively across all DHS components -- and ladies and gentlemen, that I think that for Frank, myself and others on the committee, we found to be one of the greatest challenges.

How does the DHS enterprise support the SLTP agencies and partners in pursuing cybersecurity and resilience of their infrastructure to include response and recovery? There's a lot of tremendous material and resources out there, it's really - appears to have been the challenges - what they need to know, what they need to do. And I think Frank will elaborate on a little bit more.

Who can they call when you have such a vast enterprise with a lot of different resources, and how do we get those resources to 3,000 plus counties?

And then last but not least, how effective has the Homeland Security Grant Program been in addressing the cybersecurity risks? We have many grant programs out there, and are they reaching those that are in greatest need? And how could they be better structured?

So at first blush, what we did do is we wanted to ensure that we spoke with the constituents, we spoke with the associations and the organizations that are responsible for not only the cyber oversight, but just governance at the state and local level. And through the good works of Matt Hayden and Mike Miron and their team, we had the opportunity on December 4th at TSA headquarters to meet with a remarkable group of individuals that gave us a better opportunity to understand the challenges and understand some of the needs that the state and locals were looking for.

We met with Dr. Oscar Alein, Senior Advisor for Public Health Programs, which would be tremendously, and have been tremendously impacted and continue to be impacted by cyber issues. We met with Margret Bruner, Program Director for the National Governors Association to get a better understanding of the impact at the state level and how the resources are moving from federal to state to county, and of course municipal local and tribal.

We met with Michael Garcia, Senior Policy Analyst also from the Governors Association. We met with Linda Langston, Director of Strategic Relations from the National Associations of County Governments. We have the opportunity to meet with many really very resourceful people working within the new cybersecurity division. We had an opportunity to learn more about what the TSA is doing, and some of the other organizations out there that are working within the DHS enterprise.

We also had an opportunity to hear from others such as Chuck Brooks and others that are working from the outside that also have their own opinion and recommendations.

So really across nearly all the interviews and research conducted, our greatest - we saw that the greatest challenge that emerged with local governments, their persistent struggle is limited funding, limited staff, the people, the process, and technology investments require to protect local governments and networks and services they support are exceeding the current supply of local resources. And it is a serious challenge for them.

In closing on my end, and then I'd like to turn it over to Frank, my co-chair, we know that threat awareness, local governments are struggling to stay current on the rapidly evolving and increasingly sophisticated cyber threats.

Cybersecurity hygiene and training - they have a persistent need for cybersecurity training and education for not only the IT staff and users, but for all staff across the border.

Incident response - although we have a plethora of tremendous resources out there that are really working hard to reach the masses, the local governments often don't know who to contact or what immediate actions that they should be taking following a cybersecurity incident. And many lack incident response plans even guide their actions following a breach. So it's not only we have the breach, what do we do after the breach, and how do we close the mark.

I think last but not least, and we'll be elaborating much more so because this is still work in progress. These are nowhere near the final recommendations or what we feel would be solutions. These are just some of what we have gathered from our recent discussions with the constituency.

But prioritization of cybersecurity tools and resources. They're overwhelmed. The local governments are literally overwhelmed by the tools and the resources that they can or should leverage for cybersecurity.

How do they prioritize? Who do they call? And again, when do they make that call?

And I know that there's excellent movement inside the department to address these concerns and issues, and that's been a moving situation over the past six-seven months. And I know that we're making progress there as well.

So we will be meeting again on the 18th, and we have a tremendous lineup of additional folks that we're going to be talking to so we can gain more knowledge about the challenges thereof. And we look forward to learning more and then sharing our final findings with the Secretary and with you all in the days to come.

I'd like to now turn this over if I could to Frank, Frank Cilluffo.

Frank Cilluffo:
Well, thank you Paul, and thanks for an excellent rundown on our efforts so far.

I mean, just to underscore a couple of very brief points, because I think you covered all the key data - I mean, I think that those of us in DC don't fully appreciate of how enormous of an undertaking this is to be able to ensure that our (SLPT) partners are fully up to speed on cyber.

I think the standup of (CISCA) within the Department of Homeland Security is already yielding some positive benefit. But when we look at the grant, and this is one area I don't want to get too far out in front of where our subcommittee is. But less than 4% of Homeland Security grant funding goes for cybersecurity efforts. And I think that that's a bit of a mismatch given the threat environment we're facing today.

So one of the areas we're looking at next is examining how we can potentially increase the cybersecurity grants, but do so in a way that also places honest to goodness parameters and

mechanisms to ensure we're actually driving down risk and doing so in way they can be measured in a measureable kind of way.

And one thing we have received briefings on the electoral security process, and I think building on some of that cooperation between the department and some of those folks could be a good venue to try to double down some of those efforts.

But just a couple of very small matters at the state and local level, and territorial and tribal as well. A small percentage of the spend that's being put toward IT and OT operations is going towards cybersecurity. And they have a huge workforce challenge when it comes to ensuring the best and the brightest are being employed. And we've been hearing from a number of the clients that turnover and retention is a big challenge, as much as 50% every two years.

