S. Hrg. 117–652

PROTECTING THE HOMELAND FROM UNMANNED AIRCRAFT SYSTEMS

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

JULY 14, 2022

Available via the World Wide Web: http://www.govinfo.gov

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PUBLISHING OFFICE
51–532 PDF WASHINGTON : 2024

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
ALEX PADILLA, California
JON OSSOFF, Georgia

ROB PORTMAN, Ohio
RON JOHNSON, Wisconsin
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
BENJAMIN J. SCHUBERT, *Professional Staff Member*
PAMELA THIESSEN, *Minority Staff Director*
SAM J. MULOPULOS, *Minority Deputy Staff Director*
CLYDE E. HICKS, *Minority Director of Homeland Security*
ROLAND HERNANDEZ, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*
THOMAS J. SPINO, *Hearing Clerk*

CONTENTS

WITNESSES

THURSDAY, JULY 14, 2022

ALPHABETICAL LIST OF WITNESSES

APPENDIX

PROTECTING THE HOMELAND FROM UNMANNED AIRCRAFT SYSTEMS

THURSDAY, JULY 14, 2022

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:15 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Gary Peters, Chairman of the Committee, presiding.

Present: Senators Peters, Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Johnson, Lankford, Romney, Scott, and Hawley.

OPENING STATEMENT OF CHAIRMAN PETERS[1]

Chairman PETERS. The Committee will come to order.

I would like to thank our witnesses for joining us and for their continued service to the American people.

Today's hearing will highlight the threat posed by unmanned aircraft systems (UAS), commonly known as drones, and discuss how Federal agencies are working together to combat this evolving threat. We will also examine what additional authorities and resources the Department of Homeland Security (DHS), and the Department of Justice (DOJ) need to successfully counter unmanned aerial systems (C–UAS), while working together with the Federal Aviation Administration (FAA).

In recent years, the market for commercial UAS has rapidly expanded due to the affordability and utility of drones that are readily accessible to government, to industry, and to recreational users.

The FAA estimates that by 2024, about 2.3 million UAS, including 1.5 million recreational drones and model aircraft, and about 800,000 commercial UAS, will be registered to fly in U.S. airspace. Between 2016 and 2019, airline pilots reported, on average, more than 100 drone sightings per month to the FAA.

The increase in the number of UAS operating in our air space creates a higher risk of rogue drones either failing to obey safety rules or operating with nefarious intentions, threatening manned aircraft operations, airports, critical infrastructure facilities, and high-profile, widely attended events such as sporting events, concerts, and more.

[1] The prepared statement of Senator Peters appears in the Appendix on page 39.

While most individuals operate their drones responsibly, we have already seen careless and malicious actors misuse these technologies to engage in reckless or criminal activities.

In September 2017, a privately operated drone in Brooklyn, New York, was intentionally flown beyond the operator's line of sight and collided with a U.S. Army Black Hawk helicopter patrolling a temporary no-fly zone around New York City. Thankfully, the Black Hawk and its crew landed safely, but there was significant damage to the helicopter, and the incident created an unacceptable risk to the servicemembers in that helicopter.

In 2019, a drone significantly disrupted flight operations at Newark Liberty Airport for 90 minutes, causing nine flights to be diverted, halting 43 planes inbound to the airport, and also causing significant delays for passengers.

These events demonstrate the severity of the threat posed by UAS, and if we do not act, it could only be a matter of time before someone who is recklessly operating this technology causes an accident that can have catastrophic effects.

As we work to avoid unintentional disasters, we must also account for the escalating threat of weaponized drones from terrorist and criminal organizations who could launch domestic drone attacks on mass gatherings, high-profile landmarks and buildings, or Federal property. This includes foreign adversaries, who have deployed drones in conflicts abroad, and could have the capability to deploy them here in the United States as well.

We must also be prepared to counter drones operated by criminal organizations that are reportedly using UAS for illegal activities including trafficking illicit drugs across our borders.

I am grateful to my colleagues who have led past efforts to address these concerns and to improve the safe integration of UAS into American airspace, including Senator Johnson for authoring the Preventing Emerging Threats Act. Since 2018, the authorities created by this law have bolstered our nation's ability to protect numerous large public events, including the Super Bowl, from UAS threats.

Today's hearing is an opportunity to discuss renewing and updating these authorities, which are set to expire this October, as well as the Biden administration's Domestic Counter-UAS National Action Plan, the first coordinated, whole-of-government plan to address the evolving security threats posed by UAS. I am working on bipartisan legislation that I plan to introduce in the coming weeks to reauthorize and strengthen counter-UAS authorities to better tackle this threat.

Today I am pleased that we have a panel of expert witnesses from DHS, DOJ, and the FAA who can discuss what lawmakers can do to ensure the Federal Government is better equipped to safeguard against potential threats from UAS.

I would now like to recognize Ranking Member Portman for his opening comments.

OPENING STATEMENT OF SENATOR PORTMAN[1]

Senator PORTMAN. Thank you, Mr. Chairman. Thanks to the witnesses for being here. I look forward to hearing from you. We are here today to discuss the emerging threats posed by unmanned aircraft systems, or drones. In 2018, under the leadership of Senator Ron Johnson, who is here this morning, we provided, as Congress, some new authorities to the Department of Homeland Security and Department of Justice to counter the threats posed by the use of drones.

Unfortunately, those authorities are about to expire, and this expiration could not come at a worse time, in my view. Cartels and transnational criminal organizations (TCOs) use drones to smuggle drugs and surveil U.S. law enforcement in furtherance of illicit cross-border activity. These cartels have also begun to weaponize drones in order to commit attacks. So far these attacks, as far as we know, have been in Mexico, but I think weaponized drones along the border are now an emerging threat.

To give you a sense of the scale of the problem, in joint testimony before the House Committee on Homeland Security in March, representatives from DHS said that in a previous five-month period U.S. Customs and Border Protection (CBP) identified more than 30,000 individual flights near or at the Southern Border, where half of those flights violated FAA regulations.

Again, we know that at a minimum these drones are used for surveilling our U.S. law enforcement efforts and for smuggling drugs into the country, including fentanyl, the deadly synthetic opioid. Relatively small amounts of it can kill hundreds of thousands, millions of people. I is subject to being smuggled in relatively small drones.

My office has repeatedly asked DHS, since February of this year, for more information and statistics on these drone border incursions and how they plan to address this emerging threat. Moreover, the Biden administration's Domestic Counter-Drone National Action Plan provides no explicit additional authorities for DHS to counter unmanned aircraft systems as it pertains to the border.

Make no mistake. The Mexican transnational criminal organizations will benefit from the lack of additional counter-drone authority for CBP and other agencies with responsibility for securing our nation's borders. For these reasons, I am eager to hear how DHS, DOJ, and the FAA have used their existing authority to mitigate the threats posed by illicit use of drones. I also hope to discuss what new authorities this Committee can give the Administration to improve the counter-drone mission, especially at the border.

Recently, the Biden administration provided this Committee with a comprehensive legislative proposal which seeks a number of changes and expansions to existing counter-drone authorities. I look forward to working with Senator Peters, Senator Johnson, and other Members of this Committee to review this proposal.

The Committee has already done good work to address the threat to national security and economic competitiveness imposed by Chinese-made drones, when we reported out the bipartisan American Security Drone Act last year. Among other things, this legislation

[1] The prepared statement of Senator Portman appears in the Appendix on page 41.

would prohibit the Federal Government from purchasing and using drones manufactured by our adversaries.

I am very concerned about reports of the purchase by DHS and DOJ law enforcement of Chinese drones and the national security risk that this poses. I am pleased that our legislation that we reported out of Committee but has not yet gone to the floor is included in the Senate-passed the U.S. Innovation and Competition Act of 2021 (USICA) package, and I urge our leadership, particularly Speaker Pelosi and the House, to swiftly pass USICA so this can become law.

With that said, I look forward to a productive conversation about the current drone threats to our homeland and actions being taken to prevent them. I look forward to hearing from the witnesses.

Thank you again, Mr. Chairman.

Chairman PETERS. Thank you, Ranking Member Portman.

It is the practice of the Homeland Security and Governmental Affairs Committee (HSGAC) to swear in witnesses. So if each of you would please stand and raise your right hand.

Do you swear that the testimony you will give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Ms. VINOGRAD. I do.

Mr. WIEGMANN. I do.

Ms. COULTAS. I do.

Chairman PETERS. Thank you. You may be seated.

Today's first witness is Samantha Vinograd, the Acting Assistant Secretary for Counterterrorism and Threat Prevention and Law Enforcement Policy in the office of Strategy, Policy, and Plans at the Department of Homeland Security. Ms. Vinograd began her career serving President George W. Bush as the Deputy U.S. Treasury Attaché to Iraq, and subsequently served on President Barack Obama's National Security Council (NSC) as Director for Iraq, Director for International Economics, and Senior Advisor to the National Security Advisor.

Previously she was a Cable News Network (CNN) national security analyst, a senior advisor at the Biden Institute, and a visiting fellow at the University of Chicago Institute of Politics.

Ms. Vinograd, welcome. You may proceed with your opening remarks.

TESTIMONY OF SAMANTHA VINOGRAD,[1] ACTING ASSISTANT SECRETARY FOR COUNTERTERRORISM AND THREAT PREVENTION AND LAW ENFORCEMENT POLICY, OFFICE OF STRATEGY, POLICY, AND PLANS, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. VINOGRAD. Chairman Peters, Ranking Member Portman, and distinguished Members, thank you for inviting me to testify about the Department of Homeland Security's efforts to protect the homeland from the increasing threat posed by unmanned aircraft systems or drones.

Today I will explain how the Department has relied on authorities granted in the Preventing Emerging Threats Act of 2018 to

[1] The prepared statement of Ms. Vinograd appears in the Appendix on page 43.

counter the malicious use of drones and why we are asking Congress to reauthorize and expand our counter-drone authorities to fill specific gaps that are exposing the homeland to serious threats. We are committed to judiciously and responsibly implementing our authority so that we can stay ahead of the threat while protecting privacy and civil rights and civil liberties in absolutely everything that we do.

The threat landscape from drones is heightened, and candidly, escalating extremely fast. Drones have been used to conduct dangerous kinetic attacks, have interfered with aircraft and airports, have been used to survey, disrupt, and damage critical infrastructure and services, and more. Nearly every day, transnational criminal organizations use drones to convey narcotics and contraband across U.S. borders. In fact, CBP has detected more than 8,000 illegal cross-border drone flights at the Southern Border just since August 2021.

In light of this threat environment, it is critical that DHS has the authorities to protect the homeland from UAS threats, consistent with our statutory missions. To date, DHS has relied on the Preventing Emerging Threat Act to carry out critical C–UAS mission sets, including protecting the President and Vice President, safeguarding sensitive assets, facilities, and special events in the maritime sector, protecting Federal facilities and personnel, and countering illicit narcotic and contraband trafficking.

Based on our experience through over 300 deployments there is clear evidence that there are gaps in our authorities which are exposing the American people to significant risk. For example, even though the Transportation Security Administration (TSA), is responsible for protecting airports it lacks authority to proactively and persistently protect transportation infrastructure from drone threats and avert disruptions and real tragedies. This is especially concerning since TSA has reported nearly 2,000 drone sightings near U.S. airports since 2021, several of which have resulted in pilots taking evasive action, 65 evasive actions in fact, and the disruption of airport operations.

Furthermore, State, local, tribal, and territorial (SLTT) law enforcement are often the first responders when a malicious drone incident occurs, but they are not currently authorized to detect or mitigate drone threats, thereby delaying a response. Critical infrastructure owners and operators are often the victims of drone surveillance and have even been targeted for kinetic attacks, but they have no authority to detect drones or to request mitigation from authorized law enforcement.

Bottom line, air partners are absolutely critical to protecting the homeland from UAS threats but lack the authorities to do so, which again exposes the homeland and the American people to significant risk. DHS, therefore, strongly supports the Administration's legislative proposal to reauthorize DHS's and DOJ's current C–UAS authorities as well as to expand them to remedy the gaps that I have identified. It would grant TSA the authorities it needs to protect the nation's transportation system from UAS threats. It would also authorize SLTT partners and critical infrastructure owners and operators to engage in detection of C–UAS.

Last, it would create a limited pilot program for SLTT law enforcement to engage in C–UAS protection activities in their jurisdictions under the strict oversight of DHS and DOJ. The proposal would require that authorized SLTT and critical infrastructure owners and operators adhere to comparable safeguards and standards to those that we Federal entities follow. Non-Federal entities would be required to use federally approved equipment, receive standardized training and certification, conduct risk-based assessments, coordinate with FAA to ensure aviation safety, and very importantly, adhere to Federal privacy and civil rights and civil liberties protections.

We cannot keep pace with this threat environment without these additional counter-drone authorities—it just is not possible—and we hope that this Committee will champion them. Congressional action is urgently required as our current authority will expire in less than three months, and a lapse would be catastrophic.

I thank the Committee for holding a hearing on this important topic and look forward to your questions.

Chairman PETERS. Thank you, Ms. Vinograd.

Our next witness is Brad Wiegmann, Deputy Assistant Attorney General (AG) in the National Security Division at the Department of Justice. Mr. Wiegmann brings a wealth of government experience, having served in legal positions at the Department of Defense (DOD) and the National Security Council over the span of two decades.

Previously, Mr. Wiegmann worked at the private law firm of Shea and Gardner, where he focused on civil litigation and legal policy matters. He has also served as a law clerk for Judge Patrick Higginbotham on the United States Court of Appeals for the Fifth Circuit.

Mr. Wiegmann, welcome to the Committee. You may proceed with your opening comments.

TESTIMONY OF BRAD WIEGMANN,[1] DEPUTY ASSISTANT ATTORNEY GENERAL, NATIONAL SECURITY DIVISION, U.S. DEPARTMENT OF JUSTICE

Mr. WIEGMANN. Thank you, Chairman Peters, Ranking Member Portman, and Members of the Committee. Thanks for the opportunity to testify today on behalf of the Department of Justice.

We strongly support the Administration's legislative proposal to allow us to continue to protect major national events and important Department facilities from the threat posed by misuse of drones. This legislation would also enable us, as Assistant Secretary Vinograd just said, to expand our counter-drone efforts both with respect to the types of facilities that we can protect and to empower our State and local partners to participate in this critical mission.

We understand at DOJ that drones are bringing great benefits to our society and our economy, but like many advances in technology, drones also bring serious risk to the public when they are misused. As has been alluded to already in the opening statements, we are seeing an increase in the use of drones for a wide spectrum of criminal and other dangerous activities. They can be weaponized

[1] The prepared statement of Mr. Wiegmann appears in the Appendix on page 51.

to conduct attacks using firearms, explosives, or other materials, they can conduct cyberattacks against wireless devices or networks, and they can conduct espionage or trafficking narcotics and contraband.

Beyond these nefarious uses, drones are often used carelessly to create hazards to the public. Let me just give you a few recent examples.

In February 2020, a subject was arrested and charged in connection with his efforts to use a drone to drop explosives near a Georgia mobile home park. Between September 2021 and February 2022, four defendants pled guilty to a conspiracy to deliver contraband via drones into Fort Dix Prison in New Jersey. We have recently seen Mexican drug cartels using drones to drop bombs on their rivals in Mexico as well as to traffic drugs into the United States.

In May of this year, a defendant was sentenced after using a drone to drop flyers over spectators at two separate National Football League (NFL) games in California, and it obviously could have been something much worse than flyers.

Under the current authority that Congress has granted, the Federal Bureau of Investigation (FBI) has conducted 70 counter-drone protection operations at large events, ranging from the Super Bowl to New Year's Eve celebration in Times Square. That represents only 0.05 percent of the over 121,000 events during that time for which an assessment was requested so that counter-drone support could be provided. The demand for counter-drone support has far outstripped the Federal Government's limited resources.

During those 70 operations by FBI, our counter-drone teams detected 974 noncompliant drones in restricted airspace. They located the operator in 279 cases, and they attempted mitigation against 50 drones.

Our current authority, as Chairman Peters mentioned, to counter drones expires in October, if it is not extended by Congress. The reason we need this authority is because our use of this technology would otherwise run afoul of various criminal statutes. Our legislative proposal would extend our current authority permanently and would expand it to address some critical gaps. I want to talk about a few of those briefly in my opening statement.

First, as has been mentioned, the legislation would authorize State and local law enforcement and owners and operators of critical infrastructure to use certain detection-only capabilities. We need to empower others to help us take on this responsibility. Notably, the detection-only technology does not jam or otherwise disrupt drones or other aircraft, and therefore it does not pose any risk to the safety of the national airspace system (NAS). This can be safely done today.

Second, the legislation would authorize a limited pilot program for up to 12 State and local law enforcement entities each year to engage in both detection and mitigation activities. By mitigation I mean actually interfering with the flight of the drone. This would allow our State and local partners to protect sensitive State facilities and mass gatherings in their jurisdictions. The participants in the program would be required to receive training and vetting and to follow the same rules as Federal agencies must currently follow,

and all of their activities would have to be coordinated in advance with Federal partners, including the FAA, which could withhold approval if there was a risk to the national airspace.

Third, the legislation would enable the Marshals Service to protect high-risk prisoner transports. Current authority covers our prisons and our courthouses but it does not expressly address high-risk prisoner transport, so it would fill that gap.

Finally, I want to say a word about privacy and civil liberties. We are committed to ensuring that we respect all constitutional rights and privacy as we conduct our counter-drone activities. The technologies we employ typically detect only communications being passed between the controller and the drone to direct its activities. They do not extract text messages, email, or internet search histories from phones or tablets used to control drones, nor do they allow us to listen to voice calls.

We typically collect information such as the drone vendor and model, the controlling device serial number, the geolocation of the drone, the location of the controller, and the most recent takeoff location. This is much like the information that is going to be required to be broadcast by the new remote identification (ID) rule and is currently required for manned aircraft.

As is required in current law, DOJ would continue to have guidance that contains express protections for privacy and civil liberties and State and locals would be required to follow these same rules.

I appreciate the opportunity to testify today and look forward to answering your questions.

Chairman PETERS. Thank you, Mr. Wiegmann.

Today's final witness is Tonya Coultas, Deputy Associate Administrator for Security and Hazardous Materials Safety at the Federal Aviation Administration at the Department of Transportation (DOT). In her role, she provides executive oversight of national security policies, plans, and programs involving manned and unmanned systems in addition to several other security-related topics.

Ms. Coultas has over 30 years of combined local, State, Federal, executive, and military experience, supporting defense, intelligence, safety, disaster response, and crisis management efforts. Previously Ms. Coultas served as a senior executive for the DHS National Protection and Programs Directorate (NPPD), now Cybersecurity and Infrastructure Security Agency (CISA), at the Office of Infrastructure Protection (OIP), and for the Federal Emergency Management Agency (FEMA).

Ms. Coultas, welcome to the Committee. You may proceed with your opening remarks.

TESTIMONY OF TONYA D. COULTAS,[1] DEPUTY ASSOCIATE ADMINISTRATOR FOR SECURITY AND HAZARDOUS MATERIALS SAFETY, FEDERAL AVIATION ADMINISTRATION, U.S. DEPARTMENT OF TRANSPORTATION

Ms. COULTAS. Chairman Peters, Ranking Member Portman, and Members of the Committee, thank you for inviting me to speak with you today about the FAA's role in assuring safety, security, and efficiency of the nation's airspace as it pertains to unmanned aircraft system or drones. At the FAA, we are constantly working to welcome these beneficial new technologies into the national air system while minimizing any impacts to our existing air transportation system and to the public.

