

U. S. Department of Homeland Security
Homeland Security Advisory Council Conference Call
Monday, February 24, 2020
Meeting Minutes
1:00 p.m. – 2:30 p.m.

The open session of the Homeland Security Advisory Council (HSAC) meeting was convened on February 24, 2020 from 1:00 p.m. to 2:30 p.m. 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 attended the meeting:

HSAC Members:

William H. Webster (Chair)
William Bratton (Vice Chair)
Steve Adegbite
Stewart Baker
Robert Bonner
Art Acevedo
Jim Jones
Thad W. Allen
Frank Cilluffo
Mark Dannels
Donald P. Dunbar
Leon Fresco
Paul Goldenberg
Michael P. Jackson
Cathy Lanier
Carie A. Lemack
John Magaw
Jeff Moss
Ali H. Soufan
Robert Rose
Wendy Smith-Reeve
Chad Sweet
Karen Tandy

DHS Participants:

Chad Wolf, Acting Secretary, DHS
John H. Hill, Assistant Secretary, Office of Partnership and Engagement
Mike Miron, Acting Executive Director, Homeland Security Advisory Council
Evan Hughes, Associate Director, Homeland Security Advisory Council

Operator:

Greetings everyone and welcome to the Homeland Security Advisory Council conference call. During this presentation all participants will be in listen-only mode. Afterwards, we'll have a question-and-answer session. At that time if you have a question or comment, please press the 1 followed by the 4 on your telephone keypad. If you need operator assistance, please press star followed by 0. As a reminder, this conference call is being recorded today, Monday, February 24, 2020. Now it's my pleasure to turn the conference over to Mike Miron. Please go ahead.

Mike Miron:

Thank you, operator. Judge Webster, the floor is yours, sir.

Judge William Webster:

All right, thank you very much. My name is Judge William Webster and I am the Chair of the Homeland Security Advisory Council, or HSAC, for short. I welcome you to today's public meeting where we will receive the draft reports on Unmanned Aircraft Systems and 3D Printing of the HSAC's Emerging Technology Subcommittee. I would like to welcome our HSAC members and members of the public we have an attendance.

A special thank you to the HSAC staff for their continuous support of the Council's hard work. I would like to thank Thad Allen, Cathy Lanier and Robert Rose for their leadership and their service as co-chairs of the Emerging Technology Subcommittee.

I'd like to thank all the members who served on this important subcommittee. Thad, Kathy and Robert, I look forward to hearing your presentation today.

I'd also like to thank the Secretary of Homeland Security, Chad Wolf, for joining us today. The Secretary is doing a great job leading the Department. The Secretary recently worked with DHS partners and HSAC members Cathy Lanier and Jeff Miller to protect Super Bowl 54. Thank you.

I now turn it over to HSAC Vice Chair Bill Bratton for remarks.

William Bratton:

Thank you, Judge. It's a pleasure to be on this call and to have read the reports that are going to be discussed. I would like to point out to the public that the members of HSAC are voluntary and that this is a bipartisan committee. They are not enumerated for the countless hours and travel that they put in to compile these reports. So, I want to thank them for their devotion to their country and to the hard work they consistently put in that will be reflected in the reports today. It is truly a sacrifice on their part that they are willing to volunteer their time and service to their country. So, thank you to all of them.

Mike Miron:

Thank you, Judge Webster and Commissioner Bratton for those remarks. I would also like to thank the HSAC members and members of the public for joining today's public call. For members of the public, if you wish to do so, you'll have a one-minute comment period after the two reports are briefed by the two co-chairs and vice-chair. For the record, we have 24 Homeland Security Advisory Council members participating in today's meeting. Once the reports are briefed, we will take public comments, have console deliberations, and then vote on the report. At this time, I'd like to turn the call over to Secretary Chad Wolf.

Acting Secretary Chad Wolf:

Thanks, Mike. Judge Webster, Commissioner Bratton, and HSAC subcommittee members, thank you for your continued service on the Council, for the Department, and to the nation. I remain personally grateful for each of you lending your time and talent dissolved into the most complex challenges that the Department is facing. Before moving on to some of the new taskings, and I am certainly interested in learning more about the new reports being delivered, I want to provide the Council with a few updates from the Department.

