

**S. 2836, THE PREVENTING EMERGING THREATS  
ACT OF 2018: COUNTERING MALICIOUS DRONES**

---

---

**HEARING**

BEFORE THE

COMMITTEE ON  
HOMELAND SECURITY AND  
GOVERNMENTAL AFFAIRS  
UNITED STATES SENATE  
ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JUNE 6, 2018

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

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

JOHN McCAIN, Arizona

ROB PORTMAN, Ohio

RAND PAUL, Kentucky

JAMES LANKFORD, Oklahoma

MICHAEL B. ENZI, Wyoming

JOHN HOEVEN, North Dakota

STEVE DAINES, Montana

CLAIRE McCASKILL, Missouri

THOMAS R. CARPER, Delaware

HEIDI HEITKAMP, North Dakota

GARY C. PETERS, Michigan

MAGGIE HASSAN, New Hampshire

KAMALA D. HARRIS, California

DOUG JONES, Alabama

CHRISTOPHER R. HIXON, *Staff Director*

GABRIELLE D'ADAMO SINGER, *Chief Counsel*

CHRISTOPHER S. BONESS, *Senior Professional Staff Member*

MARGARET E. DAUM, *Minority Staff Director*

J. JACKSON EATON IV., *Minority Senior Counsel*

SUBHASRI RAMANATHAN, *Minority Counsel*

DONNA M. PETERSON, *Minority Federal Bureau of Investigation Detailee*

LAURA W. KILBRIDE, *Chief Clerk*

BONNI E. DINERSTEIN, *Hearing Clerk*

# CONTENTS

---

Opening statements:	Page
Senator Johnson .....	1
Senator McCaskill .....	3
Senator Lankford .....	12
Senator Hassan .....	15
Senator Heitkamp .....	22
Senator Carper .....	24
Senator Hoeven .....	27
Prepared statements:	
Senator Johnson .....	39
Senator McCaskill .....	40

## WITNESSES

WEDNESDAY, JUNE 6, 2018

Hon. David J. Glawe, Under Secretary for Intelligence and Analysis, U.S. Department of Homeland Security .....	5
Hayley Chang, Deputy General Counsel, U.S. Department of Homeland Security .....	7
Scott Brunner, Deputy Assistant Director, Critical Incident Response Group, Federal Bureau of Investigation, U.S. Department of Justice .....	7
Angela H. Stubblefield, Deputy Associate Administrator for Security and Hazardous Materials Safety, Federal Aviation Administration, U.S. Department of Transportation .....	9

## ALPHABETICAL LIST OF WITNESSES

Brunner, Scott:	
Testimony .....	7
Prepared statement .....	54
Chang, Hayley:	
Testimony .....	7
Prepared statement .....	44
Glawe, Hon. David J.:	
Testimony .....	5
Prepared statement .....	44
Stubblefield, Angela H.:	
Testimony .....	9
Prepared statement .....	57

## APPENDIX

Letter from St. Louis Cardinals .....	71
Letter from Northern Plains Unmanned Aircraft Systems Test Site .....	75
Statements submitted for the Record:	
American Civil Liberties Union .....	77
Kirstjen Nielsen, Secretary, U.S. Department of Homeland Security .....	80
Security Industry Association .....	82
National Football League .....	83
Responses to post-hearing questions for the Record:	
Mr. Glawe and Ms. Chang .....	86
Mr. Brunner .....	123
Ms. Stubblefield .....	145



**S. 2836, THE PREVENTING EMERGING  
THREATS ACT OF 2018: COUNTERING  
MALICIOUS DRONES**

---

**WEDNESDAY, JUNE 6, 2018**

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

The Committee met, pursuant to notice, at 9:59 a.m., in room SD-342, Dirksen Senate Office Building, Hon. Ron Johnson, Chairman of the Committee, presiding.

Present: Senators Johnson, Lankford, Hoeven, Daines, McCaskill, Carper, Heitkamp, Peters, Hassan, and Harris.

**OPENING STATEMENT OF CHAIRMAN JOHNSON**

Chairman JOHNSON. Good morning. This hearing will come to order.

I want to thank our witnesses for your time here today and agreeing to appear, for your testimony, and I look forward to your answers to our questions.