Every day, commercially operated UAS contribute to our economy by inspecting infrastructure, supporting agriculture and other industries, assisting public safety agencies, and conducting a myriad of other tasks. Congress has recognized these tremendous benefits to our economy and society and has been fully supportive as we integrate this technology into our airspace in a safe and secure manner.

However, the FAA does acknowledge that potential misuse of this technology poses unique security challenges that enable malicious actors to exploit vulnerabilities or circumvent traditional ground-based security measures for our security partners.

For that reason, Congress authorized the Departments of Defense, Energy (DOE), Justice, and Homeland Security to use technologies designed to response to UAS that pose a threat within their mission responsibilities. You directed the FAA to work with these agencies to ensure that detection and mitigation measures do not compromise the safety and efficiency of the airspace.

The FAA's chief role is to support our partners' testing and eventual use of these detection and mitigation systems, many of which use radio frequency (RF) and other technologies that could potentially interfere with air navigational systems, communication, avionics systems which are all critical to safety of flight.

Along with developing our plans for certification of USA detection and mitigation systems, the FAA is also tasked with testing and evaluating these technologies for potential use near airports. We and our security partners have developed agency-specific and jointly agreed upon processes to determine when, how, and what detection or mitigation technologies can be safely used in a particular location. We also develop notification protocols to be used during an active detection or counter-UAS event.

The Administration's proposal to expand UAS detection and mitigation authorities so that other Federal departments and agencies, as well as other public and private critical infrastructure entities, will be able to use tested system to safely protect sensitive facilities, operations, and people from the malicious or errant use of UAS.

The proposal, which the FAA does support, would, among other things, give limited UAS detection-only authority to the non-Federal law enforcement community as well as airports and critical infrastructure owners and operators. It would also create a tem-

[1] The prepared statement of Ms. Coultas appears in the Appendix on page 58.

porary pilot program for non-Federal law enforcement to begin using UAS mitigation technologies under Federal oversight.

In addition, the FAA would be authorized to assess civil penalties against those who use detection or mitigation technologies in an unauthorized manner that endangers the national airspace, all areas of new or expanded authorities include robust safeguards to ensure the current level of safety in the NAS is preserved.

We recognize that expanding UAS mitigation authorities beyond our current Federal partners will present challenges, and for that reason the proposal for the pilot program reflects an incremental approach to evaluating such authorities and safeguards that include interagency coordination on participant selection, training of system operators, and requires program participants to work through DHS and DOJ in coordination with the FAA.

There is no question that a seamless security framework is critical to advancing the Administration's goal of fully integrating UAS into the NAS, maximizing the public benefits from this technology. By taking deliberate steps to support those entities, with duties to protect against emerging UAS base threats, the United States will continue to lead the way in the full integration of UAS while maintaining the safest, most efficient, and most secure airspace system in the world.

We thank the Committee for its leadership on this issue and look forward to working together to balance safety and innovation with security.

Chairman PETERS. Thank you, Ms. Coultas.

This Committee is constantly focused on all of the threats that the homeland faces on a daily basis. Clearly the three of you have outlined significant threats posed by UAS. My question for you, Mr. Wiegmann, is how would the FBI assess the potential threat from UAS along the threat spectrum? Is this low, is this medium, or is this high, and why?

Mr. WIEGMANN. I think what I would say, as the FBI director has testified before, this is a very significant threat. Given the easy ability to buy a drone, commercially, it is easy to get, they are very easy to use, and not that difficult to weaponize, as we have talked about. That is what we are seeing some of already.

The FBI Director predicted a few years ago that we would see a drone attack on a mass gathering. Happily, we have not seen one yet but I think it is a matter of time until we do see that type of misuse of drones for an attack in the United States.

Chairman PETERS. Thank you. Ms. Vinograd, in your testimony you discussed the potential use of UAS as both weapons as well as interference tools that could target airports as well as other types of critical infrastructure here in the country. I would like to explain for the Committee more specifically what authorities does DHS currently lack to counter this threat, and what should this Committee focus on as we draft legislation to reauthorize the current legislation?

Ms. VINOGRAD. Senator Peters, thank you. As my colleague just noted, the threat posed by the malicious use of drones represents a significant and increasing risk to the homeland and the American people. Currently, under the Preventing Emerging Threats Act of 2018, we are authorized to engage in protective measure against

credible threats posed by UAS to the safety and security of certain DHS protective missions. That includes, for example, the protection of government personnel—President, Vice President—Federal facilities, sensitive assets in the maritime sector and elsewhere, as well as mass gatherings like Special Event Assessment Rating Events (SEARs) and National Security Special Events (NSSEs) in addition.

What we have witnessed over the last four years as we have judiciously and responsibly implemented our existing authorities is that there are significant gaps in our ability to protect the homeland from drones. We have seen an increasing number of malicious drone incidents in and around airports. We have witnessed 2,000 sightings of drones in and around airports since 2021. Since 2021, aircraft have had to engage in 64 evasive actions. That includes four commercial carriers doing so. There have been, on average, 30 airport disruptions each year. In these scenarios, seconds matter.

What we are seeking for the Transportation Security Agency is the ability, based upon this escalating threat environment, to engage in the proactive and persistent protection of the transportation sector, to include airports. This will literally, sir, help avert tragedy, tragedy both as it pertains to the potential loss of human life and economic impact. When airports have to shut down that costs millions of dollars. This will help avert tragedy.

Second, we are seeking authority for State, local, tribal, and territorial partners, as well as critical infrastructure owners and operators, to be authorized to engage in the detection of UAS. Those authorities would be implemented under the supervision and oversight of Federal departments and agencies.

We are also seeking the ability for a time limit of a six-year pilot program for State, local, tribal, and territorial partners to engage in mitigation of C–UAS, as it pertains to State, local, tribal, and territorial partners and critical infrastructure owners and operators. As the Committee knows, DHS relies on partners all around the country to help protect the homeland. We cannot be everywhere. What we know is that the threat posed by UAS is widespread across the country, and it is critical that our partners have the authority to help protect the homeland in addition to TSA getting the authority to critically protect the transportation sector.

Chairman PETERS. Thank you. Certainly we know that State and local enforcement agencies need additional authorities. Certainly they are going to be the tip of the spear when it comes to protecting our country from these threats, and working closely with the Federal Government agencies. However, there have been concerns that have been raised by folks that such an expansion creates some significant challenges in terms of training and preparedness.

Mr. Wiegmann, I want to ask this question. The Administration's proposal would establish a pilot program to test out these expanded authorities to State and local law enforcement. However, these entities need to have proper training, including how to protect individual rights to privacy as well as effectively executing this pilot program.

How would the Department of Justice ensure that these entities have the necessary training to properly execute these authorities?

Mr. WIEGMANN. Thanks for that question, Senator. Yes, training is a big part of it, as you recognize. We need to ensure that if State and locals are going to do this they know how to do it and they need to be operating under the right rules.

One of the elements of our bill is to establish a training center that the FBI would operate in conjunction with DHS. First of all, it would only be, under the pilot, up to 12 entities per year, but we would work with each of those entities that are designated to participate in the pilot program, do the training. They would have to learn what equipment could be used, learn how to operate it, learn what the rules are because they would have to follow the same Federal rules in terms of any data they collect, how it can be retained, disseminated, and used, when they can engage in mitigation activity, what the rules of engagement are. All of those are things they would have to be trained on and then certified.

Then even after that point, when they are doing their risk-based assessments as to which facilities or events they are going to protect, that is all subject to Federal oversight as well. This is not the kind of thing where we just hand it off to the States and let them take over. It is something that we, the Federal authorities, would continue to be actively involved in, both in training and making sure they are using the authorities appropriately.

Chairman PETERS. Ms. Vinograd, how will providing additional authorities to State and local enforcement better prepare the Department of Homeland Security to protect—and let us focus on mass gatherings such as National Security Special Events and Special Event Assessment Rating Events?

Ms. VINOGRAD. Senator, as I mentioned, DHS cannot be everywhere? We rely on State, local, tribal, and territorial partners to help us protect and to advance a variety of DHS missions.

If SLTT partners are granted this authority they can help prevent catastrophic attacks against mass gatherings, a variety of sizes and in a variety of venues. As my colleague, Mr. Wiegmann, just mentioned, these authorities would be implemented under strict supervision and oversight of the Federal Government, including ensuring that these individuals authorized to conduct these operations are operating under comparable Federal safeguards as they pertain to privacy and civil rights and civil liberties.

As I mentioned in the context of TSA and airports, when we are witnessing a drone threat seconds matter. Currently, SLTT authorities that are on the ground cannot detect proactively drones nor can they mitigate them. Those seconds that I mentioned, Senator, really matter, and the inability of our SLTT partners in their jurisdictions to respond could cost lives if our partners are not granted these authorities.

Chairman PETERS. Thank you. Ranking Member Portman, you are recognized for your questions.

Senator PORTMAN. Great. Thanks, Mr. Chairman. Thanks to the witnesses for the testimony. This is obviously a serious issue, and I agree with Ms. Vinograd who said that a lapse in the authorization would be catastrophic. I think it would help these transnational criminal organizations, among others, and yet we need better data to be able to put together the right authorization to write sound policy.

We know already what happens on the border with these drones. We know they are used for deliveries, not just for drugs but also currency and firearms, other contraband. This Committee has, among its responsibilities, oversight of DHS and these border activities, and we have a particular interest—I certainly do—in this issue of the synthetic opioids that are streaming across our border today. The number, unfortunately, are higher than ever. Last month, enough fentanyl was seized—which is the synthetic opioid that is killing about two-third of those who die from overdoses, which is at a record level—we know that there was enough seized to kill about 200 million Americans in one month, and no one on the border thinks that we are seizing most, and not even a significant percentage of what is coming across. It is a big issue.

Ms. Vinograd, a question for you. Understanding this increased threat from these transnational criminal organizations, how do you assess DHS's current performance in countering the use of drones for cross-border illicit activity?

Ms. VINOGRAD. Senator, thank you. I share your concern about transnational criminal organizations and the malicious use of drones over the border, both as it pertains to smuggling contraband as well as surveillance of law enforcement, in addition to other threats.

Currently, DHS, the Secretary of Homeland Security, has designed three areas of operations along the Southwest Border as covered facilities or assets. This allows DHS, CBP more specifically, to engage in C–UAS operations in these areas of operations.

Senator PORTMAN. Let me be more specific because I do not have much time. In your testimony you state that from August 2021 to May 2022, CBP detected more than 8,000 illegal cross-border drone flights at the Southern Border. Of these 8,000 flights, how many were successfully mitigated by DHS?

Ms. VINOGRAD. Senator, I can ask CBP to get back to you and your staff with the specific statistics on that.

Senator PORTMAN. We have been asking them for this since February, persistently, and we are not getting the information. I think it is important that we have an authorization, but we have to have information. If we do not have the statistics today, if you do not have it, despite many inquiries from us, that concerns me. I want to work with, again, on this reauthorization, but we have to have better information to be able to do it properly.

With regard to drones, let's talk about China for a moment. Recently the Directors of the FBI and British M–15 warned of the national security and economic threats posed by China. They identified it our greatest long-term threat, stealing our technology, dominating our markets, and they talked about the U.S. drone market, and they talked about the use of drones.

Here is an example. According to a report by The Washington Post, China's Da-Jiang Innovations (DJI) is the leading provider of drones to U.S. law enforcement agencies, they say. DJI has servers in China. They have support from the Chinese government. The Chinese State Security Services is one of their customers. Here is our own Commerce Department saying DJI has been added to an export blacklist last after Bloomberg reported that it supplied surveillance technology to Chinese security forces in Xinjiang, where

millions of Uighur Muslims have been forced into internment camps.

There is a report last year that the U.S. Secret Service (USSS) purchased eight of DJI's drones. The FBI purchased 18 of them. Let me ask you these questions on the record. We will start with Mr. Wiegmann. Does the FBI currently purchase and use Chinese-made drones? Yes or no.

Mr. WIEGMANN. We do.

Senator PORTMAN. You do. Ms. Vinograd, does DHS currently purchase and use Chinese-made drones?

Ms. VINOGRAD. DHS has prohibited the purchase of foreign-made drones, small UAS, absent waivers in very specific circumstances.

Senator PORTMAN. OK. This report that I mentioned said that the Secret Service had purchased eight of DJI's drones. Are you saying that is inaccurate?

Ms. VINOGRAD. I am saying that with certain waivers——

Senator PORTMAN. My question to you is are you purchasing DJI drones or not, yes or no?

Ms. VINOGRAD. With specific waivers, DHS can purchase certain foreign-made——

Senator PORTMAN. Are you purchasing DJI drones, yes or no?

Ms. VINOGRAD. With certain waivers we are purchasing certain foreign-made——

Senator PORTMAN. So you are.

Ms. VINOGRAD. I can follow up with more specific details.

Senator PORTMAN. OK. But the answer is yes.

Ms. VINOGRAD. In a closed hearing I can provide more specific details, sir.

Senator PORTMAN. OK. Ms. Coultas, I do not want to leave you out. Does FAA currently purchase and use Chinese-made drones?

Ms. COULTAS. FAA's responsibility is for the integration of UAS into the NAS and testing of the UAS technology to ensure its safety and its use in the NAS. We do not actually purchase drones. We do the testing of the drones.

Senator PORTMAN. Thank you. Again, given what the FBI has told us, what the Commerce Department has told us, what we know from reports, I cannot believe we have to write legislation to force U.S. agencies to ban the use of Chinese-made drones, particularly where the servers are in China where the Chinese government is a part owner and a supporter of this particular company.

But we do have that in the USICA bill. It is a requirement in the USICA bill, and I hope we can get that legislation passed. If we cannot get that legislation passed, would you all support, including this kind of legislation, in whatever we do in terms of reauthorization? Ms. Vinograd.

Ms. VINOGRAD. I share your concerns about these drones and would welcome a conversation on specific language, sir, yes.

Senator PORTMAN. Mr. Wiegmann.

Mr. WIEGMANN. Just to be clear, we share the concern as well, Senator. We want to shift away from the use of Chinese drones, and the FBI and other parts of DOJ are working on that objective. Right now they kind of dominate the market so we are working to shift our use of drones away from Chinese drones to other alternatives.

In the meantime, FBI takes steps to do thorough cybersecurity and supply chain reviews to ensure that any risk posed by use of the technology is mitigated. But we do want to shift away from it.

We definitely support the aims of the sponsors of the bill. I think we have provided some technical assistance on some technical issues about changes we would make to the bill to make sure that we could support it and we could conduct our mission consistent with the provisions. But we share the objectives of shifting away from these drones and using other alternatives that do not pose the same type of supply chain risk.

Senator PORTMAN. Yes. Thank you. The Administration supports the legislation, the USICA legislation, and we did negotiate it with the Administration as well as Democrats and Republicans here in the U.S. Senate. We appreciate your support of the broader legislation and I hope we continue to work with each of you on both of these issues, getting better data as to what is actually happening, particularly along the border we have a special interest in this Committee, but also with regard to the use of these drones and the potential national security threat of having this information be relayed back to China and used against us.

Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Senator Portman. Senator Johnson, you are recognized for your questions.

OPENING STATEMENT OF SENATOR JOHNSON

Senator JOHNSON. Thank you, Mr. Chairman. Five years ago when we were drafting and passing the Preventing Emerging Threats Act of 2018, we obviously understood the threat that drones pose to this Nation, the very serious threat. I was very frustrated at the time that we could not offer greater authority. After being here five years later I am enormously frustrated that we have not made greater progress. I mean, we are still taking what I would consider baby steps when to me it is out of control. 2,000 sightings around airports, 69 evasive actions.

Let us get down to brass tacks here. Let us find out what our capabilities are. Have we, under the current authorities, have we actually brought down drones around the types of events that DHS can counter?

Ms. VINOGRAD. Senator, DHS has engaged in detection and mitigation of drones, concurrent with the authorities——

Senator JOHNSON. So we have taken down drones. Have we advanced our technology in five years?

Ms. VINOGRAD. We have certainly advanced our technology in five years. Yes, sir.

Senator JOHNSON. Do we have the capability right now to prevent drones from entering restricted airspace around an airport?

Ms. VINOGRAD. Currently DHS assesses that TSA could respond to an emergency in and around an airport. What we are seeking in the legislation is the ability for TSA to proactively and persistently——

Senator JOHNSON. OK. I am asking what is our capability right now, if you have the authority. First I have to find out who has the authority to establish a restricted airspace, around an airport, around a stadium, around power plants? Who has that authority?

Ms. COULTAS. The FAA, sir.

Senator JOHNSON. The FAA. Have we established that restricted airspace?

Ms. COULTAS. We work with our Federal partners as well as our non-Federal stakeholders, when requested——

Senator JOHNSON. Is the airspace around an airport restricted to drone use right now?

Ms. COULTAS. Yes.

Senator JOHNSON. All airports?

Ms. COULTAS. Yes.

Senator JOHNSON. Do we have the capability of knocking down drones if they enter that restricted airspace? Do we have that capability—maybe not the authority but do we have the capability, technologically?

Ms. COULTAS. Technologically, yes, we have the ability to mitigate malicious drone threats.

Senator JOHNSON. So should not this legislation, at a minimum, grant you the authority so we can almost immediately start knocking down drones when they enter that restricted airspace around airports?

Ms. VINOGRAD. Senator, DHS is deeply supportive of TSA getting the authority to mitigate drones around airports.

Senator JOHNSON. Now let us start expanding it, because to me that would be the No. 1 priority.

Mr. Wiegmann, there is no constitutional right to have a drone. Correct?

Mr. WIEGMANN. No.

Senator JOHNSON. You mentioned civil liberties. What civil liberty are contemplated if we are knocking down drones entering into a restricted airspace?

Mr. WIEGMANN. We would want to do so responsibly, only when it posed a threat.

Senator JOHNSON. Sure. We do not want to knock them down and create a greater problem. But, there would be no civil liberties issues. If we established a restricted airspace and somebody flies in a drone, they have no civil liberties to worry about. We are going to knock down that drone safely, if we can.

Mr. WIEGMANN. I agree, Senator. I do not think that presents a civil liberties issue.

Senator JOHNSON. I could not quite understand you.

Mr. WIEGMANN. I agree with you, Senator. I do not think it poses a risk——

Senator JOHNSON. OK.

Mr. WIEGMANN. When a drone is flying in restricted airspace, to interdict that drone is not a civil liberties issue, in my view.

Senator JOHNSON. In the proposal the Administration gave us, have we contemplated the priorities of establishing restricted airspace and granting the authority to be knocking down drones when they enter restricted airspace? For example, I am contemplating around a stadium on game day. Establish that as temporary restricted airspace so that State and local authorities, working with DHS, have the ability to knock those drones down, take them out of the sky before they pose a threat.

Mr. WIEGMANN. We have that authority now, Senator. That is what we are asking to extend. But yes.

Senator JOHNSON. Have we knocked down any drones around stadiums?

Mr. WIEGMANN. When you say "knock down," yes, we have disabled them. We have required them to divert and land or we have interdicted them. Yes, we have. At a number of events, as I mentioned in my opening testimony, we have done that, yes.

Senator JOHNSON. OK. Again, my main point here is we have to move faster. It is great to have pilot programs, but that is five, six years in the future. Trust me. The public is going to demand that we act a whole lot quicker if a commercial aircraft hits a drone that is in the restricted airspace.

I want to make sure, in this piece of legislation, we have that authority, and then the funding and the personnel to start protecting our restricted airspace as soon as possible. Is there anything that is going to prevent that from happening in this piece of legislation?

Mr. WIEGMANN. That is why we are here, Senator. We agree with you and we are seeking the authority to do just that.

Senator JOHNSON. But again, I am a little concerned about a pilot program that is going to work with 12 State, local, and tribal——

Mr. WIEGMANN. It is going to take some time.