Let me start with the FY 2021 budget. We have four appropriation hearings in the next few weeks: two this week and two next week to talk about the Department FY 2021 budget requests in the direction that the Department is resourcing itself as we look towards next fiscal year. I look forward to participating in those hearings, answering questions from members of Congress, and talking about the Department's priorities and how we're resourcing accordingly.

Next, let me talk a little bit about the Southwest border. January was the eighth month in a row where we had lower apprehension numbers along the Southwest border, which means that the

strategy we have put in place over the last several months is working, as is the combination of different factors, including the border wall system and the engagement we're doing in central Mexico. I just got back from our twelfth (administrative) since late 2018 with Honduras, Guatemala, El Salvador, Costa Rica and Panama, addressing not only the security issues that we face regionally, but also talking about prosperity in those countries which obviously leads to stability and security. So, we'll continue to make progress on that front and continue to make progress that the government of Mexico is a partner enhancing enforcement measures. As you know, Mexico deploys thousands of National Guard members to both their Southern and Northern border to engage some of the illicit travel that they see within their country as well.

Regarding the wall: we have a border wall system under the President's leadership. As of this weekend, we've built over 120 miles of new border wall. We have another 250 miles currently under construction and another 400 miles under the pre-construction phase. We're still on track to reach 450 miles of new border wall by the end of the calendar year.

Let me pivot to what the Department is doing on the coronavirus. We are heavily engaged. Obviously, HHS is the lead coordinator for the federal government on our response to the coronavirus and is certainly mapping out a medical strategy. The Department has been very engaged and we're doing quite a bit on that, from the air and land to the maritime ports of entry. We have rerouted incoming flights to 11 pre-selected airports, DHF, and have set up medical screenings in each of those airports. Then, depending on what they find in those medical screenings, people are referred to CDC for further action. The Department's doing a lot, from our frontline operators at the land ports of entry to the Coast Guard in the maritime environment as well.

Lastly, let me speak to some of the action that the Department has taken in response to New York's Green Light Law. The Green Light Law in New York makes it virtually impossible for the Department to complete its law enforcement mission. It restricts information sharing with the Department in ways that go above and beyond what any other state has done.

That requires us to take a number of actions in the CBP context. The law restricts information sharing with CBP in a way that is unique to what any other state has done. I asked the CBP operators, how does it impact your operations? They came back with several issues, including

customs enforcement and vetting trusted travelers.

To ensure that Global Entry and other trusted traveler programs would not need to be shut down over the long term, I made the decision to prohibit enrollment and re-enrollment of New York residents into that program until we could find a solution. We have had a meeting and follow-up discussions with the Governor and the President. I think we're getting close to a resolution on that front. I think we're all moving in that direction, which I think it is helpful. but just like you would not want New York to impair the FBI from sharing information with them to do their law enforcement mission, they shouldn't be doing the same with the Department. HSI, that's Homeland Security Investigations, is second largest criminal law enforcement agency in the country. Right now, they do not receive information from New York and that just can't continue. So, we look forward to remediating that with New York in the short term.

Let me turn to the HSAC now. As has been mentioned, I look forward to receiving the reports today from the Emerging Technology Subcommittee on Unmanned Aircraft Systems as well as 3D Printing. Again, thank you to Thad Allen, Cathy Lanier and Robert Rose, along with all the subcommittee members for the hours that they've certainly put into the draft. I really look forward to reading each of these reports cover to cover when approved by the Council.

I'd also like to talk about four new tasking assignments that we would like the Council to review and then begin working on. Tasking One will be an Economic Security subcommittee. This subcommittee will explore the elements of economic security as it relates to the Department's authorities and provide recommendations to ensure that the Department is optimally positioned to resource, organize, and safeguard this important component of the American market system and way of life.

Tasking Two is the Information and Communications Technology Industrial Strategy subcommittee, which looks for the evolving risk of information and communications technology. It will provide recommendations on how to increase government collaboration with industry and how to increase the shared understanding of supply chain vulnerabilities and threats. It will further examine the effectiveness of current government procurement efforts to increase the security of information and communications technology products.