I would like to ask consent that my prepared statement, be entered in the record.<sup>1</sup>

We also have a letter of support from the Security Industry Association that I would also like to have entered in the record,<sup>2</sup> without objection. Senator McCaskill.

Senator MCCASKILL. No objection.

Chairman JOHNSON. OK. Did you want to—

Senator MCCASKILL. Yes, Mr. Chairman, I would like to place into the record testimony that has been provided by the Director of Security and Special Operations of the St. Louis Cardinals.<sup>3</sup> I am really proud that the Cardinals are one of only four Major League Baseball (MLB) teams to achieve the “SAFETY” designation and distinction from the Department of Homeland Security (DHS) by working countless hours to make sure that their stadium facility is secure and that they have the proper procedures and protocol and training in place for the personnel there to keep the best fans in baseball happy, secure, and having a wonderful time with their families. They have submitted testimony on this subject to

---

<sup>1</sup>The prepared statement of Senator Johnson appears in the Appendix on page 39.

<sup>2</sup>The letter referenced by Senator Johnson appears in the Appendix on page 82.

<sup>3</sup>The letter referenced by Senator McCaskill appears in the Appendix on page 71.

the Committee, and I would ask that this testimony be made part of the record today.

Chairman JOHNSON. Without objection.

Milwaukee fans are pretty good, too.

Senator MCCASKILL. Not as good as Cardinals. Sorry. [Laughter.] More World Series than everyone but the New York Yankees.

Chairman JOHNSON. OK.

Senator MCCASKILL. We do not have the payroll or the market. [Laughter.]

Sorry. Do not get me started.

Chairman JOHNSON. On that note of nonpartisanship, we had a secure briefing yesterday, and a number of you were in attendance. I appreciate that. I am always leery of holding in open session these hearings on different threats because I really do not want to give the bad guys any ideas. I am certainly willing to make an exception in this case because I think the threats are just so incredibly obvious, and one thing that made a pretty big impression on me, which is why we have a video screen set up—if we can run it right now—is a video that was shown in that setting, which is totally not secure. This is the Islamic State of Iraq and Syria (ISIS) video put out on YouTube to basically brag about what their capabilities are when it comes to the use of drones. So why do we not quickly show that for the Committee.

[Video played.]

This is an ISIS drone all ready to drop a grenade on an Iraqi target. It looks like something coming out of the U.S. Defense Department (DOD), quite honestly, when we get it to run. It looks like something out of our Defense Department, but this is from ISIS. This is all part of their propaganda. If we can get this thing going?

Senator CARPER. Well, their drones are slow. [Laughter.]

Chairman JOHNSON. They are really not. It is well worth seeing, so we will take—

Senator MCCASKILL. Who is trying to run it?

[Video played.]

Chairman JOHNSON. It is a good thing I am not in charge because it would never get done.

Senator CARPER. What are we looking at?

Chairman JOHNSON. So this is a YouTube video posted by ISIS, and it is showing their use of a drone against an Iraqi site. I am not exactly sure. Maybe one of the witnesses can tell us what they are actually using the drone against.

Mr. BRUNNER. Chairman, it is our understanding that ISIS is targeting an Iraqi counter-improvised explosive device (IED) unit that is approaching a location.

Chairman JOHNSON. OK. Are we going to get it? OK. So you can go on YouTube and actually see it for yourself, but it is frightening. And as we began this discussion—and, really, from my standpoint, the discussion started when I was interviewing Secretary Nielsen for her current position, and she said that her top priority was getting the authority to counter this emerging threat that I think we are so far behind the curve on. I was shocked. I just assumed that if there were drones threatening, whether it is the Cardinals baseball stadium, the Brewers stadium, or whatever the U.S. Secret Service (USSS) trying to protect our President or Vice President,

activities along the border, we have no authority to counter those drones. We have given some limited authority to the Defense Department, and that is about it. They are kind of in the early stages of working with the Federal Aviation Administration (FAA), and it sounds like it is a very cooperative effort here, which we need. So from my standpoint, the piece of legislation we have introduced with bipartisan cosponsors, the Preventing Emerging Threats Act of 2018, is just a table stakes piece of legislation.

One of the reasons I wanted to hold this hearing today, we have the debate and hopefully the passage of the National Defense Authorization Act (NDAA) coming up over the course of the next couple of weeks. It is my goal to get this piece of legislation attached to that, hopefully just in the manager's amendment, so we give DHS and the agencies under the Department of Justice (DOJ) the authority, just the table stakes authority to begin the process, the very complex process, of addressing this threat that has really been there, and we should thank our lucky stars that we have not seen a real tragic incident coming from this.