So we've got a big challenge that we're trying to address and I just would like to also echo Paul's comments, thank our subcommittee, but also the departments and great in providing unvarnished briefings on what we're all trying to get our arms around.

So I've never had an unspoken thought. I'll leave it at that.

Breaking news. I just heard Bryce Harper signed with the Phillies. So for us Mets fans, not a great day.

Matt Hayden:
Thank you both Paul and Frank. And at this time, I'll just pause to see if there are any questions from the HSAC from that presentation.

Hearing none, and I'll just break for a moment from - before resuming with Judge Webster. We do still have the Secretary on the line. And I'd like to give her the opportunity to make some closing remarks.

Madam Secretary, are you available?

Secretary Kirstjen Nielsen:
Yes, thanks Matt. And Judge, I will turn it over to you.

First of all, I'm so glad I was able to listen to all the tremendous work that you all had put into our request of taskings. I truly thank you. I'm thrilled by your insights in what we will be able to do to execute the recommendations, to look forward to this final brief out.

Just really quickly, on the families and UACs, this is a very complex issue. As I mentioned at the top of the call, and I'm working very closely with the countries in the region to try to help the vulnerable populations and provide alternatives to them so that they do not have to make this journey. We continue to try to work with congress.

But I would just highlight that the significant endangerment of children which I think, Karen, was the phrase that you used, is of great concern. I'm sure you all have heard that from the men and women of CBP. So trying to find additional ways to support them is really what we're after.

On the coming foreign interference, the recommendation that you mentioned related to (HSI), I look forward to learning more about that. You are correct that they are not necessarily resourced to combat this threat. But I would be very interested in learning more as you've looked through the department as to where we best have subject matter expertise and capabilities. And you mentioned the wonderful capabilities that (ICE) have with respect to cyber to combat that.

On emerging tech, the new untraceable weapons, check, doctrine on command and control, check. The sense of urgency writ large on drones and UAS, I can certainly underscore from my position. I often talk to our international partners about this as we all see drones proliferating.

I would just mention that the unmanned concept here unfortunately is not limited to aerial. We do see unmanned surface vehicles, we see unmanned maritime vehicles. And this is going to continue to be a threat vector that expands.

So I very much look forward to learning more about what you're learning. But then of course, on the other emerging tech as well.

I spent some time yesterday with the venture capital community in California, trying to get a sense from them as to emerging technologies. I think department-wide, we need to posture ourselves much more to be on our toes to scan that horizon both for the opportunities for technology to be a force multiplier, but also for potential vulnerabilities that could introduce into the system.

And the last brief out on state local tribe and territorial cyber, yes, I think it would be very interested for your additional assessment on grants. As you know, we have some restrictions on grants that perhaps are outdated. Originally, the grants were meant to help state and local protect against and prevent terrorist acts.

We can all argue back and forth whether any given cyberattack is a terrorist attack. But we do find more and more with emerging threats that the application of the grant funding can be inadvertently limited. So I look forward to learning more about that.

And then on the incident response plans and knowing who to contact, to how to prioritize, this all rings very true to me. I look forward to ways in which the committee thinks that we could best engage state and local not only to make them aware of tools and resources that are available in a way that's accessible that we don't overwhelm them, but to get back to the basics and help them understand who to call when about what, so that they have a better sense of what they need to do, should they have an attack.

So Judge, over to you and Matt. But I just want to thank everyone again so much for all this very hard and amazing work. Really look forward to the final reports.

William Webster:
Thank you very much, Secretary Nielsen. And thank you for your really interesting and useful insights as we round this lengthy, but interesting series of meetings and discussions to a close.

I particularly want to thank HSAC staff, Matt Hayden, Mike Miron, and Catherine Fraser for their good work as well, and perhaps most important, Secretary Nielsen.

Members of the public who would like to provide additional comments, and that includes the media, may do so in writing by post to - and this is the address - the Homeland Security Advisory Council, U.S. Department of Homeland Security, 245 Murray, M-U-R-R-A-Y Lane, Southwest, mail stop 0445, Washington DC, 20528. Or by mail - by email, at - this is email in caps; HSAC, H-S-A-C@ - abbreviate at - HQ.DHS.gov, G-O-V.

Your comments are appreciated and they'll be reflected in the meeting minutes.

And I would like to thank you for your participation today. And I'm on to express my personal appreciation to all of you who weighed in to make this such a worthwhile experience for us working together.

I want to thank the members of the council and the subcommittee for their time and participation.

And so formally, the meeting of the Homeland Security Advisory Council is now adjourned. Thank you all very much. Keep up the good work.

Operator:
Ladies and gentlemen, that concludes the conference call. We thank you for your participation. And you can now disconnect your lines.

I hereby certify that, to the best of my knowledge, the foregoing minutes are accurate and complete.

Judge Webster signed document on March 11, 2019.

Signed and Dated
Judge William H. Webster, Chairman, Homeland Security Advisory Council