Senator JOHNSON. That is a pretty slow rollout, is it not?

Mr. WIEGMANN. It is going to take some time to ramp up, but it is 12 every year. It takes some time to do the training, to get up and make sure they are doing this and know how to do it, and get the technology down.

They will be able to do multiple missions, and over time we think that is——

Senator JOHNSON. My point is we have already taken five years, which I find enormously frustrating. Sure, it takes time, but we can ensure that it takes less time if we prioritize this as a serious threat and we establish this as a priority for putting more personnel to make sure it takes less time. Do you understand what I am saying?

I think 12 pilot programs a year is completely too little, and I am hoping it will not be too late. Let us look at this piece of legislation. Let us start ramping it up, OK? We spend trillions of dollars in the Federal Government. We ought to focus on this because this is a serious threat. Again, I do not want to have it be too little, and I certainly do not want us to be too late on this.

Mr. Chairman, again, I appreciate you pushing this. I want to work with you to strengthen this. I do not think this is strong enough yet. Again, let us not have a piece of legislation that is too little, too late. The bill we passed five years ago was too little. Fortunately, it has not been too late yet. Let us make sure we do a good job on this one.

Chairman PETERS. Absolutely, Senator, and we look forward to working with you. I appreciate your continued leadership on this issue.

Senator JOHNSON. Thank you.

Chairman PETERS. We will make it as strong as we possibly can. We appreciate that. Thank you, Senator Johnson.

Senator Hawley, you are recognized for your questions.

OPENING STATEMENT OF SENATOR HAWLEY

Senator HAWLEY. Thank you, Mr. Chairman. Thanks to the witnesses for being here. Ms. Vinograd, if I could just start with you.

You work in the Office of Strategy, Policy, and Plans. Is that right?

Ms. VINOGRAD. Senator, let me just say I had my first visit to the State of Missouri on Friday.

Senator HAWLEY. Oh, good.

Where did you go?

Ms. VINOGRAD. I went to Jefferson City.

Senator HAWLEY. OK.

Ms. VINOGRAD. I just want to share I am deeply impressed by your Homeland Security professionals.

Senator HAWLEY. Thank you very much.

Ms. VINOGRAD. I look forward to going back. Yes, I work in the Office of Strategy, Policy, and Plans.

Senator HAWLEY. And you work with Robert Silvers there, is that right, the Under Secretary?

Ms. VINOGRAD. I do, sir.

Senator HAWLEY. Your name is on a memo with Mr. Silvers dated September 13, 2021. The subject is "Organizing DHS efforts to counter disinformation." This is the memo that recommended the establishment of the Disinformation Governance Board (DGB). It was turned over to me and to Senator Grassley by a whistleblower.

I have to tell you we have had the darndest time getting any information about this board out of your agency. We have asked and we have asked. Members of this Committee have asked. We would know virtually nothing had it not been for this whistleblower who turned over a tranche of documents, all of which are now public.

Since I have you here and you wrote the memo let me just ask you a question or two about it. Whose idea was it to establish this board?

Ms. VINOGRAD. Senator, the Department of Homeland Security has engaged in disinformation work pertaining to threats to the homeland and the American people for over a decade. With respect to this internal working group there were discussions about the need to ensure that there were guardrails in place across the Department to protect civil rights and civil liberties and privacy, and as such there were discussions about creating this internal working group.

Senator HAWLEY. Yes, all of that I know is in the passive voice. My question is whose idea was it to set it up? You used the words "working group" but I notice that that is not at all what the memo says. It does not call it a working group. The directive that Mr. Mayorkas eventually signed off on does not make this board a working group. It had managerial authority. It had directive authority. All of that is in these documents. So let us please not go back to those tired and now disproven talking points.

Let me come back to my question. Whose idea was it to establish the board? Was it yours?

Ms. VINOGRAD. Senator, without going into internal deliberations of the Department of Homeland Security there were a series of discussions among personnel.

Senator HAWLEY. Who?

Ms. VINOGRAD. I am not going to go into the internal deliberations of the Department.

Senator HAWLEY. Why not? You are under oath?

Ms. VINOGRAD. I am under oath, sir. That said, these are internal deliberations at the Department. As you know, sir, the charter was signed by the Secretary of Homeland Security.

Senator HAWLEY. Yes. I only know that, by the way, because of the whistleblower documents. We would not know that otherwise.

Ms. VINOGRAD. Senator, the charter was signed by the Secretary of Homeland Security. The working group included representation——

Senator HAWLEY. Does the charter call it a working group, since you bring up the charter?

Ms. VINOGRAD. This was a working group, sir.

Senator HAWLEY. Does the charter call it a working group?

Ms. VINOGRAD. I do not recall the charter——

Senator HAWLEY. No. The answer is it does not. Was it your idea to establish the board?

Ms. VINOGRAD. As I testified, Senator, under oath, the establishment of the working group was a decision taken, a conversation that was had among multiple individuals at the Department of Homeland Security.

Senator HAWLEY. OK. So you are not going to answer my question. Nina Jankowicz, she was appointed to run this Disinformation Board. How was she chosen?

Ms. VINOGRAD. Ms. Jankowicz was chosen consistent with practices for the hiring and vetting of political appointees.

Senator HAWLEY. Walk me through that process. Who was involved?

Ms. VINOGRAD. I do not know the full scope of that process.

Senator HAWLEY. You were not involved in it?

Ms. VINOGRAD. I was involved in one piece of that process.

Senator HAWLEY. What was the piece that you were involved in?

Ms. VINOGRAD. I spoke with Ms. Jankowicz.

Senator HAWLEY. At what point?

Ms. VINOGRAD. As part of the standard process for political appointees I spoke with Ms. Jankowicz.

Senator HAWLEY. What timeframe would this have been?

Ms. VINOGRAD. I do not want to give you an incorrect answer.

Senator HAWLEY. That is OK. Give me just a frame.

Ms. VINOGRAD. Early 2021.

Senator HAWLEY. OK. January?

Ms. VINOGRAD. I do not recall the exact date, sir. I can get back to you on that.

Senator HAWLEY. OK. January, February time period, perhaps? That would be early 2021. The Secretary signed the charter, I believe in February 2021. When did the Secretary sign off on Ms. Jankowicz being the head of the board?

Ms. VINOGRAD. Senator, I do not know that the Secretary signed off on Ms. Jankowicz or not.

Senator HAWLEY. Oh, really?

Ms. VINOGRAD. I am not aware.

Senator HAWLEY. He testified it was his decision.

Ms. VINOGRAD. I believe the Secretary testified that he was ultimately responsible for Ms. Jankowicz.

Senator HAWLEY. So it was not his decision?

Ms. VINOGRAD. Senator, I just said I do not know the full scope of——

Senator HAWLEY. Did you recommend favorably Ms. Jankowicz to the Secretary?

Ms. VINOGRAD. After speaking with Ms. Jankowicz I was impressed by her expertise during our conversation and noted my recommendation to others in the Department.

Senator HAWLEY. So you recommended, yes. I think that sounds like a yes. You recommended favorably.

Did you, at the time that you spoke with her and recommended with her, were you aware of her long history of comments on Twitter and other platforms of disinformation, anti-free speech rhetoric, and so forth, which has since become, I think it is safe to say, infamous?

Ms. VINOGRAD. Senator, I was aware of Ms. Jankowicz's expertise in the field of disinformation and was impressed by her expertise——

Senator HAWLEY. But did you know about her many comments, spreading disinformation about Russia, about the Trump administration, about conservatives. Secretary Mayorkas, just by comparison, said he was not aware of any of this at the time. I am just curious, were you aware at the time you recommended her to him?

Ms. VINOGRAD. Senator, in my capacity as Acting Assistant Secretary for Counterterrorism, Threat Prevention, and Law Enforcement Policy, I had not read all of Ms. Jankowicz's tweets, but as I said I was aware of her expertise in the field.

Senator HAWLEY. When you said you had not read all of her tweets, I am sure she has a lot of tweets, but were you familiar with the ones that have since become public?

Ms. VINOGRAD. I was not, sir.

Senator HAWLEY. OK. You were not aware at the time. Did anybody bring those to your attention, at any time, before they became publicly released in this vetting process?

Ms. VINOGRAD. No. Not to my recollection.

Senator HAWLEY. OK. Somehow she got through this vetting process with no one, including all the way up to the Secretary, apparently aware of what she had said on these public platforms. I find that sort of extraordinary.

Was the White House involved in the selection of Ms. Jankowicz?

Ms. VINOGRAD. I am not aware of the full scope of the process, sir. As a political appointee the standard processes were followed.

Senator HAWLEY. To your knowledge the White House was not involved. Is that fair to say?

Ms. VINOGRAD. My knowledge is a political appointee. The White House was involved in my process, so I believe that that is standard process for the White House to be involved.

Senator HAWLEY. OK. So you think that they were involved in the selection of Ms. Jankowicz.

Ms. VINOGRAD. I am not aware of the full scope of the hiring or vetting process. It was the same as pertains to other political appointees.

Senator HAWLEY. I am just trying to get at what your knowledge is. I am not asking you what you think may have happened, but to your knowledge was the White House involved in selecting Ms. Jankowicz? Just yes or no.

Ms. VINOGRAD. I really do not know, sir.

Senator HAWLEY. OK. You have no idea. All right. What is the current status of the Disinformation Board, to your knowledge?

Ms. VINOGRAD. It is on pause.

Senator HAWLEY. What does that mean exactly?

Ms. VINOGRAD. It means the Disinformation Governance Board never met. The Secretary has asked the Homeland Security Advisory Committee (HSAC), to review how the Department can most effectively address disinformation and how to do so in a way that protect civil rights and civil liberties. He has also asked that the HSAC review how the Department can be as transparent as possible with the American public and increase trust in the work that we do. The HSAC was asked to conduct their review within 75 days, and while that work is pending the Disinformation Governance Board, is on pause. It is not meeting. There is not work underway.

Senator HAWLEY. Last question, and I know there are other Senators waiting to ask questions. Did the board every meet? Did any members of the board ever meet with Twitter executives? We have minutes of planned meetings with Twitter executives to ask for cooperation in tracking speech. Did that ever happen at any point, to your knowledge?

Ms. VINOGRAD. I disagree with your characterization of——

Senator HAWLEY. Did the meetings with the Twitter executives ever happen, to your knowledge?

Ms. VINOGRAD. If I can finish, I disagree with your characterization of the purpose of a meeting that never happened. The meeting with Twitter never happened.

Senator HAWLEY. OK. To your knowledge it never happened.

Listen, I have to let other Senators question. I will just say that I regret that it has taken months to get the most basic information about this board, and again, we would know none of this, none, had it not been for a whistleblower who turned over these documents. Frankly, that is totally unacceptable.

Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Senator Hawley. Senator Carper, you are recognized for your questions.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thanks. Welcome to each of our witnesses. I want to start with Ms. Coultas. Do you pronounce your name Coultas?

Ms. COULTAS. That is correct, Senator.

Senator CARPER. All right. Thank you. In your testimony I believe, ma'am, that you mentioned that unmanned aircraft systems, also known as drones, represent the fastest-growing sector in aviation today. I understand that as of September 2020, about two

years ago, there were 1.7 million drones that were registered with the FAA and that this number will only increase in the years to come.

That said, could you just take a minute or two and explain to us how the expansion of drone use has impacted the current threat landscape and how the FAA plans to grapple with continued disruption to U.S. airspace by drone users?

Ms. COULTAS. Thank you, Senator, for that question. What the FAA currently does to contribute to the security of the airspace——

The FAA has been doing a number of things, working with our security partners and our non-Federal stakeholders over the last several years as UAS continue to be integrated and grow across the economy, both with industrial users of the drones as well as hobbyists and industry. Things that we have been doing to help mitigate and work with our security partners and ensure the safety of the NAS, which obviously is FAA's No. 1 priority is to ensure that as drones are integrated into the NAS that it is done in a safe manner and does not affect the rest of the NAS as well as passenger commercial flights.

Things that we have been doing is we authorize and we put in existing what we call temporary 99.7s, working with our security partners who will request temporary air restrictions over certain events, who meet certain security measures and needs necessary. Some of those may be mass gathering events. We have talked here about stadiums, Super Bowl, and other types of events, the borders. There are other events that go on nationwide throughout the year that we work with our security partners to put in also those additional air restrictions around those events.

We also look at conducting tabletop exercises (TTXs), again working with the State, local, tribal, and territorial and Federal partners when they are at these events and using such scenarios that if a drone would come into the airspace or if we have, as you heard said, careless or clueless or maybe a noncompliant or potentially a criminal actor of a drone, how would we actually respond? Who has those authorities? What does that response and coordination look like? We have been working on that for the last several years.

In addition, we have remote ID, which starting September of this year manufacturers will be required to have all drones manufactured to have what we call a self-identifier or a licensed place. All drones manufactured after September will have to have that on all drones, and operators of drones will have to be compliant with the remote ID rule by September of next year.

Senator CARPER. All right. Thank you.

My second question would be one I would address to each of you, and all take a shot at it, if you would, please. Protecting our homeland security is, I think, of the utmost importance when it comes to addressing threats posed by drones. Ironically, last week my family was at a beach together, and one of the visitors that joined us at the beach brought their drone, and sat it down in front of us, sent it out over the ocean some distance, and almost out of sight, brought it back, taking pictures of us and others. Pretty amazing.

Two or three days ago I was back home in Wilmington, Delaware, and we are experiencing an epidemic of off-road dirt bikes in Wilmington, and all kinds of cities across the country, where these

people get on the streets and they ride their dirt bikes all over the place and create mayhem and havoc. One of the tools to try to stop that is to track them using drones. Actually, the drone can be used not just to support criminal activity but actually to stop them, and I think we need to be mindful of that.

Protecting our homeland security is of the utmost importance when it comes to addressing the threats posed by drones, given that they can be used by criminals to conduct illegal surveillance and espionage as well as trafficking of drugs and firearms. As such, close coordination with the Department of Homeland Security, Department of Justice, and Federal Aviation Administration is critical when it comes to mitigating these threats.

Could each of you take a moment or two to explain how your respective agencies work together, not as a stovepipe but work together, and with your State and local counterparts to monitor and counter threats posed by drones?

Ms. Vinograd, would you take the first shot at that, please?

Ms. VINOGRAD. Certainly, and let me just say, sir, that I agree. The Department of Homeland Security agrees that drones have a variety of beneficial uses—emergency response, deliveries, recovery, investigative purposes, and so much more. What we are focused on is the malicious use of drones, whether intentional or unintentional.

Your question about cooperation is critical because the Department of Homeland Security just could not utilize its current C–UAS authorities absent incredibly close participation with our Federal partners, to include, for example, the FAA. As we seek the Secretary's authorization, for example, to designate a covered facility or asset, which would then allow us to engage in C–UAS activities, we are coordinating every piece of that authorization with the FAA, for example.

When we get a request for C–UAS activities to protect a SEAR event or an NSSE event or a mass gathering at the request of the State executive, that request goes into an interagency working group that reviews the risk, reviews the threat, reviews capabilities, reviews who is best positioned to respond, and more. We got a question earlier, sir, and I will stop here, about temporary flight restrictions (TFRs). DHS works incredibly closely with the FAA when DHS or parts of DHS request a TFR with FAA to implement that TFR, and we are necessary to grant waivers to allow for authorized activity to include First Amendment-protected activity as well.

Senator CARPER. All right. Thank you, ma'am. Mr. Wiegmann.

Mr. WIEGMANN. Yes. I would just heartily agree with that. I think the counter-drone business is very much a team sport. Everything we do we work hand-in-glove with DHS and with FAA. We have to whether we want to or not, to work on TFRs and so forth, to get them. So everything we do we work together. Horizontally, there is a lot of collaboration, and then also we are starting to do more of the what I would say vertical, with our State and local partners, including in Delaware. My understanding is that Delaware State Police is part of our State and local working group on drone activity, and so that is a group that we have and convene. If we get the authority that we are asking for today we will be

working more much intensively with State and locals all across the country, both on their detection-only activities but also with the pilot program that we described.

This is an activity where law enforcement and Homeland Security officials are working together all the time, together with FAA.

Senator CARPER. All right. Thank you. My time has expired. I will have the opportunity to submit some questions for the record because I have several more I would like to offer. Thanks so much for joining with us today and for your collaboration and for your commitment. Thanks so much.

Chairman PETERS. Thank you, Senator Carper. Senator Lankford, you are recognized for your questions.

OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. Mr. Chairman, thank you. Thank you to all of our witnesses as well today and for the ongoing work. I do have some questions about the collaboration you all were discussing at this point.

When I was visiting with some of the folks at our Southern Border several months ago, there were some of our border stations that were trying to get counter-UAS equipment up and running and operable. In one of our areas along the border we had over 10,000 incursions in just that area with the UAS coming across the border from Mexico into the United States, and they were very eager to be able to get that.

When I asked what is the issue, the equipment was there, the people were there, they waiting on authorization and there was an ongoing dialog between DHS and FAA to be able to discuss how we were going to get this up. So literally the equipment, the people, the need, everything was there.

My question is about this collaboration. How long does it take? In this particular instance we had a situation where that same equipment along the border was being used in a different region of the border, and had been used for a while, but in this particular region it took month to actually get counter-UAS equipment up and working in that area. How do we speed up this process? Where is the slowdown?

Ms. VINOGRAD. Senator, as noted earlier I share your concern about the malicious drone threat at the Southwest Border. I will turn to my colleague from FAA in a moment.

As you know, sir, the Secretary of Homeland Security has authorized three areas of operations along the Southwest Border as covered facilities or assets, so we have three up and running, if you will. There are four additional AORs that are pending.

We have taken significant steps internally to make the process internally more efficient between CBP and the Program Management Office (PMO), which is part of my team. In addition, we have started doing, safely, concurrent processes with FAA such that this can move as expeditiously as possible.

There are four areas of operations—I do not know if it is one of the ones that you visited—four areas of operations still pending. I will tell you it is a priority for me, it is a priority for the Secretary, to get these authorized as quickly as possible.

Senator LANKFORD. What is the holdup, because this is months when that same technology is used in other places along the border. Where is the spot where it is getting stuck?

Ms. VINOGRAD. I will turn to my colleague from FAA in a moment, but as these AORs are in the process of being authorized there is a lot of coordination with the FAA, and each covered facility or asset, sir, is different, so there are different complexities in each area of operations.

Now again, we are committed to doing this quickly. The threat is significant. But each area of operations is different, which is why we coordinate with the FAA.

Senator LANKFORD. I get it. We are still back to the same spot. This seems to be defining quickly along geologic time rather than clock time on it, because it is taking months in process. When I have interacted with the Secretary it is on FAA's desk, and then I talk to the FAA and they would say, no, it is on the Secretary's desk. It just seems to be getting lost. What I am trying to figure out is how to get this unstuck.

Ms. VINOGRAD. I cannot go into further details in this hearing except on one thing. On one of the AORs, sir, it is a matter of just a few weeks, at a maximum. The others are a little bit more complex, and I would be glad to speak with you in a closed session, just more specifically about what that looks like. But we are committed to doing this with urgency and with care.

Senator LANKFORD. Great. Thanks. How long does it take to be able to get one of these coordinations done with FAA, to be able to look at an existing technology that is out there in a new geographic region?

Ms. COULTAS. It varies based on the technology and the location and the complexity of the request that we receive. In some cases it can take just a matter of days to issue a TFR, but then others it does take longer, depending on what the actual area is and other TFRs that may be in the area.

Senator LANKFORD. Can you define "longer" for me? Because a matter of days I can get. What does "longer" mean?