Tasking Three is a Building Youth Focused Engagement subcommittee which would explore opportunities to build youth-focused engagements that can be implemented nationwide in order to prevent radicalization to violence. This subcommittee can identify key national and local partners to contribute to the development and implementation of the program. Recommendations will align with the Department's day one priorities of Civil Rights, Civil Liberties and individual privacy protection.

Lastly is Tasking Four. The Biometrics subcommittee will review the Department's authorities and governance to ensure that it has a single and reliable approach to biometric identity management both internally and with external partners. This subcommittee will also review the Department's multiyear biometric vision strategy and implementation plan to include its effective performance metrics and oversight.

I'll provide additional information on these four taskings in a memorandum to Judge Webster, asking him to create these four subcommittees under the Council in the days to come. We also make these taskings public by placing them on the HSAC website for public awareness. I look forward to our next in-person meeting with the HSAC in May and will turn it back over to Mike.

Mike Miron:

Thank you very much, Mr. Secretary. Currently, I'd like to ask Thad Allen, Cathy Lanier, Bob Rose, the co-chairs and vice-chairs of the Emergency Technologies Subcommittee, to brief the reports. Thad, Cathy and Bob, the floor is yours.

Thad Allen:

Thank you very much. This is Thad Allen, co-chair with Cathy of the Emerging Technologies Subcommittee. I have just a couple of opening remarks. We've been working on this for a couple of years now and the tasking has experienced various leadership changes at the Department. It's always a challenge, what with the technology moving so rapidly in both its application and terms of capabilities, plus changing risk vectors at the same time. I would only make the comment that any reports we provide on emerging technologies should be considered on a point in time basis and need to be monitored in the future for changes because they move so rapidly. To that end, we're going to be proposing a permanent structure that will help us monitor these technologies and be responsive to the Secretary's tasking and institutionalized relationships

from the Department. With that, we'll move to Cathy Lanier who will brief the Final Report on Unmanned Aircraft Systems. Cathy?

Cathy Lanier:

Thank you. I appreciate your opening comments and the chance to work with you and the rest of the team here. Keeping pace with technology change is certainly a theme I'm familiar with, as we've been working hard on this project. In our initial report on unmanned aerial systems, we focused our recommendations on legal framework legislation and regulation. For this report, we focus a bit more on policy implementation, standards, standardization and future mitigation challenges.

From our view, the accelerated pace of technological change in today's global environment creates both opportunities and risks. The opportunity is to capitalize on the value of the technologies and the risk is that we will not be able to keep up with the pace of change. This is most critical in the legislative and regulatory space of bureaucratic government where policy does not move quickly. This report provides an assessment of the current state and perceived future advancements. Over the next three to 10 years, these advancements could pose a threat to the homeland as well as recommendations for mitigation. Now I'll talk a little bit on the Reauthorization Act.

Since Reauthorization Act and our interim report, DOJ and DHS have conducted testing of detection tracking and mitigation at several different venues. Consistent with the legislation, each test site requires extensive documentation to meet the requirements of the legislation and obtain approval of either the Attorney General or Secretary of Homeland Security. While the implementation time has dropped significantly from initially an eight-week timeline for the initial deployment, the process is still too complex and is not agile enough to support counter-UAS operations and time sensitive situations. Adding to our challenge, UAS is fast becoming more capable and sophisticated, and the barriers to entry in terms of the necessary expertise for operators are quickly diminishing. Enterprises are employing increasingly larger fleets, and more individuals are becoming drone operators.

Like the vast majority of industrialized countries, the U.S. will be actively pursuing national strategies for the use and integration of UAS. Integration of UAS capable of sustained, routine,

autonomous, beyond-line-of-sight operations and mixed-use airspace is ultimately the goal. To achieve smart cities and other initiatives, you are going to have to build systems that supports that activity. That means integrating autonomous features that allow the UAS to sense and operate in dynamic environments using artificial intelligence, deep learning and big data to draw from.