Again, I appreciate the witnesses being here. With that, I will turn it over to our Ranking Member.

#### **OPENING STATEMENT OF SENATOR MCCASKILL<sup>1</sup>**

Senator MCCASKILL. Thank you, Mr. Chairman, and thank you for holding the hearing. I look forward to continued work with you on this bill and that we can hopefully continue to adjust and take input to provide the kinds of authorities needed for our government to keep us safe, while at the same time protect Americans' privacy.

The Department of Transportation (DOT) estimates that there could be as many as 4 million drones owned and operated by recreational and commercial users by 2021, and the FAA estimates that recreational and commercial drone sales will increase to 7 million by 2020. We know that drones can be used for good and for bad. People fly them for fun and use them to take amazing aerial photographs. They are used for crop dusting, newscasting, and I understand that they have great potential for precision agriculture, which is so necessary today in light of all the challenges and stresses that our farming families face in terms of input costs.

Drones also play a critical role for public safety. We know they support firefighting, search and rescue operations, and that they monitor critical infrastructure. We are constantly innovating in America, and in just a few years drone capabilities and advancements may far exceed our imagination today. We must encourage and foster that innovation in Congress.

But, unfortunately, drones have the potential to cause great harm. Terrorist organizations, as the Chairman has just indicated, have used drones overseas, and we expect that terrorists are interested in exploiting those same capabilities here in the United States.

The Federal Bureau of Investigation (FBI) Director has testified that the threat of that terrorists will use drones in the United States is imminent. As the Director explained to this Committee, drones are easy to acquire and operate but are "quite difficult to

<sup>1</sup>The prepared statement of Senator McCaskill appears in the Appendix on page 40.

disrupt and monitor.” That is the challenge we face: how to disrupt and monitor the bad guys without interfering with privacy or recreational uses of these instruments by the American public.

Then-Acting Secretary Elaine Duke testified that drones could be used to transport illicit materials or for violent purposes, and that we lack the signals to interdict drones. Just last month, we heard from Secretary Nielsen, who expressed concern about drones as a “very serious, looming threat,” and that the Department is unable to effectively counter malicious use of drones because they are hampered by Federal laws enacted long before the unmanned technology existed.

I would really like to hear DHS and DOJ address today, in this public hearing, how they can help owners and operators of critical infrastructure secure mass gatherings. I understand that you do not have this authority yet, but if you do, I want to know how you intend to leverage your authority to help State and local stakeholders. What do they get out of Congress passing this bill? What do the people that are running the 4th of July parade in Webster Groves get from this legislation? How are we helping them address the threat where it will really come home? And, that is, through the interdiction of drones in situations where casualties could occur by people who want to destroy not just the United States but our way of life.

I want to thank the DHS, FBI, and FAA for working with the Committee to help develop the language in our bill. It was informed by the findings of an interagency group, which I understand you were all a part of, that identified impediments and gaps in the Federal Government’s ability to respond. The interagency committee concluded that without changes in the law, Federal agencies will be prevented from developing, testing, evaluating, and countering most drone technologies that we need to address.

I look forward to hearing from our witnesses today about how this act helps you address these gaps and impediments. I also look forward to hearing from other stakeholders, many who I understand will submit statements for the record about ways in which we can ensure that any legitimate concerns are addressed before we move a bill out of Committee.

We have a real security threat that I think we must address, and I look forward to working with the Chairman to make sure that our legislative approach is the right one.

Thank you, Mr. Chairman.

Chairman JOHNSON. Thank you, Senator McCaskill.

It is the tradition of this Committee to swear in witnesses, so if you will all 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?

Mr. GLAWE. I do.

Ms. CHANG. I do.

Mr. BRUNNER. I do.

Ms. STUBBLEFIELD. I do.

Chairman JOHNSON. Please be seated.

Our first witness is the Honorable David Glawe. Mr. Glawe is the Under Secretary for Intelligence and Analysis at the Department of Homeland Security. Prior to his confirmation, he was a

Special Assistant to the President and served several years as the Assistant Commissioner and Chief Intelligence Officer in Customs and Border Protection (CBP) for DHS. Mr. Glawe has a certificate from the John F. Kennedy School of Government at Harvard University and a Bachelor of Arts degree from the University of Northern Iowa. He has also received the National Intelligence Superior Service Medal for his work supporting the intelligence community and promoting our national security. Mr. Glawe.