Ms. COULTAS. I am not in the area of issuing the TFRs, so it varies. We are working with our security partners now and also other areas of the country where they are trying to get TFRs. So it can vary. As long as we have the information, working closely with our security partners, in getting that. I cannot give you a definitive how long, because the operations in all vary.

Senator LANKFORD. Here is my challenge on this, and I will just take one specific region on the Southwest Border. When I go there and I see the people, I see the equipment, everyone is trained, everyone is ready to go, and they are waiting on a piece of paper to be signed somewhere in Washington, I get on the phone and start calling around and saying, "Where is this? How do we get this unstuck?" because they are dealing with, literally, at that point, thousands of UAS coming across from Mexico, carrying narcotics, doing surveillance. We have the technology sitting there. I am trying to figure out how do we get this unstuck, because it is on someone's desk, moving, doing something. If there is a need to assist in process, this Committee is very engaged to be able to help get processes unstuck, but we are trying to figure out why it is still stuck.

Ms. VINOGRAD. Senator, I try to be in the business of unsticking things as well, and I will tell you that for the one that I mentioned that is forthcoming in just a small number of weeks, what we are waiting for in that particular context, and in others, is to ensure that this equipment can be safely used and operated in that airspace. I am happy to follow up with more details in a closed session, but we, again, are deeply committed to ensuring that this first AOR happens in a very small number of weeks and that the other additional AORs that, again, are just more complex from the airspace perspective, are unstuck quickly as well.

Senator LANKFORD. Yes. How long has that one been pending? You said that one is going to get unstuck in weeks. How long since when it first started?

Ms. VINOGRAD. I do not have the exact date in front of me, sir, but when you say "first started," it has been just a few weeks since we can move to this next stage of basically looking at this particular airspace and the complexities there and ensuring that the equipment can be safely used. But I can get you a more specific answer in writing.

Senator LANKFORD. That would be helpful. Let me ask this same question when we deal with Bureau of Prisons (BOP) and how this is managed. Obviously, a huge issue with cellphones being snuck in, individuals that are actually operating their gangs and criminal activity, stalking people that they had threatened outside of that facility from inside the facility, bringing narcotics in. This has been a big issue for our Bureau of Prisons.

What would slow us down now? Those are fixed locations, most of them in remote areas. What would be the challenge of trying to get this counter-UAS across all of our Bureau of Prisons facilities, starting with the most remote? Why is that not already happening?

Mr. WIEGMANN. We are working on that. We have deployed technology at a number of prisons. I know it is several, and I think there is another 20 that are going to be coming on board. It is really just a question of getting people trained, getting the technology, working with the FAA on the TFRs and so forth.

Look, I understand your impatience and I share it, so we want to do this because it is a huge problem. I share your view, and we are working with BOP, which is definitely concerned about this issue. We just had charges this past week in a prison in Texas where people were smuggling in contraband into the prison. That is not the first one. There are others. So I share your concern and BOP is ramping up.

Senator LANKFORD. OK. That is helpful. I would say good except that this is something that we have talked about often around this dais, to try to say what is the slowdown. We are always trying to figure out what is the issue, because we will allocate funds, we will do the studies, we will do the pilots, we will approve all the process, and it seems to be years to actually get to execution on something that should be pretty straightforward, especially a Bureau of Prisons area that is very remote, that we are not dealing with the complexities of being in a city. This one should not just be as hard as it seems to be.

Mr. Chairman, thank you.

Chairman PETERS. Thank you, Senator Lankford. Senator Scott, you are recognized for your questions.

OPENING STATEMENT OF SENATOR SCOTT

Senator SCOTT. First I want to thank Chair Peters and Ranking Member Portman for holding this hearing on a critical and important topic. Plus, I mean, clearly from listening to you all you know the importance of this and you are taking it seriously.

As you know, Communist China funds technology like drones to spy on Americans and steal our data. I proposed legislation such as the Counter Chinese Drone Act and the American Security Drone Act to help protect national security and the privacy of American citizens. I am proud to have led the effort to pass the American Security Drone Act in the Senate, but I think we have to go further and pass the Countering CCP Drone Act.

The legislation is the next step to ensure that the Federal funds from the Federal Communications Commission (FCC) cannot be used to obtain communications equipment and services provided or produced by Communist China's drone company like DJI. I have a few questions on the reauthorization of the Preventing Emergency Threats Act.

Mr. Wiegmann, I know. I practiced it. I said it the wrong way. Current law already waives certain specific provisions and prohibitions under Title 18 for action taken by DOJ and DHS against drones. This proposed bill waives all of Title 18. Why do you need to waive all of Title 18 and why not just keep the existing waivers in place?

Mr. WIEGMANN. a couple of things. DOD and DOE have a broad Title 18 waiver, so it helps us interoperate with them if we have the same authorities they have. So that is one.

Two, is while you are correct that our current authority for DHS and DOJ only extends to certain provisions in Title 18—and we have been able to use that effectively thus far—we cannot predict, as this is a changing technology landscape that other statutes could come into play in the future. We would be back in Congress, asking again if there is some new technology that is going to implicate a different statute that we were not thinking of.

We think the cleanest approach, given that we do not think that law enforcement officials using this technology that we have all talked about here today to try to prevent threats from drones, it should not be criminal at all. It should not be any criminal provision that they are subject to rather than just a few statutes.

We think it is a cleaner approach. We are obviously happy to discuss that with the Committee if that is not their view. But we think it is cleaner to have the same authority that DOD and DOE have, which a full sweep.

Senator SCOTT. Do you have examples where you needed it? If this was not in place, where have you needed this in the past?

Mr. WIEGMANN. Thus far we have been able to work with the existing exemptions that we have from specific statutes. We cannot predict, necessarily, whether in the future, as technology changes, whether other statutes could come into play.

Senator SCOTT. OK. Senator Lankford talked a little bit about the prisons. We know use of drones over prisons is a real threat.

They have been used to drop drugs, weapons, and other contrabands in to inmates. Drug cartels, we know they are using drones for smuggling contraband across the border, into prisons, and for surveillance. How will this bill improve the law enforcement efforts to counter this threat?

Mr. WIEGMANN. To counter drug threat?

Senator SCOTT. Yes. To deal with the prison fight, issues of our prisons. How would this bill change anything?

Mr. WIEGMANN. We already have the authority to protect our prisons so it would extend it. The key thing is it expires in October if we do not extend it, so we would not have the authority unless we get the extension.

Senator SCOTT. I imagine it does not really change anything.

Mr. WIEGMANN. But other than that we have the authority in prisons, so we are good. We just need to extend that authority for prisons.

Senator SCOTT. OK. All right. Ms. Vinograd, under the proposed reauthorization of the Preventing Emerging Threats Act it authorizes a limited pilot program under which DHS and DOJ, in consultation with the Department of Transportation, could designate certain State and local law enforcement entities to use counter-drone detection mitigation authorities.

Can you talk about the selection process for this pilot program and how State and local entities would be selected? By the way, have you talked to agencies in Florida?

Ms. VINOGRAD. Senator, thank you. I will turn to my colleagues from the Department of Justice in a moment. What we are seeking in this legislation is two things for State, local, tribal, and territorial partners. No. 1 is the ability for SLTT partners—excuse my acronym—to engage in detection of drones or UAS. In addition to that—and I should say compliant with all Federal standards and safeguards—what we are seeking is a six-year pilot program for SLTT partners to engage in mitigation.

That selection process would be an interagency process. These individuals would comply with Federal standards and certifications. They would use equipment from an authorized equipment list that has been coordinated with FAA and FCC. We believe that this is critical, such that SLTT partners, as the first responders on the ground, in Florida and elsewhere, would be able to take urgently needed action to detect and mitigate drone threats.

I will turn to my colleague from the Department of Justice.

Mr. WIEGMANN. I am going to look, if it is OK, in the back row to see if we have been talking with anyone in Florida about the potential. Yes, we have.

Senator SCOTT. Is that typically through, what, the Sheriff's Departments or police?

Mr. WIEGMANN. Daytona, I am hearing that we have talked to them about this. As we select cities around the country to participate in the program it is going to be their level of interest——

Senator SCOTT. It is really, they are going to drive this.

Mr. WIEGMANN [continuing]. Their expertise, and so forth, and if they would apply, and we will see how that process works. We have not exactly figured out what the criteria are or how we are going

to select jurisdictions to do it, but I imagine it will be in locations all over the country and buildup.

Senator SCOTT. You know when I talked about it with DJI, the drones, do you all have thoughts about whether we ought to just blanket outlaw the ability for a Chinese company to be able to sell drones in this country, or whether the Federal Government ought to be able to buy them or not? Do you guys have any thoughts on that?

Ms. VINOGRAD. From the Department's perspective we share your concerns about China, generally, and Chinese-manufactured drones. Senator, DHS has issued guidance internally that prohibits the procurement of small UAS manufactured by foreign countries. There are some limited circumstances in which waivers may be granted, but generally we share your concern about Chinese-manufactured drones.

Mr. WIEGMANN. Yes. The problem is that right now, as you know, they dominate the market.

Senator SCOTT. I have found some.

Mr. WIEGMANN. What is that?

Senator SCOTT. We found a little bit but not much.

Mr. WIEGMANN. They have a huge chunk of the market, and so if we need to use drones for law enforcement purposes they are kind of the main game. We are working to transition away from that. There is impatience. It is a question of time. In the interim we are taking steps to mitigate whatever risks, supply chain risks or others, from use of the drones, but eventually we want to transition away from it. The waivers that Sam mentioned are necessary for that purpose. They do serve a useful purpose for all manner of things that we do. It is not ideal, but we are trying to transition away from them, is how I would say it.

Ms. COULTAS. From the FAA's perspective, we are really responsible for the integration of drones into the national airspace and testing of the drones to ensure the safety as they are integrated. But we do not have a position on the purchasing of or acquiring.

Senator SCOTT. OK. Ms. Vinograd, I have one quick question. Did you see this stuff that came out in Ukraine that DJI drones were being tracked? Have you guys looked into that at all, or is that classified? Do you know?

Ms. VINOGRAD. I have seen that and I would be glad to follow up in a closed hearing.

Senator SCOTT. OK. Yes, that would be great. I would love to learn what happened on that.

Ms. VINOGRAD. Certainly.

Senator SCOTT. Thank you.

Chairman PETERS. Thank you, Senator Scott. Senator Rosen, you are recognized for your questions.

OPENING STATEMENT OF SENATOR ROSEN

Senator ROSEN. Thank you, Chairman Peters. I appreciate you holding the hearing and I appreciate all of you being here today and what you have been working on. I want to focus on protecting our stadiums, because my home State of Nevada, it is the entertainment capital of the world. We are quickly emerging as a sports capital of the world as well. We have a new Allegiant Stadium,

home of the Raiders. Las Vegas is the first city to secure the NFL draft, the Super Bowl, and the Pro Bowl all at once. This, unfortunately, continues to make Las Vegas a target-rich environment for bad actors.

Since the September 11th terrorist attacks, Congress, Executive Branch, you have recognized the need to protect stadiums and supports events, and the FAA initially imposed, like you talked about, temporary flight restrictions, over stadium events, including for unmanned aircraft. Congress subsequently strengthened and codified these requirements. However, sports leagues have reported an increase in violations of flight restrictions by drones.

Mr. Chairman, I ask that I be permitted to enter into the record a letter from a coalition of sports organizations[1] in support of the Administration's counter-UAS proposal.

Chairman PETERS. Without objection it will be entered.

Senator ROSEN. Thank you.

Ms. Coultas, as the FAA considers new drone policies, do you think it is important to take into account these longstanding protections for stadiums, ensure that Federal policies keep up with evolving threats? How do you plan to do that?

Ms. COULTAS. Thank you for your question, Senator. The FAA, yes, we do agree that as the technology continue integrating drones into the airspace that the ability for the detection and then, when necessary, mitigation is in place as well. We are working closely with our stadium stakeholders to ensure—as you mentioned, we already do have standing TFRs for the NFL, Major League Baseball (MLB), National Association for Stock Car Auto Racing (NASCAR), as well as the Division I colleges. Then we also work very closely, for the Super Bowl and other types of larger events, to ensure that we put the appropriate air restrictions around those mass gathering events that are held at stadiums and other venues, to both ensure the safety of that event and security but also to ensure the safety of the airspace over that event.

Senator ROSEN. Let me ask you this follow-up then. There is draft legislation from the Administration that does extend the authorities for critical infrastructure but it does not specifically mention stadiums. You are talking about all the things that you are already doing. Shouldn't we be specific in identifying stadiums and other types of critical infrastructure so we are sure that we want to avoid confusion and we are sure that communities have the resources to protect themselves? Ms. Coultas and then Ms. Vinograd.

Ms. COULTAS. So yes, the legislation specifically says critical infrastructure, and we did not define exactly which sectors or entities within the critical infrastructure sectors. I would say I would leave that up to Congress, if they wanted to give us more specifics and mention. But we take that as it is all entities, because critical infrastructure encompasses, in addition to stadiums, as you know, it is chemical facilities, it is the energy sector, it is dams, it is a whole host of different sectors that may want to come and petition, through DHS or to Justice, to the FAA, to get both temporary restrictions or permanent restrictions in addition to being able to use detection equipment and then eventually may mitigation.

---

[1] The letter referenced by Senator Rosen appears in the Appendix on page 69.

I would defer to my DHS colleague if she wants to expand on that.

Ms. VINOGRAD. I concur with my FAA colleague. We have no objections to more specificity. We want to ensure that all critical infrastructure owners and operators, to include stadiums and sports venues, have the authority that we are requesting in the bill.

Senator ROSEN. I am just worried that there is going to be confusion, and so we can at least maybe define, as a minimum, a certain group, allowing for the flexibility, of course, to add more as needed. We will continue to work with you on that.

But I do want to build on what Senator Scott asked about the pilot program to extend the counter-drone capabilities, to work with State and local law enforcement, again protecting all the critical infrastructure. First of all, do you agree that the pilot program should include stadiums? I think you do. As you say, you have been talking to Florida. We have a great Fusion Center in Las Vegas. We have a lot of things to protect there.

Have you been speaking with anyone in Nevada, and do you believe that the training and surveillance should be shared across these multiple law enforcement agencies and that that is a good thing to involve the communities?

Mr. WIEGMANN. Yes, I agree, and I am going to look again in the back row to see if we are in touch with folks in Nevada. Yes, we are in touch with folks in Nevada. Look, right now we can only protect the Super Bowl, the World Series, et cetera, and one of the main purposes of the bill is, there are a couple thousand NFL games every year. There are 20,000 baseball games every year. We are only covering the super high profile. The big advantage of this State and local pilot is to allow that force multiplier, right, for the people who are on the front lines to be able to protect those venues for the ordinary game that is going on. That is a big piece of it, and including in Nevada. I fully expect that the jurisdictions that participate in the pilot would be scattered across the country.

Senator ROSEN. I think your force multiplier, that is the way we should look at our State and local communities as force multipliers. You cannot do it all alone.

I have about a minute left. I would like to quickly move on to cybersecurity because we know that the drones really present significant cybersecurity risks. Of course, country of origin, as we have talked about with China, manufacturing. But there are malicious actors. They can exploit data. They can spoof our Global Positioning System (GPS). They can hijack control of drones that are necessary, law enforcement drones perhaps.

Assistant Secretary Vinograd, can you talk about some of the specific threats, and could you list them in what you might think are the highest threats we need to be worried about first, to the least, if that is possible? All threats may be not quite equal.

Ms. VINOGRAD. Senator, just to clarify, cybersecurity threats or drones threats more broadly?

Senator ROSEN. Cybersecurity threats, to the drones, I guess.

Ms. VINOGRAD. Certainly. Senator, you mentioned several key ones, which are the exploitation of information on that drone or information that is being transmitted between the command-and-control center. Just to clarify, our C–UAS authorities, the hearing

today is about counter-UAS authorities or questions more specifically about drones. Moving back to the subject of the hearing, which is the counter piece of it, how we stop the stuff, we only, when we are countering UAS, intercept the signal between the command and the control center, and that is the only information that we interrupt and that we, in certain cases, retain.

When we look at drones being used for malicious purposes we are certainly concerned about a malicious actor of some kind trying to engage in a cyberattack to change the course of that drone, weaponize it, and/or use it for its own malign purposes, like surveillance, like intrusion into an unauthorized facility, and things of that nature.

From a counter-UAS perspective, again we are focused on the signal between the command-and-control center, and then from the actual drone perspective we are very aware of cybersecurity risks that could allow the drone to be manipulated for a range of malign purposes.

Senator ROSEN. I guess we will have to work on that with CISA. I am just concerned that making sure that our State and local communities understand which threats they have to deal with, the highest threats going down, so that we can be sure to protect the ones we love.

Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Senator Rosen. Senator Padilla, you are recognized for your questions.

OPENING STATEMENT OF SENATOR PADILLA

Senator PADILLA. Thank you, Mr. Chair. Before I ask my questions I want to be very clear that the potential threat posed by UAS is one that Congress must address before the existing authorities expire. We absolutely agree on that. I know in California we have seen how a rogue UAS can disrupt critical function, including wildfire suppression efforts.

My questions are not related to the need for reauthorization but making sure that we do so in a responsible way. The first area of questions has already been covered by Senator Scott, and that had to deal with the sort of broad exemptions to Title 18 that are called for in the Administration's proposal. I know there was a recognition, a back and forth of that is not currently the case. There are a lot of specific exemptions and it may not be easy but you are making it work. There is more than one way to get this done.

Instead of just asking that question over again I will follow up, Mr. Wiegmann, with this. Title 18 for the U.S. Code includes prohibitions against, for example, committing war crimes, intimidating voters, and engaging in video voyeurism. I understand why the Department of Justice and DHS might need to be exempt from the Wiretap Act, but why do you need to be exempt from prohibitions against the examples I just gave?

Mr. WIEGMANN. Yes, we do not, although, again, to be honest, none of those activities would be authorized by this statute, because you can only take under the statutory regime those actions which are necessary to detect and then mitigate a credible threat. It is hard for me to imagine a voyeurism or war crime coming into play there.

The statute would not give protection against those offenses because of the way it is structured. It would not exempt you from those offenses because those would never come into play.

Senator PADILLA. I hear you, but sadly, as we have seen, from administration to administration, interpretations and philosophies can shift. What we do put into statute, in terms of exemptions, does matter. I think it is critical and important.

A question in a different area. Whether it is broad exemptions or more specific exemptions is one thing, but we are also discussing the proposal to have a reauthorization that is permanent and not one with a sunset provision. The proliferation of drone usage as well as the rapid development of drone technology itself demonstrates why the government needs to have clear authorities, in my opinion, to engage in UAS mitigation activities. But as I mentioned, the pace of technological develop as well as the ever-growing uses for drones, including for valuable journalistic and civic engagement purposes, seems to suggest that there is considerable value in Congress regularly revisiting this area of the law.

The Administration's proposed legislation seeks permanent C–UAS authorities rather than including a sunset provision that would require not just Congress but the Executive Branch to come together in a few years to evaluate how well the expanded authorities called for in the statute are working. I am happy to debate whether it is three years, five years, or whatever the timeframe makes sense.

Ms. Vinograd, let me direct a question to you. Why should we not all be required to revisit the broad authorities being granted in this bill in a few years?

Ms. VINOGRAD. Senator, just to be clear, what we are seeking in this legislation is the lack of a sunset clause for most of the authorities. SLTT pilot program, we are not requesting indefinite authorities for.

The sunset clause, as it currently stands, is really impeding the Department's ability to effectively use our authorities, insofar as it makes it incredibly difficult for us to engage in multi-year planning, multi-year testing, and things of that nature.