By understanding air traffic congestion, avoidance system health and lost DataLink protocols, they will also leverage more efficient means of tool and power management, including lithium and hydrogen batteries, giving them even greater indoor range and payload. It will certainly leverage the emerging 5G technology and its ability to transfer large amounts of data with reduced latency over long distances.

By 2030, we can expect to see a fully integrated airspace with UAS operating near airports and other sensitive sites; collecting data doing inspections on critical infrastructure such as pipelines and power lines. Robotic features will be incorporated to allow for simple taskings such as opening access panels, removing/tightening screws, or repairing downed lines. We should also see significantly smaller UAS being used for internal 3D mapping purposes in mines, collapsed structures and other tactical applications.

UAS fleet operations should be well established, with the systems capable of communicating with each other to gather data and coordinate tasks. Count on these threats from nefarious and harmful UAS activity. Securing critical data contained in UAS will become increasingly complex and will require the use of emerging and converging technologies in the future. In our previous report, we talked about the importance of an integrated platform for countering the UAS threat in the future. Radar RF, like for optical IR and acoustic means of detecting, tracking and identifying, will become more complicated in the future. Our ability to disable and neutralize via Connectix jamming and spoofing will also become a challenge.

Integrated platforms of the future will need to be advanced enough for detection and tracking. Emerging technologies such as passive radar systems that detect and track objects by processing reflections from non-cooperative sources of illumination in the environment. Other examples are Specialized Kinetic Payloads, Interceptor UAS “Hunter Drones”, and improvements to current radars such as smaller weight, dimensions and cost, and incorporation of micro-doppler radar

techniques to discern UAS from biologicals and jet propulsion aircraft. Our recommendations in this report are confined to three buckets. Because this report is one to 20 pages long, I try to consolidate our recommendations into three categories.

First, the expedited implementation of policy and protocol. We still are not moving fast enough. We've had legislation for more than 18 months now and clear policy and doctrine is not mature or complete. This needs immediate attention. This one is easily achievable. Legislation has been passed, so the issue is just slow policy development.

Standards, development of a national CUS mitigation policy so that there is a common federal standard for countering UAS operations, and a good model for development of state and local, tribal and territorial law enforcement to counter UAS mitigation policies when that authority is expanded is needed. This is going to require someone to focus and drive DOJ and DHS components to come up with policy, and the Secretary is someone who can do that. Requirements are needed for the FAA to establish and publish UAS detection and mitigation system standards and provide straight-forward guidance to those seeking to deploy, detect, track and identify technologies. This was a recommendation that was also in the Blue-Ribbon Task Force recommendations for countering UAS in airports.

We also recommend clear directions to other federal, state, local, and tribal territorial law enforcement regarding the current legal statutory and regulatory limitations on technological enablers that are used to detect, crack, identify and disable potential threats UAS.

And lastly, future actions. Expansion of mitigation authority to other federal, state, local and territorial authorities with clearly defined protocols for its use is critical because most responses to these types of threats will involve local authorities. Moreover, ensuring that future legislative efforts are fast-paced and flexible to keep up with rapidly evolving technology is recommended. The Preventing Emergency Threats Act of 2018 was the first legislative effort and successfully authorized testing of mitigation technology for UAS threats that had been present for many years. This is a step in the right direction despite the significant limitations included in the final bill. The conditions that must be met to gain approval, even just for testing telling UAS technologies, are extremely time consuming and difficult to achieve.

Additionally, the legislation's exclusion of the use of approved mitigation technology by state and local law enforcement and the Transportation Safety Administration essentially eliminates counter UAS capabilities at the overwhelming majority of mass gatherings and commercial airports nationwide.

Lastly, we note that the legislation as written prohibits the sharing of even basic information with critical partners, which in turn tampers with coordination and mitigation efforts.

I'll close by saying that all these recommendations are important if we're going to be able to mitigate current threats. These three critical components that I mentioned will make the biggest difference. I participate in the HSAC and projects like the Blue-Ribbon Task Force because these are serious threats to the security of the homeland and our critical infrastructure. But my current and former day job, protecting soft target mass gatherings, is most impacted by progress with the recommendations highlighted on today's call. With that, I will turn it back over to you, Mike.