**TESTIMONY OF THE HONORABLE DAVID J. GLAWE,<sup>1</sup> UNDER SECRETARY FOR INTELLIGENCE AND ANALYSIS, U.S. DEPARTMENT OF HOMELAND SECURITY**

Mr. GLAWE. Chairman Johnson, thank you, Ranking Member McCaskill as well, thank you.

Chairman Johnson, Ranking Member McCaskill, and distinguished Members of the Committee, thank you for inviting DHS to speak with you today. We appreciate the opportunity to discuss the Department of Homeland Security's role in countering threats from unmanned aircraft systems (UAS) or drones, in our national airspace system (NAS).

First, I would like to thank the Committee for its attention to this issue and holding this hearing to highlight the critical importance of the interagency efforts to secure the national airspace. I would also like to thank Chairman Johnson, Ranking Member McCaskill, and the other Members of this Committee for introducing and cosponsoring a bill that addresses security threats from small unmanned aircraft systems. With enactment of this proposal, Congress would reduce risks to public safety and national security and ensure that the United States remains a global leader in unmanned aircraft innovation.

Unmanned aircraft systems offer tremendous benefits to our economy and society. They promise to create countless American jobs, transform the delivery of household goods, improve safety of dangerous occupations, and expand access to life-saving medical supplies. DHS strongly supports the Federal Aviation Administration's efforts to integrate unmanned aircraft systems into our national airspace. We must also recognize the increasing security challenges that require a layered and parallel government security response to protect the public from the misuse of this technology.

This threat is real. We are witnessing a constant evolution in the danger posed by drones as the technology advances and becomes more available and affordable worldwide. Commercially available drones can be employed by terrorists and criminals to deliver explosives or harmful substances, conduct surveillance both domestically and internationally against U.S. citizens' interests and assets. We know ISIS fighters in Iraq and Syria have used unmanned aircraft to deliver explosives and continue to plot unmanned aircraft use in terrorist attacks elsewhere. This is a significant threat to the homeland.

The technology also presents a growing risk to law enforcement officers as they execute their mission. On the Southern Border,

---

<sup>1</sup>The joint prepared statement of Mr. Glawe and Ms. Chang appears in the Appendix on page 44.

transnational criminal organizations (TCOs) are using drones to traffic narcotics and conduct countersurveillance to avoid U.S. law enforcement and interfere with ongoing law enforcement operations. The U.S. Coast Guard (USCG) is also observing increased overflights of unmanned aircraft while performing its missions. I am confident this threat will evolve and malicious use of drones will be more sophisticated.

Current statutory authorities do not address threats posed by careless, reckless, or malicious use of drones. DHS needs counter unmanned aircraft system (C-UAS) authorities to detect, track, and mitigate threats from small unmanned aircraft. Without this authority, DHS is unable to develop and deploy countermeasures to mitigate nefarious use of this technology. The enactment of this bill will be a first step to secure our borders, protect critical infrastructure and large crowds at special events, and provide direct support to our State and local partners.

This bipartisan legislation you cosponsored represents a critical step in enabling the Department of Homeland Security to address this vulnerability. It is similar to the existing statutory authorities granted to the Department of Defense in the 2017 and 2018 National Defense Authorization Acts, and it contains robust measures to protect privacy and civil liberties.

The threat is real and dynamic. Malicious cyber actors, transnational criminal organizations, terrorists, and foreign intelligence services have used it and will use it for nefarious purposes. I support your introduction of this bill which acknowledges the need for flexibility to address this threat and perform our mission.

Chairman Johnson, Ranking Member McCaskill, and distinguished Senators of the Committee, thank you again for your attention to this important issue. I look forward to the partnership as we address the threat and continue our work to protect the homeland. My colleagues and I look forward to answering your questions.

Chairman JOHNSON. Thank you, Mr. Glawe.

Our next witness is Hayley Chang. Ms. Chang is the Deputy General Counsel for DHS. She has previously served in the Department of Justice as an Assistant U.S. Attorney. She also served as Counsel to the Deputy Attorney General (AG) and advised DOJ leadership on the Committee on Foreign Investment in the United States. Ms. Chang is a graduate of Cornell Law School and holds a Bachelor's degree from Hillsdale College.