We agree that there is a critical need to regularly engage with the congressional branch on how these authorities are being exercised. Under the Preventing Emerging Threats Act of 2018, we are required to report to Congress every six months, which DHS has done judiciously. In addition, in this bill, for the SLTT pilot program, two years after the enactment of this bill we are also required to report to Congress on just that SLTT pilot program.

Senator PADILLA. Yes. You may disagree but what I am hearing is an argument for a longer reauthorization, not a shorter one. But I still believe in the power of the sunset mechanism to force these conversations. I think it keeps us from talking every day, every week, every month, not just every six months, not just every two years. But as I mentioned in my preface here, the continuously evolving technology, innovation makes additional things possible, additional performance and capabilities, let alone the growing number of uses of the technology. I think more regular required conversation from Congress to Congress and from administration to administration would be worthwhile.

I know it has been a long morning for all three of you. I will leave my comments and that, but look forward to working with you as this proceeds.

Thank you, Mr. Chairman.

Mr. WIEGMANN. Thank you, Senator.

Chairman PETERS. Thank you, Senator Padilla. Senator Sinema, you are recognized for your questions.

OPENING STATEMENT OF SENATOR SINEMA

Senator SINEMA. Thank you to our witnesses for joining us today.

The counter-drone, or C–UAS, authorities expiring this October are critical to our homeland security. These authorities allow DHS and DOJ to protect Arizona's critical infrastructure and communities. As Chair of this Committee's Border Subcommittee and the Commerce Committee's Aviation Subcommittee, I am also keenly aware of the threats posed by drones to our nation's borders and airports.

In Arizona, cartels are using drones to smuggle drugs across the border in an attempt to evade law enforcement, and across our nation there are too many examples of drones blocking flight paths and even shutting down airports.

We must maintain and enhance our nation's C–UAS capabilities while also safeguarding privacy and the rights of legitimate drone users. I look forward to working with the Chairman, the Administration, and my colleagues to do just that.

My first question about future threats is for Mr. Wiegmann and Ms. Vinograd. Drone technology is rapidly evolving and while most drones currently rely on RF technology, in the future more advanced drones may become the norm. At DOJ and DHS what are you doing to prepare for the drone-related threats of the future, including autonomous, unmanned systems and drone swarms that could conduct synchronized operations? As Congress considers reviewing the existing C–UAS authorities, what can we do to help you research and mitigate these threats?

Ms. VINOGRAD. Senator, thank you. As you mentioned, the technology is evolving incredibly rapidly, and that is why at the Department of Homeland Security we have designed research testing and evaluation.

Senator, we agree that the technology is evolving incredibly rapidly, and what the Department of Homeland Security is committed to is trying to ahead of that evolving threat. We do so through our Science and Technology (S&T) Directorate, where we are engaged in a significant amount of critical research, testing, and evaluation, such that we can try to stay ahead of the curve as it pertains to the evolving technology.

In addition, as my colleague, Mr. Wiegmann, mentioned, we are seeking exemption from Title 18 such that we can ensure that we have the ability to keep pace and/or stay ahead of the evolving threat environment as this technology rapidly increases, and candidly proliferates the kinds of threats that drone may pose to the American people and to the homeland.

Mr. WIEGMANN. Yes, I do not have much to add to that other than we obviously work with our colleagues at DHS and DOD also in technology kind of working groups, to make sure that we are

doing the best we can to have the state-of-the-art technology to counter this threat.

Senator SINEMA. Thank you. Ms. Vinograd, as Chair of the Border Subcommittee and the Aviation Subcommittee I am particularly concerned about the threat that drones pose to our border and our airports. If the current C–UAS authorities expire in October can you discuss the impact that would have on our border security?

Ms. VINOGRAD. The expiration of existing counter-UAS authorities would be catastrophic from a border security perspective. Our counter-UAS authorities currently allow for critical counter-UAS operations at our borders, and the expiration of those authorities would allow a range of adversaries, including transnational criminal organizations to increase their malicious use of drones to engage in smuggling, surveillance, and other malicious activities.

Senator SINEMA. Thank you. My third question for Ms. Vinograd and Ms. Coultas. Can you describe how the Administration's legislative proposal would help protect airports and flight paths from drones, and specifically, how do the current gaps in the Federal Government's C–UAS authorities hinder your agencies from achieving this?

Ms. VINOGRAD. I will say that of all the things that keep me awake at night, one that is foremost on my mind is the potential for major tragedy at an airport. We currently, at the Department of Homeland Security, work in close partnership with the FAA at airports. However, DHS, the Transportation Security Agency, lacks the authority to engage in proactive or persistent C–UAS operations at airports. What that means is TSA is not authorized to be on the ground at airports engaging in proactive detection and, as necessary, proactive mitigation.

I will tell you, just from a threat perspective, we have had 2,000 sightings of drones in and around airports since 2021. In 2021 and 2022, year to date, we have had 64 evasive actions by aircraft, including four commercial carriers taking evasive action, Senator. We have had 30 airport disruptions just in 2021. This already amounts in significant economic damage and a potential for real loss of human life. I am very concerned about the lack of explicit authority at airports. That is why we are seeking explicit authority for TSA to engage in proactive and persistent detection and mitigation in close partnership with FAA.

Ms. COULTAS. To build off of my colleague from DHS, obviously the No. 1 priority for the FAA is the safety and security of the airspace, and around airports we, too, are very concerned about the number of drone sightings that we consistently see across this country.

We are working very closely with our DHS partners, and the FAA is supportive of expanding the authorities to TSA, to give them the authority to be able to do not just the detection but the mitigation, if necessary, at the airport environment.

Senator SINEMA. Thank you. My next question is for Mr. Wiegmann. Like all technologies, drones old both promise and peril. The same drones that our adversaries could use to surveil a sensitive government facility can be used by journalists to ship footage for the news and to hold government accountable.

I know that DOJ has devoted considerable time and resources to ensuring that privacy and civil liberties are protected during C–UAS operations. Can you discuss some of these safeguards, and how often are drones that in a restricted airspace are actually interdicted, and when they are what data is intercepted, and for how long?

Mr. WIEGMANN. OK. Under the statute we can only intercept data that is necessary for countering a threat. As I mentioned in my opening testimony, what we are typically talking about is—and I have a list here of the types of data—the drone vendor and model, the drone and controlling device serial number, the geolocation of the drone, the location of the controller, and the most recent take-off location and home location.

We are not talking about content of communications. We are talking about metadata, signals information, essentially, that the drone is generating, that will allow us to find out where it is, where it is going, where it has been, and who is controlling it, so that we can hopefully interdict it.

Once we collect that information, the ordinary course, if it is not of any use we discard that information right away. But under the statute we can only keep it as long as it is necessary and in no event longer than 180 days, unless it is necessary to keep it longer for a specific purpose, like for a criminal investigation, if someone has violated the airspace and we need the information in order to pursue a criminal investigation or prosecution.

So all of this is laid out in existing law, in the statute. Restrictions on what you can collect, how long you can retain it, and when you can disseminate it are all in the statute, and those would be carried over under the new bill. We would continue all of those same privacy protections into the new bill and they would also be applied to State and locals. To the extent State and locals are engaged in the same activity under the pilot program they would also be bound to respect all of those privacy protections.

I do not know if that answers your question.

Senator SINEMA. Yes. Thank you. Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Senator Sinema.

I would like to take this opportunity to thank our witnesses once again for participating in today's hearing and in discussing the Administration's proposal to both extend and expand current authorities to counter UAS, to protect our homeland from serious threats posed by unmanned aircraft systems.

As we heard today very clearly from each of our witnesses, a malicious actor could deploy UAS to cause a catastrophic incident at any time, and we cannot and must not wait for that incident to occur. As Chairman of this Committee I will work to ensure that these authorities do not lapse in October, so our Federal law enforcement partners can continue their very crucial missions to protect us from these threats.

I also plan to introduce legislation, in the very near future, with Senator Johnson that both extends and provide a careful expansion of these counter-UAS authorities.

The record for this hearing will remain open for 15 days, until 5 p.m. on July 29, 2022, for the submission of statements and questions for the record.

This hearing now stands adjourned.
[Whereupon, at 12:01 p.m., the hearing was adjourned.]

APPENDIX

Chairman Peters Opening Statement As Prepared for Delivery
Full Committee Hearing: Protecting the Homeland from Unmanned Aircraft Systems
July 14, 2022

I'd like to thank our witnesses for joining us and for their continued service to the American people. Today's hearing will highlight the threat posed by unmanned aircraft systems, or UAS, commonly known as drones, and discuss how federal agencies are working together to combat this evolving threat.

We will also examine what additional authorities and resources the Department of Homeland Security, and the Department of Justice, need to successfully counter UAS, while working together with the Federal Aviation Administration.

In recent years, the market for commercial UAS has rapidly expanded due to the affordability and utility of drones that are readily accessible to government, industry, and recreational users.

The FAA estimates that by 2024, about 2.3 million UAS, including 1.5 million recreational drones and model aircraft, and about 800,000 commercial UAS, will be registered to fly in U.S. airspace. Between 2016 and 2019, airline pilots reported, on average, more than 100 drone sightings per month to the FAA.

The increase in the number of UAS operating in our air space creates a higher risk of rogue drones either failing to obey safety rules or operating with nefarious intentions, threatening manned aircraft operations, airports, critical infrastructure facilities, and high-profile, widely-attended events such as sporting events, concerts, and more.

While most individuals operate their drones responsibly, we have already seen careless and malicious actors misuse these technologies to engage in reckless or criminal activities.

In September 2017, a privately operated drone in Brooklyn, New York, was intentionally flown beyond the operator's line of sight and collided with a U.S. Army Black Hawk helicopter patrolling a temporary no-fly zone around New York City.

Thankfully, the Black Hawk and its crew landed safely, but there was significant damage to the helicopter, and the incident created an unacceptable risk to the servicemembers.

In 2019, a drone significantly disrupted flight operations at Newark Liberty Airport for 90 minutes, causing 9 flights to be diverted, halting 43 planes inbound to the airport, and causing significant delays for passengers.

These events demonstrate the severity of the threat posed by UAS. If we do not act, it could only be a matter of time before someone who is recklessly operating this technology causes an accident that has catastrophic effects.

And as we work to avoid unintentional disasters, we must also account for the escalating threat of weaponized drones from terrorist and criminal organizations who could launch domestic drone attacks on mass gatherings, high-profile landmarks and buildings, or federal property. This includes foreign adversaries, who have deployed drones in conflicts abroad, and could have the capability to deploy them in the United States as well.

We must also be prepared to counter drones operated by criminal organizations that are reportedly using UAS for illegal activities including trafficking illicit drugs across our borders.

I am grateful to my colleagues who have led past efforts to address these concerns and improve the safe integration of UAS into American airspace, including Senator Johnson for authoring *the Preventing Emerging Threats Act*.

Since 2018, the authorities created by this law have bolstered our nation's ability to protect numerous large public events, including the Super Bowl, from UAS threats.

Today's hearing is an opportunity to discuss renewing and updating those authorities, which are set to expire in October, as well as the Biden Administration's Domestic Counter-UAS National Action Plan, the first coordinated, whole of government plan to address the evolving security threats posed by UAS. I'm working on bipartisan legislation that I plan to introduce in the coming weeks to reauthorize and strengthen counter-UAS authorities to better tackle this threat.

Today I am pleased we have a panel of expert witnesses from DHS, DOJ, and the FAA who can discuss what lawmakers can do to ensure the federal government is better equipped to safeguard against potential threats from UAS.

Opening Statement
Ranking Member Rob Portman
U.S. SENATE COMMITTEE ON HOMELAND SECURITY
& GOVERNMENTAL AFFAIRS
"PROTECTING THE HOMELAND FROM UNMANNED AIRCRAFT SYSTEMS"
JULY 14, 2022

Thank you, Mr. Chairman, for holding this hearing.

We are here today to discuss the emerging threats posed by unmanned aircraft systems, or "drones", in the United States.

In 2018, Congress provided authorities to the Department of Homeland Security and the Department of Justice to counter the threats posed by the use of drones.

Unfortunately, those authorities are about to expire. And this expiration could not come at a worse time.

Cartels and Transnational criminal organizations (TCOs) use drones to smuggle drugs and surveil U.S. law enforcement in furtherance of other illicit cross-border activity. These cartels have also begun to weaponize drones in order to commit attacks in Mexico. It is only a matter of time before weaponized drones commit attacks on our border.

To give you a sense of the scale of the problem—in joint testimony before the House Committee on Homeland Security in March, representatives from DHS stated that in a previous 5-month period, CBP sensors captured more than 30,000 individual flights near the southern border where half of the flights violated FAA regulations.

My office has repeatedly asked DHS since February of this year for more information on statistics for these drone border incursions and how they plan to address this emerging threat. Moreover, the Biden Administration's Domestic Counter-Drone National Action Plan provides no explicit additional authorities for DHS to counter unmanned aircraft systems as it pertains to the border.

Make no mistake, the Mexican transnational criminal organizations will benefit from the lack of additional counter-drone authority for CBP and other agencies with responsibility for securing our nation's borders.

For these reasons, I am eager to hear how DHS, DOJ, and the FAA have used their existing authority to mitigate the threats posed by the nefarious use of drones. I also hope to discuss what new authorities this committee can give the administration to improve the counter-drone mission, especially at the border.

Recently, the Biden Administration provided this committee with a comprehensive legislative proposal which seeks a number of changes and expansions to existing counter-drone authorities. I look forward to working with Chairman Peters and my colleagues on the committee to review this proposal.

This committee has already done great work to address the threat to national security and economic competitiveness posed by Chinese-made drones when we reported out the bipartisan *American Security Drone Act* last year. Among other things, this legislation would prohibit the federal government from purchasing and using drones manufactured by our adversaries. I'm pleased this legislation was included in the Senate-passed USICA package and I continue to urge Speaker Pelosi to swiftly pass USICA so this can become law.

With that said, I look forward to a productive conversation about the current drone threats to our homeland and the actions being taken to prevent them.

Thank you again, Chairman Peters.

Testimony of
Samantha Vinograd
Assistant Secretary (Acting) for
Counterterrorism, Threat Prevention, & Law Enforcement
Office of Strategy, Policy, and Plans
Department of Homeland Security

on

Protecting the Homeland from Unmanned Aircraft Systems

Before

The United States Senate
Committee on Homeland Security and Governmental Affairs

Washington, D.C.
Thursday, July 14, 2022

Chairman Peters, Ranking Member Portman, and distinguished Members of the Committee, thank you for inviting me to testify regarding the current authority for the Department of Homeland Security (DHS) and Department of Justice (DOJ) to counter threats from unmanned aircraft systems (UAS[1] or "drones") and proposed legislation to reauthorize and expand the authority. This legislation is essential for DHS and DOJ to continue critical missions to protect national security and public safety, while remedying major gaps in our counter UAS (C-UAS) authority, so we can keep pace with the dynamic and evolving threat environment.

Today, I am here with my partners from DOJ and the Federal Aviation Administration (FAA) to ask for your help. During the past four years, DHS and DOJ have judiciously implemented the C-UAS authority that Congress granted through enactment of the *Preventing Emerging Threats Act of 2018* (the Act) while ensuring the protection of privacy, civil rights, and civil liberties. Through numerous deployments, DHS and DOJ also have demonstrated the safe exercise of C-UAS authority, with extensive coordination with the FAA, and minimized impacts to the national airspace system. Congressional action is urgently required, as DHS and DOJ authority to detect and counter drone threats will expire in less than three months on October 5, 2022. A lapse in our authority would result in perilous and unacceptably high national security and public safety risks. Sustaining and enhancing C-UAS authority is the foundation of the security architecture necessary to continue the integration of drones into the national airspace and for commercial purposes, which will yield substantial benefits to our economy and way of life.

Technological advances have accelerated drone capabilities across military, commercial, and recreational applications. Their compact size and often low cost make them suitable for many beneficial and critical uses, including minimizing safety risks for critical tasks previously done by humans. Drones are playing a transformative role in transport and delivery, critical infrastructure management, agriculture, search and rescue, disaster response, public safety, coastal security, military operations, journalism, entertainment, and others. Estimates suggest that rapidly advancing drone technology and integration will result in new innovations and generate significant economic growth and opportunity for businesses and private citizens. To be clear, DHS supports the lawful use of drones, including by commercial and recreational users, which constitute the vast majority of UAS users. Like all technology, however, drones can be exploited for malicious use, threatening national security and public safety, which is DHS's concern.

My testimony will address four points: (1) describe the evolving threat environment and domestic drone incident data; (2) summarize DHS's current C-UAS authority and major gaps; (3) explain the Administration's legislative proposal to reauthorize and expand C-UAS authority and why it is necessary; and (4) highlight how DHS will continue to responsibly implement, use, and ensure oversight of C-UAS authority.

[1] The term "unmanned aircraft system" means an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the operator to operate safely and efficiently in the national airspace system. *See* 49 U.S.C. § 44801(12)

Dynamic and Evolving Threat Environment Is Increasing and Diversifying

As drone usage proliferates and integration into the national airspace system progresses, threat actors are increasing and diversifying their malicious use, and errant actors are increasingly interfering with manned aviation. The threat can take several forms, which I will describe and place in context with domestic drone incident data.

- Globally, drones continue to be used by adversaries **as a weapon**. This threat vector is a major concern for protecting mass gatherings and VIPs and is a major reason Congress provided C-UAS authority to DHS and DOJ nearly four years ago. Abroad, threat actors have used drones to attempt assassinations of the Venezuelan president in 2018 and Iraqi prime minister in 2021. In Mexico, drug cartels since 2021 have increasingly used drones to attack the military, police, and rivals. In Ukraine, the extensive use of both off-the-shelf and military drones has further demonstrated drones' lethality and versatility. Drones have even been weaponized here in the U.S. Domestically, the U.S. Secret Service (USSS), since 2018, has encountered hundreds of drones violating temporary flight restrictions that protect the President and others. In January 2022, an animated video released by Iran's leader depicted an Iranian drone targeting a former U.S. President at his home.

- Drones continue to **interfere** with manned aviation, resulting in damage to aircraft, disruptions to airport operations, and economic harm. The Transportation Security Administration (TSA), since 2021, has reported nearly 2,000 drone sightings near U.S. airports, including incursions at major airports nearly every day. The most serious drone incidents force pilots to take evasive action during takeoff and landing to avoid potentially fatal collisions. During 2021-2022, TSA reported 63 drone incidents requiring evasive action, including four involving commercial aircraft. Drones also have collided with helicopters used by the police, first responders, and the military – threatening lives and disrupting missions. Additionally, drones have significantly impacted airport operations. Since 2019, drone incidents have caused U.S. airports to fully halt operations three times, and in 2021, over 30 partial suspensions of operations – resulting in millions of dollars of economic damage.

- Drones continue to disrupt and damage critical infrastructure and services. In the Middle East, drones in 2021 and 2022 have been used to attack international airports and energy facilities, killing or injuring people and halting operations. At home, the energy and chemical sectors consistently report suspicious activity by drones. In 2020, law enforcement discovered a crashed drone outside an electrical substation in Pennsylvania, which had been modified to cause an intentional power disruption. This attempt was unsuccessful, but next time we may not be so fortunate. During 2021-2022, the FBI identified 235 reports of suspicious drone flights at or near chemical plants in Louisiana. Similar UAS incidents also occurred at oil storage facilities in Oklahoma and natural gas facilities in Texas. Particularly in this time of global energy shortages, any interruption of supplies or attack on these facilities could be devastating. In addition to planning or carrying out such an attack, drones may also be used to conduct hostile surveillance or steal U.S. technology.