Mike Miron:

Thank you, Cathy. Mr. Rose, the floor is yours, sir.

Robert Rose:

Thank you, Mike. Secretary Wolf, Judge Webster, Commissioner Bratton, my Emerging Technology chairs, Thad Allen and Cathy Lanier - thank you for giving me the opportunity to serve. It's been truly a privilege. I look forward to engaging on the new taskings of the Secretary.

I'm going to talk very briefly about 3D printing, highlighting the six potential threats to Homeland Security and then provide a few suggested mitigation solutions. The first threat is sabotage of critical parts: the intentional modifications that result in premature failure, such that a modified printed file appears to meet all requirements while actually containing concealed, minuet flaws or flaws that cannot be identified. Second is the concealment and bedding of illicit objects within a 3D printed part during the printing process. The printed part may appear normal and legal to the casual observer, but could contain illicit objects such as illegal drugs, explosives, or embedded technologies for espionage.

The third threat is untraceable weapons which have no serial number, making them undetectable to any metal detectors. Certain polymer materials are used to produce firearms and firearm parts that are more durable than plastic but untraceable. Explosives can be fabricated from widely available materials that are not individually a cause for concern until they have been combined with others.

Of course, another threat would be supply chain exposure, as 3D printing production capabilities are vulnerable to malware and malicious interference. Actors can make the printer inoperable or digitally store parts so that sensitive proprietary or critical design information may be exposed during the digital transfer files between designers, engineers and manufacturing technician. It could also be used to steal or replace files to cause failure of the printer, of the build, or premature failure of the parts.

Fifth is the significant problem of counterfeits using 3D printing for credit card scammers, weapons, weaponized UAS, ban products, and explosives. An actor with physical access to a park could take a 3D scan and produce digital design files to replicate high value goods and infringe on copyright and trademark violation. Economic impacts of the loss of market, jobs, and tax revenues may lead to the distribution of lower quality and potentially dangerous products into the marketplace.

The last threat we identify in the final report is that of biometrics spoofing, which includes the fabrication of masks to spoof facial recognition software, prosthetics and fingerprints to deceive fingerprint readers.

The first of the three recommendations we provide in our report was technologies for integrated attribution. Traceability of 3D printed parts to source machines or source files can support intellectual property protection, counterfeit detection and deterrence, and prosecution by law enforcement. A potential solution here would be a blockchain, as relates to 3D printing, through a distributed decentralized public ledger that encrypts, validates, and permanently records transactions. Multiple authorized parties can update the distributed public ledger, uniquely tagging embedded 3D printed parts to trace the history from fabrication to end user.

Second, we recommend enhanced detection mechanisms, including enhanced imaging and detection tools, that can aid in countering concealment threats. Such capabilities could include: rapid through-part imaging to identify objects contained within printed parts that otherwise appear innocuous, a high-resolution two-part imaging to identify flaws intentionally embedded in the critical parts that may lead to premature part failure, and detection of printed explosive materials.

Lastly, this report recommends the reinforcement of cybersecurity measures. An important attribute of 3D printing is the ability to rapidly share design data, 3D models and manufacturing files across networks with multiple users and systems. We need robust means for protecting digital data domains through sensitive proprietary or critical design information. Such measures taken to protect digital data should be monitored on a routine basis to ensure that they address evolving attack vectors.

So, Mr. Secretary, Judge Webster and Commissioner Bratton, that's a summary of the 3D printing threats and possible solutions. Again, thank you for the opportunity to serve.

Mike Miron:

Thank you, Bob. Thad, the floor is yours.

Thad Allen:

Do you want me to speak after the public comments or right now?

Mike Miron:

You can speak now and then we'll go to public comments.

Thad Allen:

As you can see with the complexity and the detail associated with these two reports, the range of emerging technologies is striking. I now turn to a recommendation that is separate from this report. After having some internal discussion with Cathy and Bob, I will independently pursue for the next meeting of the HSAC a recommendation for the creation of a standing committee to look at emerging technologies, rather than address these things on an ad hoc basis as identified. This can create a sustained ongoing function that can support the Department of the Secretary.