Do you have a statement or are you just here to answer questions?

Ms. CHANG. Yes, Mr. Chairman.

Chairman JOHNSON. OK. You are here to answer questions?

Ms. CHANG. I have a statement.

Chairman JOHNSON. OK, great. Go ahead.

**TESTIMONY OF HAYLEY CHANG,<sup>1</sup> DEPUTY GENERAL  
COUNSEL, U.S. DEPARTMENT OF HOMELAND SECURITY**

Ms. CHANG. Thank you. Good morning, Chairman Johnson, Ranking Member McCaskill, Members of the Committee. Thank you for asking DHS here today to talk about the emerging drone threat. Thank you for your bill, the Preventing Emerging Threats Act of 2018, which gives our officers the tools they need to evolve with the threat and keep our families and communities safe.

I would like to especially thank you for a critical piece of that bill, the opening line, “Notwithstanding any provision of Title 18 United States Code.” That is the heart of the issue. Without direction that is that clear, our front-line officers will find their hands continually tied as they try to keep us safe.

Because technology is evolving faster than the law, things that were not illegal yesterday are suddenly deemed illegal today. Things that are not illegal today could be deemed illegal tomorrow. While some have suggested smaller, short-term fixes, tweaks and new exceptions to individual subsections of the code, that would not give our front-line officers the clarity that they need. It is too much to place that burden on our front-line officers to risk uncertainty and confusion when they need to move forward to address this threat. And, worse, without a law that is this clear, we put our officers at risk for criminal penalties just for doing their jobs. That is why we thank you for taking the straightforward approach. Just like Congress provided last fall for our partners at the Department of Defense and the Department of Energy (DOE), this clear guidance communicates to our front-line officers that they are valued and empowered to do their jobs.

We look forward to answering the Committee’s questions today. Thank you.

Chairman JOHNSON. Thank you, Ms. Chang.

Our next witness is Scott Brunner. Mr. Brunner is the Deputy Assistant Director of the Critical Incident Response Group (CIRG) for the Federal Bureau of Investigation. Prior to his current role, Mr. Brunner served as the Assistant Special Agent in Charge of the National Security Intelligence Program of the Louisville FBI Division. Mr. Brunner joined the FBI in 1995 as a Special Agent in the Portland Division and has been in law enforcement since 1992, when he became a patrol officer for the Oklahoma City Police Department. Mr. Brunner.

**TESTIMONY OF SCOTT BRUNNER,<sup>2</sup> DEPUTY ASSISTANT DIRECTOR,  
CRITICAL INCIDENT RESPONSE GROUP, FEDERAL BUREAU OF INVESTIGATION,  
U.S. DEPARTMENT OF JUSTICE**

Mr. BRUNNER. Good morning, Chairman Johnson, Ranking Member McCaskill, and members of the Committee. Thank you for the opportunity to discuss the FBI’s concerns regarding the threat posed by unmanned aircraft systems. On behalf of the men and women of the FBI, let me begin by thanking you for your ongoing support of the Bureau.

<sup>1</sup>The joint prepared statement of Ms. Chang and Mr. Glawe appears in the Appendix on page 44.

<sup>2</sup>The prepared statement of Mr. Brunner appears in the Appendix on page 54.

Today's FBI is a global, threat-focused, intelligence-driven organization. Each FBI employee understands that to defeat the threats facing our Nation, we must constantly strive to be more efficient, effective, and looking over the horizon. Just as our adversaries continue to evolve, so must the FBI. We live in a time of acute and persistent terrorist and criminal threats to our national security, our economy, and our communities. These diverse threats underscore the complexity and breadth of the FBI's mission.

We remain focused on protecting the United States against terrorism, foreign intelligence, and cyber threats; upholding and enforcing the criminal laws of the United States; protecting privacy, protecting civil rights and civil liberties; and providing leadership and criminal justice services to our Federal, State, municipal, and interagency partners.

One significant threat to the safety of the American people concerns low-cost UAS. Today's UAS have evolved considerably from the early remote control aircraft of the 20th Century. UAS now have longer flight durations, larger payloads, and sophisticated maneuverability. They are easy to acquire, relatively easy to operate, and quite difficult to disrupt and monitor. Rapid development of UAS technology offers substantial benefits such as creating new and innovative ways to deliver goods and services and providing a safe means of inspection of critical infrastructure.