- Nearly every day, transnational criminal organizations (TCOs) use drones to convey illicit narcotics and contraband across U.S. borders and conduct hostile surveillance of law

enforcement. From August 2021 to May 2022, U.S. Customs and Border Protection (CBP) has detected more than 8,000 illegal cross-border drone flights at the southern border, an average of nearly 900 incursions per month. Since 2019, CBP officers have seized hundreds of pounds of methamphetamine, fentanyl, and other hard narcotics that drug traffickers have attempted to transport through thousands of cross-border drone flights. As drone technology evolves, so does the threat. CBP assesses that TCOs are pursuing the use of larger drones with increased speed, range, and payload capacity – to fly faster, higher, farther and with more contraband – in an effort to evade CBP and law enforcement.

- Drones can be used by hostile foreign intelligence agencies or criminals to collect intelligence and enable espionage, steal sensitive technology and intellectual property, and conduct cyber-attacks against wireless devices or networks. Most commercial drones have high-definition cameras, can be easily retrofitted with a variety of sensors, and are difficult to detect given their small size. Details and data on this aspect of the threat are sensitive and can be best covered in a closed, non-public setting. The potential implications can be significant for sensitive U.S. facilities, the defense industrial base, technology firms, and others.

DHS Uses Current Authority to Detect and Counter Drone Threats, But Gaps Remain

The "Act" grants DHS and DOJ relief from several federal criminal statutes to take certain actions to detect and counter UAS posing a credible threat. Specifically, such relief is largely from provisions of Titles 18 and 49 of the U.S. Code that generally prohibit aircraft sabotage, computer fraud and abuse, interference with the operation of a satellite, wiretapping, and use of pen registers and trap-and-trace devices. This relief allows actions authorized in the Act, including electronic detection and mitigation of UAS threats through communications signal intercept and interruption, kinetic/physical mitigation, and device seizure. This authority expressly enables the protection of a designated "covered facilities or asset"[2] from UAS threats that relate to specific mission sets, which for DHS includes facilities and missions of the USSS protective operations, U.S. Coast Guard (USCG), Federal Protective Service (FPS), and CBP. The Act also authorizes protection of shared DHS and DOJ mission sets, including protection of National Special Security Events (NSSE) (e.g., Presidential Inauguration) and Special Event Assessment Rating events (e.g., Indianapolis 500). Additionally, the shared mission area includes support to state, local, tribal, or territorial (SLTT) law enforcement (upon request of the chief executive officer of the respective state or territory) for mass gatherings that are limited to a specific timeframe and location, within available resources, and also, the protection of an active federal law enforcement investigation, emergency response, or security function that is limited to a specified timeframe and location.

DHS's current authority is essential to critical missions. USSS relies on the authority to protect the President, Vice President, and NSSEs. USCG utilizes the authority to protect sensitive assets, facilities, and special events. FPS uses the authority to protect federal facilities.

[2] Defined in the *Preventing Emerging Threats Act of 2018* as any facility or asset that is identified as high-risk and a potential target for unlawful unmanned aircraft activity by the Secretary or the Attorney General, in coordination with the Secretary of Transportation with respect to potentially impacted airspace, through a risk-based assessment; is located within the United States; and directly relates to an authorized DHS mission, DOJ mission, or joint DHS or DOJ mission, acting together or separately. *See* 6 U.S.C. § 124n(k)(3).

CBP depends on the authority to counter illicit trafficking of narcotics and contraband across our borders and the hostile surveillance of its personnel. Since October 2018, DHS has prudently implemented the C-UAS authority granted through the Act and ensured the protection of privacy, civil rights, and civil liberties. Through over 300 deployments, DHS has proven the safe exercise of C-UAS authority, via extensive coordination with the FAA, and minimized impacts to the national airspace system.

Despite the Act and progress made to date, there remain major gaps in authority that impede DHS's mission to protect national security and public safety. In December 2021, DHS submitted a C-UAS Assessment to this committee and several others in Congress, which evaluated drone threats to U.S. airports and critical infrastructure; current federal or SLTT law enforcement authorities; an assessment of additional authorities needed by each Department and law enforcement; and an assessment of additional research and development needs to counter the threat. The most critical gaps identified by the DHS Assessment include a lack of authority for:

A. TSA to persistently protect U.S. airports – a stunning gap in the Department's authority;
B. SLTT law enforcement to detect and mitigate drone threats; and
C. Critical infrastructure owners and operators to detect drones operating near their facilities or request law enforcement assistance to mitigate drone threats.

The sunset clause in the Act has also made it more difficult to implement new C-UAS programs and initiatives. With no guarantee that the authority would be reauthorized, it has been difficult for DHS to fully prioritize new C-UAS programs, which require long term stability and sustainment. Uncertainty, and competing priorities have exacerbated the situation, leading to challenges with procurement and acquisition, personnel recruitment, and specialized training.

C-UAS Reauthorization Would Fix Major Gaps

DHS strongly supports the Administration's legislative proposal, which represents a comprehensive approach that seeks to reauthorize and expand current federal authority, including for DHS. This legislative proposal is essential for us to continue critical missions to protect national security and public safety while remedying major gaps in authority and policy, so we can keep pace with the dynamic and evolving threat.

1. First, the legislation would reauthorize DHS and DOJ current C-UAS authority. Congressional action is urgently required, as our authority to **take C-UAS actions** will expire in less than three months on October 5, 2022. A lapse in our authority would result in perilous risks and leave the nation vulnerable to drone threats.

2. Second, the legislation would expand authority to remedy gaps identified in the DHS Assessment and during the interagency policy process led by the National Security Council, specifically:
   - Authorize TSA to **proactively** protect transportation infrastructure from drone threats, which would remedy an extraordinary gap in the Department's authority.
     - This provision would enable TSA to deploy C-UAS detection and mitigation equipment beyond limited emergency circumstances. TSA has reported an alarming number of drone incursions near airports. Collision with a commercial plane could

endanger lives while disruptions to airport operations would cause significant economic damage to the aviation industry.

- Create a limited 6-year pilot program for SLTT law enforcement to mitigate threats in their jurisdictions through federal sponsorship and oversight by DHS and DOJ.
  - SLTT law enforcement lack the authority to mitigate drone threats; if selected to participate in this pilot, SLTT would have to comply with all federally standardized processes and procedures to include equivalent protections for individuals' privacy and civil rights/liberties.
  - Federal law enforcement and C-UAS equipment are limited and cannot be everywhere. (DHS and DOJ only have been able to protect about 1% of SEAR events.)
  - C-UAS systems would be tested and evaluated by DHS or DOJ and approved by FAA.
  - This measured approach builds on best practices and lessons learned by DHS and DOJ.
  - A select number of SLTT law enforcement agencies would participate in this pilot.
- Explicitly authorize SLTT law enforcement and critical infrastructure owners and operators to conduct drone detection-only with safe and proven technology.
  - Drone detection is critical to air domain awareness. As millions of drones fly in the national airspace, we must distinguish legitimate, compliant operators from threats.
  - Detection equipment authorized for use would be limited to a DHS list of approved systems.
- It is also important to enable critical infrastructure owners and operators to purchase and preposition mitigation equipment, which could be operated by authorized Federal entities or SLTT law enforcement participants in the pilot program.
- All proposed expansions would continue to require safeguards with which DHS and DOJ must continue to comply. These safeguards include: DHS or FAA-approved equipment lists; standard training and certification; risk-based assessments; coordination with FAA to ensure aviation safety; privacy, civil rights, and civil liberties protections; and DHS or DOJ oversight.

How DHS Policy and Guidance Governs the Use of C-UAS Authorities

To ensure consistent application of C-UAS authorities across Components, DHS established a C-UAS Program Management Office (PMO) within the Office of Strategy, Policy, and Plans. The PMO manages and supports C-UAS activities across the Department to ensure Component alignment with the Secretary's strategy and policy guidance and serves as a single point of contact for interagency partners. The PMO has worked closely with the FAA to develop objective standards that define critical elements needed for successful coordination across the Department, in each Component, and for the operator. Additionally, the Secretary issued the DHS-wide C-UAS Policy Guidance on September 10, 2019, requiring DHS Components to establish additional internal C-UAS policies, conduct assessments on the protection of privacy, civil rights, and civil liberties, and develop operational plans for each C-UAS deployment.

How the DHS Process for Authorizing Use of C-UAS Authorities Ensures Oversight

Recognizing the complexity and nuances associated with deploying C-UAS equipment domestically, the DHS Secretary's C-UAS Policy Guidance establishes formal process for obtaining C-UAS deployment authorizations. The process requires all Components to: identify a "covered facility or asset" to be designated; conduct a risk-based assessment prior to requesting the Secretary designate a "covered facility or asset;" coordinate with FAA to allow an assessment of potential impacts to the national airspace system and to evaluate the need and regulatory basis for establishing flight restrictions; and, then obtain authorization from the Secretary to conduct C-UAS activities pursuant to the Act. DHS and FAA closely coordinate these processes to ensure deployments do not negatively impact the national airspace system, to monitor how C-UAS authorities are used, and to ensure senior leadership visibility and concurrence.

How DHS Protects Privacy, Civil Rights, and Civil Liberties When Using C-UAS Authority

DHS is committed to protecting national security, public safety, and our values. These values include respecting the privacy, civil rights, and civil liberties of citizens and visitors, as well as, operating with transparency and accountability. The Secretary designates each covered facility or asset authorized for C-UAS activity. Every request includes an operations plan that clearly defines the boundaries and protocols for that specific protection mission. DHS C-UAS is a limited and controlled program. The only data our C-UAS systems collect are transmissions between the controller and the drone, which are similar to the data that manned aircraft transmits publicly via a transponder. This limited data is collected and retained consistent with the protections of the Act, the First and Fourth Amendments, and guidance from the DHS Privacy Office and the Office for Civil Rights and Civil Liberties. DHS is unable to access other content (e.g., phone calls, texts, email) on the operator's phone or other control device. C-UAS is not a surveillance program.

Above and beyond privacy protections in the Act, DHS applies *Section 222 of the Homeland Security Act of 2002* (as amended) to require DHS Component C-UAS programs to submit a Privacy Threshold Assessment (PTA) and obtain DHS Privacy Office approval prior to deploying C-UAS technology. The DHS Privacy Office uses the PTA to determine the need for a Privacy Impact Assessment (PIA), which includes measures to mitigate privacy risks. Moreover, DHS has published PIAs on its public website. DHS has also issued detailed guidance for collection of communications, data retention and sharing, and considerations on privacy, civil rights, and civil liberties as an annex to the Secretary's C-UAS Policy Guidance.

Again, the Administration's legislative proposal for expansion of C-UAS authorities would map Federal safeguards comparable to those required of DHS and DOJ to SLTT and critical infrastructure owners and operators. These include DHS or FAA approved equipment lists; standard training and certification; risk-based assessments; coordination with FAA to ensure aviation safety is preserved; privacy, civil rights, and civil liberties protections; and DHS or DOJ oversight.

Conclusion

In closing, DHS remains committed to protecting national security and public safety by countering the malicious use of drones. This legislation is essential to continue DHS's critical missions while remedying major gaps in authority, so we can keep pace with the dynamic and evolving threat. We appreciate Congress's foresight in granting C-UAS authority and are ready to work with you and key stakeholders across the government, private sector, law enforcement, and civil society to enact this important legislation. Thank you again for the opportunity to testify today, and I look forward to your questions.

Department of Justice

STATEMENT OF

BRAD WIEGMANN
DEPUTY ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

AT A HEARING ENTITLED

"PROTECTING THE HOMELAND FROM UNMANNED AIRCRAFT SYSTEMS"

PRESENTED

JULY 14, 2022

STATEMENT OF
BRAD WIEGMANN
DEPUTY ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

AT A HEARING ENTITLED
"PROTECTING THE HOMELAND FROM UNMANNED AIRCRAFT SYSTEMS"

PRESENTED
JULY 14, 2022

Good morning, Chairman Peters, Ranking Member Portman, and distinguished Members of the Committee, and thank you for the opportunity to testify on behalf of the Department of Justice. The Department strongly supports the Administration's consolidated counter-unmanned aircraft systems ("Counter-UAS") legislative proposal. Enacting this legislation is critical to continuing our efforts to protect major national events and important Department facilities and assets from the threat posed by misuse of unmanned aircraft systems ("UAS"), or drones. This bill would also enable us to expand UAS detection and counter-UAS efforts with respect to the types of facilities and assets that the Department can protect, and it would empower our State and local law enforcement partners, subject to appropriate oversight and limitations, to address the threat at events that the federal government does not have the resources to protect, and to protect important State facilities and assets.

I. The Threat Posed by Misuse of Drones

The use of UAS technology in the United States is growing rapidly. UAS will bring substantial benefits to our society and economy as the technology transforms the delivery of goods and the provision of services. In fact, commercial use of drones is already generating billions of dollars of economic growth. Law enforcement and public safety use of drones is also increasing and can enable us to perform critical public safety missions while reducing risk to personnel and the public.

Today there are nearly a million drones in the United States registered with the FAA and doubtless many more that are unregistered. Like other technologies that bring great public benefits, drones present serious risks to the public when misused. In April of this year, the Administration released its "Domestic Counter-UAS National Action Plan," which noted that:

> The UAS threat can take several forms, including platforms designed or modified to conduct kinetic attacks using payloads of firearms, explosives, or possibly even weaponized chemical, biological, or nuclear material; cyber attacks against wireless devices or networks; espionage; and the illicit trafficking of narcotics and contraband.

Beyond use by actors with nefarious intent, UAS are also often employed by operators without knowledge or regard for regulatory boundaries, who create hazards for Federal, state, local, tribal, and territorial governments, commercial activities, and the public.

Four years ago, in a hearing before this committee, the FBI Director testified that "given their retail availability, lack of verified identification requirement to procure, general ease of use, and prior use overseas, UAS will be used to facilitate an attack in the United States against a vulnerable target, such as a mass gathering." Although thankfully we have not yet seen a successful drone attack on a mass gathering in the United States, we are starting to see individuals in our country attempting to weaponize drones to conduct attacks against others, just as we have seen occur many times abroad.

In February 2020 a subject was arrested by State law enforcement and charged in connection with his efforts to use a drone to drop explosives near a Georgia mobile home park. In September 2020, a defendant in Pennsylvania was sentenced to five years for his efforts to use an unregistered drone to drop homemade bombs to terrorize his former girlfriend. Not far from the U.S. border, Mexican drug cartels have used drones to drop bombs on their rivals, just as terrorist groups in the Middle East have used them to launch deadly attacks.

Drones can also be misused to disrupt essential government functions. In February 2022, a defendant was sentenced to two years' probation for "buzzing" a group of firefighters in Virginia with a drone multiple times and then crashing the drone into a pole inside the fire station. In September 2019, a defendant in California recklessly operated a drone that crashed into a Los Angeles Police Department helicopter; he subsequently pleaded guilty to unsafe operation of an unmanned aircraft. The drone damaged the police helicopter, forced the pilots into an emergency landing, and damaged a vehicle when the drone fell from the sky after the crash.

We are also seeing an increase in the criminal use of drones in the prison context. In October 2019, a defendant was sentenced to 48 months in prison for operating an unregistered drone to facilitate a controlled substance delivery to the Autry State Prison in Georgia. In the summer of 2021, three defendants, including two brothers, were each sentenced to twelve months in prison for attempting to use a drone to smuggle contraband into the Telfair State Prison in Georgia. Between September 2021 and February 2022, four defendants, including two former federal inmates, pleaded guilty to an elaborate conspiracy to deliver contraband via drones into the federal correctional facility at Fort Dix in New Jersey.

Outdoor mass gatherings, like open-air sports stadiums, are particularly vulnerable to drone attacks. For example, in 2022, a defendant was sentenced after using a drone to drop flyers over spectators at two separate NFL games occurring the same afternoon in California. A more nefarious actor could have used the drone to drop explosives or spray deadly chemical agents on the crowd.

Under the important authority granted in the Preventing Emerging Threats Act of 2018, Congress facilitated certain counter-UAS missions by the Departments of Justice and Homeland Security. The FBI has conducted 70 UAS detection and counter-UAS protection operations at

large events, ranging from the Super Bowl to the New Year's Eve celebration in Times Square. That represents only 0.05% of the over 121,000 events during that time for which State, local, and federal officials requested an assessment and Special Events Assessment Rating so that UAS detection and counter-UAS support could be provided. These numbers make clear that the demand for such support to protect our communities has far outstripped the federal government's limited resources and that we cannot do this alone. The events that FBI has protected have also shown that the threat posed by drones used recklessly, but perhaps not with intent to engage in violence, is significant. During those 70 operations, FBI's counter-UAS teams detected 974 unauthorized drones operating in flight restricted areas, located the operator in 279 instances, and attempted mitigation against 50 drones.

II. The Administration's Consolidated Counter-Unmanned Aircraft Systems Legislative Proposal

Recognizing the growing threat posed by misuse of drones, the National Security Council assembled an interagency group to identify the critical gaps in law and policy that impede our ability to defend our national security interests and public safety from this threat. Based on the work of that group, in April of this year, the Administration released the first-of-its-kind Domestic Counter-UAS National Action Plan ("Action Plan"). That Action Plan identifies a number of gaps and includes eight recommendations to better protect the homeland from those using UAS for nefarious purposes. At the top of the list is a recommendation to "Expand Legislative Exemptions for UAS Detection and C-UAS Mitigation Activities."

The Action Plan's key recommendations are to make the authority in the 2018 Act permanent and to expand it in targeted ways based on our experience under the law and our assessment of the growing threat. The Act's authority will lapse in October 2022 if not extended by Congress. The Administration's consolidated counter-UAS legislative proposal addresses many of those recommendations. The authority remains necessary because use of UAS detection and counter-UAS technology by the Department of Justice and the Department of Homeland Security could otherwise run afoul of various criminal laws that prohibit destructive activity with respect to aircraft as well as interception of signals and communications such as those between a drone controller and a drone. *See, e.g.*, 18 U.S.C. § 32 (the Aircraft Sabotage Act); 18 U.S.C. §§ 2510 *et seq.* (the Wiretap Act, also known as Title III); 18 U.S.C. §§ 3121-3127 (the Pen/Trap Statute). These criminal laws apply even to government conduct, and where they contain exceptions (e.g., for a court to authorize interception of signals), those exceptions are not practical for protective counter-UAS missions in which decisions must be made in real-time to address threats. The exemptions in the 2018 Act do not enable use of UAS detection or counter-UAS technology to permanently protect transportation facilities such as civilian airports; other critical infrastructure such as power plants or oil refineries or chemical facilities; or high-risk prisoner transports. Nor does the 2018 Act permit State and local law enforcement to engage in any UAS detection or counter-UAS activity that require a legal exemption.

Consistent with the Action Plan's recommendations, the consolidated legislative proposal would permanently enact the exemptions that Congress provided to the Department of Justice and the Department of Homeland Security in 2018. It would not require the authority to sunset, which would give us more certainty as we plan for the future. Experience gained over the past

four years has demonstrated both the value of counter-UAS activity by the Departments of Justice and Homeland Security, and that these operations can be conducted safely and with strong safeguards for privacy and civil liberties. Permanent exemptions will enable the Departments of Justice and Homeland Security to invest more resources in this mission with confidence that it will be permitted to continue. The legislative proposal retains the requirements for semi-annual briefings to specified committees, thereby ensuring appropriate Congressional oversight.

The bill would also expand the authority of the Departments of Justice and Homeland Security in important ways to address some of the gaps identified in the Action Plan.

First, the legislation would authorize State, local, Tribal, and territorial ("SLTT") law enforcement entities and owners or operators of airports or critical infrastructure to use certain UAS *detection-only* capabilities, subject to specified conditions and safeguards. As noted above, experience has shown that the demand for protection across the country from UAS-based threats greatly exceeds the federal government's capacity. We need to empower local law enforcement agencies across the country, who are primarily responsible for keeping our citizens safe at the local level, to take the steps needed to protect their communities from this emerging threat. We also need to allow critical infrastructure operators to take steps to protect their own facilities and assets.