One way to think about that would be to establish some kind of executive agency within FNT that becomes an integrated entity within the components, just so we have some routine tracking and clerical support for the information we are developing. We deal with them all. We talked with all the components on the UAS issue as we were developing them. We think that over time, incrementally without a lot of fuss and bother, we can institutionalize a better way for SNG to work with the components. To that end, we'll be putting together some recommendations and we'll be talking about them in the future. But for now, the two reports today are our submission to be determined in the future. They include: biotechnology, gene editing splicing, quantum information science, and quantum computing and advanced robotics. We will be reporting on progress and will be way ahead on that at the next HSAC meeting. With that, I'll turn it back over to you, Mike.

Mike Miron:

All right, thank you so much, and once again thank you to Thad, Cathy and Robert for your presentations today.

I would now like to open the meeting for public comment. Comments will be limited to one minute each. Your comments will be reflected in today's meeting minutes. Operator, please prompt the members of the public to determine if there are any public comments at this time.

Operator:

Certainly, thank you very much. Ladies and gentlemen, if you'd like to register a question or a comment, please press 1,4 on your telephone keypad. You will hear a three-tone prompt to acknowledge your request. Once again, for comments please press the 1 followed by the 4 on your telephone keypad now. One moment please for the first comment.

As a reminder for comments, please press the 1 then 4 on your telephone keypad. One moment.

Mr. Miron, we have no comments at this time.

Mike Miron:

All right, thank you. This concludes the public comment period. Thank you again, members of

the public. I now turn it over to Judge Webster.

Judge William Webster:

Thank you, Mike. I'd like to thank Thad, Cathy, Robert, and all the subcommittee members for their excellent work on these two reports. I now open it up to members of the HSAC for comments on the report. I'm asking Thad, Cathy, Robert and Mike to moderate the discussion. Thus far, I've heard no comments. Are there any comments? All right, Mike, I'll turn over to you at this point.

Mike Miron:

Thank you, Judge Webster, and if there is no further discussion, is there a motion from the HSAC members to approve the reports and send to the Secretary?

Group:

Motion to move.

Thad Allen:

Second.

Mike Miron:

All right, who is the first? Just for record keeping, was that you Jeff Moss?

Jeff Moss:

No, that was somebody else.

Robert Rose:

I think I went first.

Mike Miron:

Okay, thank you, and who is the second?

Robert Bonner:

Rob Bonner

Mike Miron:

Okay, thank you, Rob. Thank you, Mr. Bonner. At this time, those in favor of approving the recommendations please indicate 'aye'.

Group:

Aye.

Mike Miron:

Those opposed, please indicate 'nay'. (silence). If there are any abstentions, we should record them as well. (silence). All right. Thank you. The reports are approved, and the recommendations passed by acclamation. Members of the public and media who would like to provide any additional questions or comments, the comment period is still open, and you may do so by emailing the HSAC at hsac@hq.dhs.gov.

HSAC information and meeting minutes may be found at <https://www.dhs.gov/homeland-security-advisory-council>. Judge Webster, I now turn the floor over to you to close the meeting.

Judge William Webster:

Thank you very much. Thank you again to our subcommittee co-chairs Thad Allen and Cathy Lanier, and our Vice Chair Robert Rose, for their leadership and the subcommittee's really great work. I want to thank the HSAC members and members of the public for attending today's call and give a special thanks to Mike and Evan for organizing today's meeting. We're now going to bring this public session to a close. This meeting is now adjourned. Thank you.

Mike Miron:

Thank you. Thank you, everyone. Have a great afternoon.

Operator:

That concludes our conference call for today. Everyone have a great rest of your day and you may disconnect your line.

Mike Miron:

Thank you, operator. END

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

Judge Webster signed document on March 10, 2020

A handwritten signature in black ink, reading "William H. Webster". The signature is written in a cursive style with a large, stylized initial "W".

Signed and Dated

Judge William H. Webster, Chairman, Homeland Security Advisory Council