Notably, the "detection-only" technology that this part of the bill would authorize would not include authority to mitigate the drone through jamming or to otherwise disrupt drones or other aircraft. Rather, the information obtained through detection of drone signals can disclose the location of the drone operator, so that law enforcement or security personnel can locate that operator and address the threat through more traditional means. The detection technology authorized for use would be tested and evaluated by the Department of Homeland Security or the Department of Justice, and approved by the FAA, the Federal Communications Commission ("FCC"), and the National Telecommunications and Information Administration ("NTIA") to ensure that each system does not adversely impact the national airspace system. Only technologies on the approved list could be employed consistent with the exemptions in the law. Any non-federal entity using detection-only authority must also issue a written policy certifying compliance with the privacy protections in the bill and comply with any additional guidance issued by the Secretary or the Attorney General. This "detection-only" authority would provide significant public safety benefits and could be safely employed today.

Second, the legislation would authorize a limited pilot program for SLTT law enforcement entities, subject to a six-year sunset provision. The Departments of Justice and Homeland Security could designate annually up to 12 SLTT law enforcement entities to engage in *both UAS detection and UAS mitigation* activities, consistent with the safeguards and oversight required in the bill. Those entities would be required to receive appropriate training and vetting to enable them to both detect and mitigate UAS threats to covered facilities or assets, including mass gatherings. Because these operations could include use of more sensitive mitigation technology, all of their activities would have to be coordinated in advance with federal partners including the FAA, which could withhold approval if the FAA identifies a risk to the national airspace system from a proposed operation. Moreover, all activities will be carried

out under the direct oversight of the Departments of Justice or Homeland Security. This is an initial step that will allow Congress, the Executive Branch, and SLTT law enforcement entities to evaluate costs and benefits, learn best practices, and employ transformative technology with controls that will continue to ensure airspace safety and the proper use of the radiofrequency spectrum through required coordination with federal authorities. As with the detection-only authority, SLTT pilot program participants could only use equipment that the Department of Homeland Security maintains on a list of authorized equipment, in coordination with DOJ, FCC, NTIA, and FAA.

Third, the legislation would expressly authorize the U.S. Marshals Service ("USMS") to protect high-risk prisoner transports using UAS detection or mitigation technology. Current authority covers courthouses and prisons but does not expressly address prisoner transports. The bill would close this gap and allow the use of technology where, for example, we believe there is a substantial risk involving a terrorist or organized crime figure whose confederates could use drones to attack or monitor a transport. We estimate that there are fewer than fifty such cases in any year, and even fewer where protection might be provided.

Finally, the legislation and its corresponding policies continue to ensure that we respect privacy and constitutional rights as we conduct our UAS detection and mitigation activities, by limiting government actions towards protected First Amendment activities and restricting what information may be collected and shared. It is important to note that the technologies that we employ typically detect the presence of drones operating in a specific space and the only communications that are identified are the electronic data passed between the operator's controller and the UAS. Those communications direct the physical operation of the drone. The technologies used by the Department of Justice do not extract text messages, e-mail, or internet search histories from phones or tablets used to control drones, nor do they allow law enforcement to listen to voice calls. Specifically, the detection systems collect information such as the drone vendor and model; drone and controlling device serial number and media access control, or MAC, address; geolocation of the drone; location of the controller; and the most recent takeoff location and "home" location. This is much like the information required to be broadcasted by manned aircraft, and similar to that which the FAA will require most drones to broadcast under the Remote Identification of Unmanned Aircraft rule. However, for drones that do not comply with FAA requirements, it is critical that the government can collect the information unilaterally.

As required in the 2018 Act, the Attorney General's Counter-UAS Guidance that regulates Department of Justice component UAS detection and counter-UAS operations contains explicit protections for privacy, civil rights, and civil liberties. These include protections to ensure drones operated by the media are allowed to safely operate within FAA flight restricted areas consistent with FAA regulatory policies and procedures. Department of Justice actions under the law must be consistent with the First and Fourth Amendments, and the Department's Guidance requires each component deploying relevant technologies to train personnel on privacy and civil liberties in the counter-UAS context. Importantly, under the proposed legislation, SLTT entities and owners or operators of airports or critical infrastructure who operate detection technologies would be required to adhere to the same privacy protections imposed on federal law enforcement under the existing 2018 law.

In closing, the proposed legislation by itself will not eliminate the threats presented by malicious or irresponsible use of drones. However, it will significantly enhance our ability to mitigate this threat in a manner that is measured, responsible, and consistent with the FAA mandate to integrate drones safely into the national airspace system.

I appreciate the opportunity to testify today, and I would be pleased to answer your questions.

***

STATEMENT OF
TONYA COULTAS, DEPUTY ASSOCIATE ADMINISTRATOR
FOR SECURITY AND HAZARDOUS MATERIALS SAFETY
FEDERAL AVIATION ADMINISTRATION
HEARING BEFORE THE UNITED STATES SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS, ADMINISTRATION COUNTER-UAS NATIONAL ACTION PLAN LEGISLATIVE PROPOSAL
JULY 14, 2022

Chairman Peters, Ranking Member Portman, and members of the committee:

Thank you for inviting me to speak with you today. My name is Tonya Coultas, and I am the Deputy Associate Administrator for the Federal Aviation Administration's (FAA) Office of Security and Hazardous Materials Safety. In this role, I share the Associate Administrator's responsibilities for formulating policies and plans, and directing national programs involving internal security, intelligence analysis and threat warning, emergency response, safe air transportation of dangerous goods, and support to aviation security partners. This includes ensuring programs and operations are coordinated and integrated with the appropriate internal and external organizations, including the National Security Council, the Departments of Defense (DOD), Energy (DOE), Homeland Security (DHS), Justice (DOJ), and our other security and safety partner agencies, to resolve complex national security, safety, and crisis-response challenges. My office remains the focal point within FAA for coordinating Unmanned Aircraft System (UAS) security issues, including policy related to the use of UAS detection, as well as UAS mitigation (or "Counter-UAS") capabilities.

UAS, also known as drones, have low barriers for entry into the National Airspace System (NAS). For most small UAS, this means a lower cost to both purchase and operate, wider availability, and greater ease of operation. As a result, UAS represent the fastest growing sector in aviation today, with the last decade seeing exponential growth in the number of UAS operations. Every day, commercially-operated UAS contribute to our economy by inspecting

infrastructure, supporting industries such as agriculture, real estate, entertainment, motion pictures, and insurance, and assisting public safety agencies, which are just a few of the many diverse missions in which UAS are engaged. In time, these missions are expected to include medical and other small parcel delivery, wireless signal continuity during disaster relief, and wildfire mitigation. The need to fully integrate this technology into the NAS in a safe and secure manner continues to be a national priority—one in which both the FAA and our security partners are heavily invested.

UAS technology offers tremendous benefits to our economy and society, as Congress has recognized, but we must acknowledge that potential misuse of this technology poses unique security challenges that may enable malicious actors to exploit vulnerabilities or circumvent traditional ground-based security measures. Today, I would like to discuss with you the FAA's role in maintaining the safety and efficiency of the NAS, the status of coordination with our federal partners to support the safe integration of UAS detection and mitigation capabilities into the NAS, and the next incremental steps (as reflected in the Administration's legislative proposal) for incorporating state, local, tribal, and territorial (SLTT) law enforcement entities, airports, and other critical infrastructure into the security framework necessary to support the full integration of this technology into our aviation system.

FAA's Mission is to Ensure the Safe and Efficient Use of the NAS

The FAA's primary mission is to provide the safest, most efficient aerospace system in the world. We are responsible for providing air traffic control and other air navigation services 24 hours a day, 365 days a year, for 29.4 million square miles of airspace. In addition to this critical operational role, the FAA exercises its statutory authority to carry out this mission by issuing and enforcing regulations and standards for the safe operation of aircraft and airports, and

by developing procedures to ensure the safe movement of aircraft through the nation's skies. In exercising its authority, the FAA must recognize the public's right of transit through the navigable airspace by compliant operators.

The FAA's chief role in UAS detection and mitigation is to support our partners' testing and eventual use of these systems while ensuring the safety and efficiency of the NAS is not compromised and that the right of access to the airspace by compliant operators is preserved. Many currently-available UAS detection, tracking, and mitigation systems utilize radio-frequency (RF) based and other technologies that could potentially interfere with the aviation RF spectrum, negatively impacting air navigation services, communications, and avionics systems, which are critical to safety of flight. This requires close coordination between the FAA and our security partners. The FAA relies upon its partners to provide technical specifications and operational concepts to allow the FAA to conduct specific, data-intensive analyses for each novel UAS detection use and each potential Counter-UAS use to ensure the concept of operations balances the need for operator notification, airspace access, and appropriate airspace safety mitigations with the protective missions of our security partners. Neither the FAA nor our partner agencies want to jeopardize safety or interfere with compliant UAS operations.

FAA Integration Activities

The FAA expects UAS operations in the NAS will evolve from low-density, disconnected, visual line of sight operations, to a complex, UAS Traffic Management (UTM) based network of interconnected aircraft operating beyond visual line of sight. As this ecosystem grows in scale and complexity, we are working closely with our federal partners to develop a security framework to address the risks and vulnerabilities inherent in this system. Today, UAS

registration, implementation of remote identification (remote ID), airspace awareness, and enforcement are fundamental pillars of this security framework.

One of the biggest challenges for our federal security partners is threat discrimination—knowing who is flying and where helps the FAA and our security partners understand what the operator's intent may be, and is critical to threat assessment and response. Mandatory registration and external marking requirements contribute to security by helping to match an unmanned aircraft to its owner. Remote ID will enable authorities to connect a suspect UAS to its control station location, as well as identify the registered owner. When remote ID is fully realized, the FAA, our federal security partners, and SLTT law enforcement will have an additional tool to provide improved situational awareness that will aid in identifying, locating, and, if necessary, taking traditional enforcement actions against non-compliant UAS operators. However, even after the remote ID final rule is implemented, the FAA acknowledges that UAS detection and/or Counter-UAS authority may remain a necessary tool for our federal security partners.

Compliance with basic airspace requirements—the "rules of the road"—is essential to maintaining safety in the NAS and ultimately will make it easier for our national security and law enforcement partners to recognize a drone that is being operated in an unsafe or suspicious manner. UTM will offer a suite of capabilities that will incorporate components from the FAA, industry, and our government partners to create a comprehensive system of low-altitude airspace management for UAS. Planned UTM capabilities include a number of components—the FAA's Low Altitude Authorization and Notification Capability (or "LAANC"), remote ID, and dynamic airspace management—that will support the needs of industry, the FAA, and our security partners. To establish the UTM system, the FAA is developing a UAS regulatory and traffic

management framework that is compatible with the evolution of the technology required to support UTM and complement the Air Traffic Management system.

In addition, Congress directed the FAA in Section 383 of the *FAA Reauthorization Act of 2018* to test and evaluate UAS detection and mitigation technologies that could be used to address potential safety risks posed by UAS near airports. Also, Section 383 required the FAA to develop a plan for the certification of UAS detection and mitigation systems in the NAS, and convene an Aviation Rulemaking Committee (ARC) to make recommendations for the plan. The FAA has launched a robust testing effort and is taking steps to convene the ARC. This work is a critical step expected to inform the development of future standards for the certification of UAS detection and mitigation systems to ensure the safe integration, and reliability of, these systems for broader use in the NAS.

Advance Coordination on Policy Development and Concepts of Operations

Congress has provided the DOD, DOE, DOJ, and DHS relief from applicable federal criminal statutes in titles 18 and 49, United States Code, necessary to respond to UAS that pose a threat to designated covered facilities and assets. The FAA collaborates and coordinates closely with each federal partner to support research, testing, training, and operational use of UAS detection and mitigation technology to address UAS-based threats.

Congress established the foundation for UAS detection and mitigation coordination between the FAA and our security partners in the specific statutory provisions that granted relief from applicable federal criminal statutes to DOD, DOE, DOJ, and DHS, respectively, as well as in the FAA's authorizing statute in title 49, United States Code. Building from that foundation, the FAA and our security partners have collaborated to develop agency-specific and jointly agreed-upon processes that use objective standards to determine when, how, and what detection

or mitigation technology can be safely used in a particular location without introducing unacceptable risk to the NAS. The FAA has worked with each authorized federal department to define what actions constitute a threat; develop departmental guidance for agencies with covered missions; apply a risk-based approach to the designation of select locations for protection; develop a concept of operations that incorporates a graduated approach for measured responses; analyze and mitigate the spectrum impact of selected systems; establish flight restrictions, as appropriate, to provide public notice; and establish interagency notification protocols and reporting requirements.

Many factors have been considered in the development of these processes. For example, as noted earlier, the FAA's priority is the safety and efficiency of the NAS, as well as the preservation of access to the NAS by compliant operators. Any activity taken in furtherance of UAS detection or mitigation depends upon a thorough and jointly conducted risk-based assessment, as outlined in the current DHS and DOJ authorities. Through this process, the FAA evaluates potential secondary impacts on the NAS, identifies additional mechanisms for mitigating any secondary risk, and works with our federal partners to identify mutually agreeable solutions.

One example of an airspace mitigation that the FAA may identify as required to address potential adverse effects associated with UAS detection and mitigation systems is the establishment of a flight restriction. Flight restrictions established by the FAA serve two purposes—first, they provide advance warning to operators to stay away from an area and, second, they provide mitigation of secondary hazards introduced by the detection or mitigation system to aviation safety. The size, shape, and volume of a given flight restriction or other airspace mechanism, and whether the restriction is mandatory or advisory, is directly related to

whether we are serving one or both of those purposes. For example, the restriction may need to be tailored in size and shape to account for the mitigation of a specific hazard within the area of engagement.

The ability to provide reasonable advance notice to airspace users is also an integral requirement, which Congress recognized in the current provision for the joint risk-based assessment. From both a safety and security perspective, it is a mission essential requirement for the FAA to inform the flying public when the FAA establishes flight restrictions so that they understand where they should not operate.

A critical aspect of the Counter-UAS coordination process is the FAA's analysis of potential RF spectrum interference with navigation, communications, avionics, and other aviation-related systems—either in the air or on the ground—when a detection or mitigation system is being operated. Through technical coordination with our security partners, as well as the Federal Communications Commission (FCC) and National Telecommunications and Information Administration (NTIA), we determine whether a system will interfere with other systems operating in the NAS, such as avionics aboard manned or unmanned aircraft, or air traffic control systems. If there is interference, the FAA notifies the Department of Transportation Operations Center and works with the federal security partners to identify a solution that may allow the federal partner to conduct its security operations without compromising the safety of the NAS. We are also able to evaluate potential impacts to persons and property on the ground or to other aircraft depending upon the response of the UAS once mitigated. Recently, our federal partners have involved FAA subject matter experts in airspace safety and management in the classroom and practical training and certification processes for

Counter-UAS operators. We look forward to continuing this collaboration on system training going forward.

Coordination During Counter-UAS Operations

The FAA has also worked closely with each of its security partners to develop notification protocols during an active (*i.e.*, emitting or potentially impactful) detection or Counter-UAS event. These protocols require a federal security partner to notify the FAA's Domestic Events Network (DEN) of a UAS operation that may provoke an authorized response. Once alerted, the DEN contacts the local air traffic control facilities in the potentially affected airspace to address the possible impacts on other users of the airspace. Local air traffic control is also kept informed during and after an activation event. These protocols are designed to enable air traffic control to increase situational awareness regarding operational impacts and prepare to resolve any safety issues, provide operational support to any needed security-focused response actions, and provide an immediate alert to avoid impacting other aircraft operating in the area.

Proposed Expansion of UAS Detection and Mitigation Authorities

Unlike DOD, DOE, DHS, and DOJ, most federal departments and agencies, as well as public and private entities, lack the necessary authority to use some of the most readily available technologies to protect sensitive facilities, operations, and people from the malicious or errant use of UAS, due to constraints imposed by federal law.

The FAA provided input to help shape the Administration's proposal from the earliest stages of development. The proposal reflects a whole-of-government approach to take additional incremental steps to expand UAS detection and mitigation capabilities through relief from applicable federal statutes, and the FAA plays an integral role in nearly every aspect of the proposed expansion. We support the Administration's proposal and recognize that our security

partners need to address gaps in their authorities. As discussed, we have an excellent track record of coordination with our federal security partners, and we believe this proposal builds on that relationship to address security gaps while maintaining the essential safeguards required to protect the safety of the NAS.

The Administration's proposal includes provisions to renew, and make permanent, the relief granted to DHS and DOJ, which were established in the Preventing Emerging Threats Act of 2018, new provisions for improved federal cooperation, and measured areas of expansion based on lessons learned from federal implementation and coordination accomplished to date. These areas of expansion include ensuring DHS and DOJ are able to use UAS detection and mitigation technologies to protect airports and other critical infrastructure from UAS-based threats; limited UAS detection-only authority for the SLTT law enforcement community, airports, and critical infrastructure; and a temporary pilot program for SLTT law enforcement entities to begin using UAS mitigation technologies under direct oversight of DHS and DOJ. This pilot program will allow the federal government to evaluate the costs, risks, and benefits associated with a possible, more permanent expansion of the authority in the future, and to identify any additional necessary safeguards should the authority be expanded further. The proposal would also give the FAA authority to assess civil penalties against non-federal entities or people who use detection or mitigation technologies in an unauthorized manner that endangers the national airspace.

As we see with ground-based threats, SLTT law enforcement are most likely to be the first to identify a potential threat—like a UAS flying over people in a parking lot before a football game. The limited detection-only authority provided for in the Administration's proposal will enable law enforcement officials, as well as security personnel in their protective duties at

airports and critical infrastructure, to locate and engage the UAS operator so that they can assess the risk in real time and take appropriate action. Importantly, this will allow authorized users of UAS detection technology to detect signals from UAS that may not be remote ID-compliant.

The Administration's proposal includes a pilot program for SLTT law enforcement entities to conduct UAS mitigation activities in coordination with our federal security partners. We are confident the safeguards contained in the pilot program, including the direct oversight of all activities by DHS and DOJ, training of SLTT program participants, FAA coordination procedures, and reliance on a fully vetted federally-managed list of authorized equipment, are sufficiently robust to preserve safety of the NAS. We recognize that expanding UAS mitigation authorities beyond our current federal partners will present challenges. For that reason, the proposal takes an incremental approach to evaluating such authorities by requiring participants to work through one of the federal security agencies that already have an established track record coordinating the use of UAS mitigation technology with the FAA. Given the currently available UAS detection and mitigation technology and the impacts it can have on aircraft and NAS systems, we believe the proposal incorporates a responsible path to evaluate the benefits and risks associated with a potential broader, more permanent expansion of authority.

The Administration's proposal reflects a commitment to ensuring that any UAS detection or mitigation activities are conducted by trained and proficient users in a standardized, responsible, and deliberate manner using equipment that has been fully evaluated and authorized for use by the federal government. It leverages all existing operational coordination requirements with the FAA, FCC, and NTIA to ensure the safety of the airspace and the communications spectrum, safeguard against possible cyber intrusion, and provide for direct federal oversight of all UAS mitigation activities.

Conclusion

There is no question that a seamless security framework is critical to advancing the Administration's goal of fully integrating UAS into the NAS, thus realizing the full potential of public benefits from this technology. By renewing the vital authorities of our federal security partners and taking incremental, deliberate steps to evaluate the safest means to support SLTT law enforcement agencies and security personnel in their protective duties at airports and critical infrastructure to address emerging UAS-based threats, the United States will continue to lead the way in the full integration of UAS while offering the safest, most efficient—and most secure—aerospace system in the world. We thank the committee for its leadership on this issue, and look forward to working together to balance safety and innovation with security. This concludes my statement. I will be happy to answer your questions at this time.

July 14, 2022

The Honorable Nancy Pelosi
Speaker
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Charles Schumer
Majority Leader
United States Senate
Washington, D.C. 20510

The Honorable Kevin McCarthy
Minority Leader
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Mitch McConnell
Minority Leader
United States Senate
Washington, D.C. 20510

Dear Speaker Pelosi, Majority Leader Schumer, Minority Leader McCarthy, and Minority Leader McConnell:

We write to express our strong support for the Biden Administration's recently released draft Preventing Emerging Threats Act renewal legislation. Once fully implemented, the tailored counter-UAS legislative expansion will play an important role in helping to ensure the safety of major sporting events, including the safety of the millions of American fans who attend these events each year.

The undersigned sports organizations—the National Football League (NFL), Major League Baseball (MLB), National Association for Stock Car Auto Racing (NASCAR), and National Collegiate Athletic Association (NCAA)—collectively host thousands of events for millions of fans each year. Many of these events occur in open-air stadiums, arenas, racetracks, and other venues at which unauthorized, uncrewed aircraft system (UAS or drone) incursions are common. These incursions have been occurring for years and they are increasing in frequency.

The unauthorized use of drones (whether malicious or otherwise) presents a significant and rising threat to all large gatherings of people, including major sporting events. The NFL hosts 272 regular season football games each season, held in 30 stadiums across the country, plus additional games in the postseason. At these events, the NFL seeks to protect the over 17 million fans who attend NFL games each year as well as the 2,000 professional players and the hundreds of coaches and other staff associated with the NFL's 32 member clubs. MLB hosts 2,430 baseball games each season (plus additional games in the postseason), held in 30 stadiums across the United States and Canada. At these events, MLB seeks to protect the approximately 70 million fans who attend MLB games each year, as well as thousands of players, coaches, and other staff who are also present at those venues. Each year, NASCAR sanctions approximately 1,200 events in more than

30 U.S. states, as well as Canada, Mexico, and Europe. The NCAA and its member institutions must protect more than 40 million fans during Division I regular season and championship football games each year.

Security at these events is provided by a multilayered system that includes the sports organizations' security officials; individual team security professionals; owners and operators of stadiums and other venues; local law enforcement officials; and state and, at times and where resources permit, federal authorities. While federal authorities can and do contribute to the safety of mass gatherings like sporting events, it is simply impossible for federal officials to provide counter-drone capabilities at the thousands of sporting events conducted by our organizations.

For that reason, the sports organizations enthusiastically support the Administration's efforts to expand detection authority and implement a pilot program extending counter-drone authority, under appropriate oversight and training, to certain state and local law enforcement officials involved in protecting mass gatherings at sporting events. In addition to supporting the proposed legislation, we believe the proposed legislation could benefit from certain clarifying language explicitly stating that specified stadium events—which already receive a certain level of statutory protection—are covered by the proposed legislation. We believe this clarifying language will help ensure alignment with the Administration's and Congress's intent to close critical gaps in policy and law that directly impede the ability to protect against unauthorized drone use at protected stadium events.

The sports organizations have worked for years to combat safety and security threats posed by unauthorized drone operations, and have worked closely with policymakers in Congress and the executive branch on policies designed to mitigate threats posed by drones. We look forward to continuing to work closely with federal, state, and local government stakeholders to ensure that drones are integrated into the national airspace system in a manner which protects the safety of the millions of fans, participants, and others who attend our events every year.

Thank you for your attention to this important matter. We urge you to quickly pass this legislation so that the security benefits may be realized.

Sincerely,

National Football League
Major League Baseball
National Association for Stock Car Auto Racing
National Collegiate Athletic Association

cc:

The Honorable Maria Cantwell
Chair
Senate Committee on Commerce, Science and Transportation

The Honorable Roger Wicker
Ranking Member
Senate Committee on Commerce, Science and Transportation

The Honorable Peter DeFazio
Chairman
House Committee on Transportation and Infrastructure

The Honorable Sam Graves
Ranking Member
House Committee on Transportation and Infrastructure

The Honorable Gary Peters
Chairman
Senate Committee on Homeland Security and Governmental Affairs

The Honorable Rob Portman
Ranking Member
Senate Committee on Homeland Security and Governmental Affairs

The Honorable Bennie Thompson
Chairman
House Committee on Homeland Security

The Honorable John Katko
Ranking Member
House Committee on Homeland Security

The Honorable Dick Durbin
Chairman
Senate Committee on Judiciary

The Honorable Chuck Grassley
Ranking Member
Senate Committee on Judiciary

The Honorable Jerry Nadler
Chairman
House Committee on the Judiciary

The Honorable Jim Jordan
Ranking Member
House Committee on the Judiciary

Responses to Post-Hearing Questions for the Record from Samantha Vinograd

Question#:	1
Topic:	C-UAS Assessment
Hearing:	Protecting the Homeland from Unmanned Aircraft Systems
Primary:	The Honorable Kyrsten Sinema
Committee:	HOMELAND SECURITY (SENATE)

Question: The C-UAS legislation enacted in 2018 required DHS, in coordination with DOJ and FAA, to submit an assessment to Congress by October 5, 2019. The intent of that requirement was to provide Congress with information to help us refine and improve our nation's laws regarding countering drones. Although the content of the assessment was meaningful, unfortunately, we didn't receive it until December 2021 - two years past the statutory deadline.

As Congress considers the new C-UAS legislation I helped introduce, will DHS commit to rigorously adhere to any deadlines enacted by Congress in connection with this proposal?

Response: The U.S. Department of Homeland Security (DHS) is committed to working collaboratively with Congress and interagency partners to adhere to requirements and deadlines enacted in connection with any of our authorities.

Question#:	2
Topic:	Covered Facilities Designation
Hearing:	Protecting the Homeland from Unmanned Aircraft Systems
Primary:	The Honorable Kyrsten Sinema
Committee:	HOMELAND SECURITY (SENATE)

Question: Please provide the Committee with a list of locations currently designated as "covered facilities or assets". Additionally, are there specific examples of designated locations, beyond those already in the public record, which can be shared publicly without harming homeland security?

Response: DHS can provide a list of locations currently designated as "covered facilities or assets" to the Committee in a closed setting.

Question#:	3
Topic:	Working with Israel
Hearing:	Protecting the Homeland from Unmanned Aircraft Systems
Primary:	The Honorable Jacky Rosen
Committee:	HOMELAND SECURITY (SENATE)

Question: The U.S. does not face the threat from UAS systems alone. Many American allies, including our partner Israel, face significant UAS threats from Iran-backed proxies. Just this month, Israel Defense Forces took out three Iranian drones launched by Hezbollah toward the Karish gas field. Congress first authorized a cooperative U.S.-Israeli Counter Unmanned Aerial Systems (C-UAS) program through the Defense Department in 2018, and bilateral collaboration on counter UAS projects continues today.

Assistant Secretary Vinograd, can you give the committee an overview of how DHS is working with our Israeli partners and other international allies to counter the threat unmanned systems pose to our critical infrastructure?

Is there additional international cooperation that can help protect America?

Response: DHS works closely with FVEY and other international partners to help raise the global security baseline for a number of shared interests, including countering the threats from unmanned aircraft systems (UAS). Providing state, local, tribal, and territorial law enforcement organizations as well as critical infrastructure owners and operators with the capabilities and resources to protect their high-risk facilities is a priority for DHS. Partnering with allies to help develop proactive and strategic policies and procedures for our international counterparts is crucial to our shared success in the Countering UAS space. Working in conjunction with the Departments of State, Defense, and Justice, DHS regularly engages with partners in foreign countries to discuss shared concerns regarding UAS, Counter-UAS (CUAS) policy, C-UAS equipment evaluation, best practices that can be adopted, and lessons learned from deploying equipment and engaging with operators.

Question#:	4
Topic:	Disinformation Memo
Hearing:	Protecting the Homeland from Unmanned Aircraft Systems
Primary:	The Honorable Josh Hawley
Committee:	HOMELAND SECURITY (SENATE)

Question: You are listed as one of the authors of a memorandum to the Secretary dated September 13, 2021, re "Organizing DHS Efforts to Counter Disinformation." Sen. Grassley and I included a copy of this document in our public letter to Secretary Mayorkas dated June 7, 2022. It has been entered into the record for this hearing.

Can you authenticate this document?

Whose idea was it to draft this document?

Whose idea was it to establish a Disinformation Governance Board?

Who else was involved in drafting this document?

Response: Your first and second questions reference a document that was not released by DHS; I cannot comment on its authenticity. Your second and third questions request information about internal deliberations and recommendations, which would be inappropriate to release given the Department's responsibility to protect the integrity of its deliberative processes from the potential chilling effect of release. Secretary Mayorkas approved the charter for the Disinformation Governance Board on February 24, 2022.

Question#:	5
Topic:	Interviews
Hearing:	Protecting the Homeland from Unmanned Aircraft Systems
Primary:	The Honorable Josh Hawley
Committee:	HOMELAND SECURITY (SENATE)

Question: At the hearing, you testified that you personally interviewed Ms. Nina Jankowicz. Please provide a list of every interaction you had with her (date, time, and subject of meeting), including any interviews you conducted to evaluate her candidacy to lead the Disinformation Governance Board.

Response: As I testified on July 14, 2022, I met with Ms. Jankowicz prior to her selection consistent with the standard process for considering political appointees within the Department, and recommended her for selection based on her expertise in the field of disinformation.

Question#:	6
Topic:	Recommendation
Hearing:	Protecting the Homeland from Unmanned Aircraft Systems
Primary:	The Honorable Josh Hawley
Committee:	HOMELAND SECURITY (SENATE)

Question: When you recommended Ms. Jankowicz to lead the Board, to whom did you make this recommendation?

Please describe the nature of your recommendation and evaluation of Ms. Jankowicz's qualifications to lead the Board.

Response: As I testified on July 14, 2022, I met with Ms. Jankowicz prior to her selection consistent with the standard process for considering political appointees within the Department and recommended her for selection based on her expertise in the field of disinformation.

Question#:	7
Topic:	Twitter Posts
Hearing:	Protecting the Homeland from Unmanned Aircraft Systems
Primary:	The Honorable Josh Hawley
Committee:	HOMELAND SECURITY (SENATE)

Question: At the time of your recommendation, were you aware of any of Ms. Jankowicz's posts on Twitter?

Since your initial recommendation, have you had the opportunity to review Ms. Jankowicz's posts on Twitter? If so, do you stand by your recommendation that she lead the Board?

At the time of Ms. Jankowicz's appointment, who at the Department of Homeland Security or the White House was familiar with her posts on Twitter?

Response: As I testified on July 14, 2022, I had not read the posts of Ms. Jankowicz on Twitter that were referenced at the July 14, 2022, hearing at the time of her selection. I have since become aware of the posts. While I cannot speculate how awareness of those posts would have affected my recommendation concerning her candidacy, I can say, as I testified on July 14, that Ms. Jankowicz's expertise in the field of disinformation led me to recommend her selection. I cannot speak as to which officials at the Department or the White House may have been familiar with her posts on Twitter at the time of her appointment, as I was not familiar with those posts at that time.

Question#:	8
Topic:	White House Involvement
Hearing:	Protecting the Homeland from Unmanned Aircraft Systems
Primary:	The Honorable Josh Hawley
Committee:	HOMELAND SECURITY (SENATE)

Question: Please describe the extent of the White House's involvement in the appointment of Ms. Jankowicz.

Response: I do not have personal knowledge of the White House's involvement and cannot speculate regarding it.

Question#:	9
Topic:	Current Leadership
Hearing:	Protecting the Homeland from Unmanned Aircraft Systems
Primary:	The Honorable Josh Hawley
Committee:	HOMELAND SECURITY (SENATE)

Question: Since Ms. Jankowicz's resignation, has the Department filled her position? If so, who currently leads the Board?

Response: On August 24, 2022, Secretary Mayorkas terminated the Disinformation Governance Board and rescinded its charter consistent with the prior recommendation of the Homeland Security Advisory Council (HSAC). Accordingly, the Department has not filled Ms. Jankowicz's position.

Question#:	10
Topic:	Concerns
Hearing:	Protecting the Homeland from Unmanned Aircraft Systems
Primary:	The Honorable Josh Hawley
Committee:	HOMELAND SECURITY (SENATE)

Question: Did anyone at the Department raise concerns about Ms. Jankowicz's appointment based on her posts on Twitter?

Response: As I testified on July 14, 2022, I had not read the posts of Ms. Jankowicz on Twitter that were referenced at the July 14, 2022 hearing at the time of her selection. I cannot speculate as to whether officials at the Department raised concerns about Ms. Jankowicz's posts on Twitter, as I was unaware of the posts at that time.

Question#:	11
Topic:	Full Involvement
Hearing:	Protecting the Homeland from Unmanned Aircraft Systems
Primary:	The Honorable Josh Hawley
Committee:	HOMELAND SECURITY (SENATE)

Question: Please describe the full extent of your involvement in the Disinformation Governance Board, including its formation and selection of individuals to sit on the Board.

Response: The Disinformation Governance Board never met and has no membership. On August 24, 2022, Secretary Mayorkas terminated the Disinformation Governance Board and rescinded its charter consistent with the prior recommendation of the HSAC.

Question#:	12
Topic:	Responding to Requests
Hearing:	Protecting the Homeland from Unmanned Aircraft Systems
Primary:	The Honorable Josh Hawley
Committee:	HOMELAND SECURITY (SENATE)

Question: Have you had any personal involvement in reviewing, responding to, or delaying the Department's response to congressional oversight requests, including my several requests for all documents and communications related to the Disinformation Governance Board?

Response: The Department is evaluating requests for production of documents and communications related to the Disinformation Governance Board consistent with the standard process for responding to congressional oversight requests.

Question#:	13
Topic:	Current Status
Hearing:	Protecting the Homeland from Unmanned Aircraft Systems
Primary:	The Honorable Josh Hawley
Committee:	HOMELAND SECURITY (SENATE)

Question: The Homeland Security Advisory Council subcommittee recently concluded "that there is no need for a Disinformation Governance Board." In light of this finding, what is the current status of the Board?

Response: On August 24, 2022, Secretary Mayorkas terminated the Disinformation Governance Board and rescinded its charter consistent with the prior recommendation of the HSAC.

Question#:	14
Topic:	Reach Out
Hearing:	Protecting the Homeland from Unmanned Aircraft Systems
Primary:	The Honorable Josh Hawley
Committee:	HOMELAND SECURITY (SENATE)

Question: Did the Disinformation Governance Board or any of its members ever reach out to Twitter, Google, Facebook, Apple, or other Big Tech companies? Did they ever meet or communicate with executives at any of these companies? If so, please describe the full extent of their interactions.

Since September 13, 2021, has anyone at the Department ever reached out to Twitter, Google, Facebook, Apple, or other Big Tech companies in connection with disinformation, misinformation, or malinformation? Has anyone from the Department ever met or communicated with executives at any of these companies? If so, please describe the full extent of their interactions.

Response: The Disinformation Governance Board never met and has no membership. On August 24, 2022, Secretary Mayorkas terminated the Disinformation Governance Board and rescinded its charter consistent with the prior recommendation of the HSAC.

Your question about departmental outreach to companies is the subject of ongoing litigation in the civil matter captioned Missouri v. Biden, Civil Action No. 22-cv-1213 (W.D. La.). I cannot comment on such matters while litigation on the same subject is pending.

Question#:	15
Topic:	Documents
Hearing:	Protecting the Homeland from Unmanned Aircraft Systems
Primary:	The Honorable Josh Hawley
Committee:	HOMELAND SECURITY (SENATE)

Question: Please provide all documents related to the Department's Disinformation Governance Board, including its formation and selection of individuals to serve on the Board. For any documents that are responsive to this request but withheld from the Committee, please identify the name of each document, the date of its creation, the custodian, a summary of its contents, and the basis for withholding the record.

Response: The Disinformation Governance Board never met and has no membership. On August 24, 2022, Secretary Mayorkas terminated the Disinformation Governance Board and rescinded its charter consistent with the prior recommendation of the HSAC.

The Department is evaluating requests for production of documents and communications related to the Disinformation Governance Board consistent with the standard process for responding to congressional oversight requests.

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General *Washington, D.C. 20530*

The Honorable Gary Peters
Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Please find enclosed responses to questions arising from the appearance of Deputy Assistant Attorney General Brad Wiegmann of the Department of Justice's National Security Division before the Committee on Homeland Security and Governmental Affairs on July 14, 2022, at a hearing entitled, "Protecting the Homeland from Unmanned Aircraft Systems."

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter. The Office of Management and Budget has advised us that there is no objection to submission of this letter from the perspective of the administration's program.

Sincerely,

Christina M. Calce
Deputy Assistant Attorney General

Enclosure

cc: The Honorable Rob J. Portman
Ranking Member

RESPONSES OF
THE DEPARTMENT OF JUSTICE

TO QUESTIONS FOR THE RECORD
ARISING FROM A JULY 14, 2022, HEARING

BEFORE THE
COMMITTEE ON HOMELAND SECURITY & GOVERNMENTAL AFFAIRS
U.S. SENATE

ENTITLED
"PROTECTING THE HOMELAND FROM UNMANNED AIRCRAFT SYSTEMS"

QUESTIONS FROM SEN. SINEMA

1. The C-UAS legislation enacted in 2018 required DHS, in coordination with DOJ and FAA, to submit an assessment to Congress by October 5, 2019. The intent of that requirement was to provide Congress with information to help us refine and improve our nation's laws regarding countering drones. Although the content of the assessment was meaningful, unfortunately, we didn't receive it until December 2021 – two years past the statutory deadline.

   As Congress considers the new C-UAS legislation I helped introduce, will DOJ commit to rigorously adhere to any deadlines enacted by Congress in connection with this proposal?

Response: Yes, the Department of Justice is committed to working with other Executive Branch agencies to meet any deadlines established in law concerning reports to Congress on C-UAS matters.

2. In 2020, DOJ released a document entitled "Guidance Regarding Department Activities to Protect Certain Facilities or Assets from Unmanned Aircraft and Unmanned Aircraft Systems." Section VI of such document describes various privacy protections with respect the Department's utilization of C-UAS authorities.

   If our proposal to enhance these authorities is enacted, will you commit to the continuation of the protections under this guidance and their application to new contexts provided for under the legislation?

Response: If the proposed legislation is enacted, the Department of Justice plans to continue the privacy protections described in Section VI of the Guidance and apply them in any new contexts that may be authorized, subject only to revisions that might be appropriate to reflect any changes Congress enacts in the legislation.

Post-Hearing Questions for the Record
Submitted to Ms. Tonya Coultas
From Senator Kyrsten Sinema

"Protecting the Homeland from Unmanned Aircraft Systems"
July 14, 2022

Question 1:
The C-UAS legislation enacted in 2018 required DHS, in coordination with DOJ and FAA, to submit an assessment to Congress by October 5, 2019. The intent of that requirement was to provide Congress with information to help us refine and improve our nation's laws regarding countering drones. Although the content of the assessment was meaningful, unfortunately, we didn't receive it until December 2021 – two years past the statutory deadline.

As Congress considers the new C-UAS legislation I helped introduce, will FAA commit to rigorously adhere to any deadlines enacted by Congress in connection with this proposal?

Response:
The FAA takes the directives from Congress with utmost seriousness and we will continue to do our best to meet statutory deadlines defined by Congress.

○