But this technology also raises new risks. If operated negligently, recklessly, or maliciously, UAS can cause injuries, damage, and death. The FBI is concerned that criminals and terrorists will exploit UAS in ways that pose a serious threat to the safety of the American people. Sadly, these threats are not merely hypothetical. For more than 2 years, the Islamic State of Iraq and ash-Sham and other terrorist groups overseas have perfected the use of cheap, commercially available drones for attacks and reconnaissance. As Director Christopher Wray testified last year, the FBI is concerned that these deadly tactics will soon reach our homeland in the form of domestic attacks, domestic terrorist attacks, illegal surveillance over critical infrastructure, or as a vehicle for either chemical, biological, radiological (CBR) attack or traditional kinetic attacks on large open-air venues such as concerts, ceremonies, and sporting events, or attacks against government facilities, installations, and personnel. That threat could manifest itself imminently.

In addition to national security threats, UAS pose criminal threats. Drug traffickers have used UAS to smuggle narcotics across the U.S. Southern Border, and criminals have used UAS to deliver contraband inside Federal and State prisons. Similar to national security threat actors, criminal actors have utilized UAS for both surveillance and countersurveillance in order to evade or impede law enforcement.

UAS technology renders traditional, two-dimensional security measures, such as perimeter fences and security gates, ineffective, enabling criminals, spies, and terrorists to gain unprecedented, inexpensive, and often unobtrusive degrees of access to previously secure facilities. Finally, the mere presence of UAS operations in the vicinity of an emergency scene, even negligently, could impede emergency service operations, especially aviation-based responses.

At present, the FBI and our Federal partners have very limited authority to counter this new threat. Potential conflicts in Federal criminal law limit the use of technologies that would enable the FBI to detect or, if necessary, to mitigate UAS that threaten critical facilities and assets. Absent legislative action, the FBI is unable to effectively protect the United States from this growing threat. As you know, the Administration recently proposed counter-UAS legislation designed to fill this gap. The legislation would authorize the Department of Justice and the Department of Homeland Security to conduct counter-UAS activities notwithstanding potentially problematic provisions in the Federal code. The legislation would extend these authorities within a framework which provides appropriate oversight, protects privacy and civil liberties, and maintains aviation safety.

Chairman Johnson, Ranking Member McCaskill, and Members of the Committee, thank you again for this opportunity to discuss the FBI's concerns regarding the threats posed by UAS. We are grateful for the support you have provided to the FBI, and your support makes a difference every day in the lives of Americans that we strive to protect. We welcome the introduction of the Preventing Emerging Threats Act of 2018. This legislation would provide the authorities requested in the Administration's proposal, which we believe are necessary to mitigate the national security and criminal threats posed by UAS.

I look forward to discussing this important legislation with the Committee today.

Chairman JOHNSON. Thank you, Mr. Brunner.

Apparently we do have the video ready, but we are not going to run it now. I want you to get it ready, so as soon as Ms. Stubblefield is done with her testimony, we can hit play.

Our next witness is Angela Stubblefield who has served as the Deputy Associate Administrator for Security and Hazardous Materials Safety for the Federal Aviation Administration since 2013. She previously served as the Director of National Security Programs and Incident Response for FAA. Prior to joining FAA, Ms. Stubblefield served both as active-duty and in civilian positions for the United States Marine Corps. She graduated from George Mason University with a Master's in transportation policy, operations, and logistics and a Bachelor's degree from the University of Virginia. Ms. Stubblefield.

**TESTIMONY OF ANGELA H. STUBBLEFIELD,<sup>1</sup> DEPUTY ASSOCIATE ADMINISTRATOR FOR SECURITY AND HAZARDOUS MATERIALS SAFETY, FEDERAL AVIATION ADMINISTRATION, U.S. DEPARTMENT OF TRANSPORTATION**

Ms. STUBBLEFIELD. Thank you, Mr. Chairman, and good morning, sir. Good morning, Ranking Member McCaskill and Members of the Committee. Thank you for inviting the FAA to speak today.

The FAA's primary mission is to provide the safest, most efficient airspace system in the world. We ensure aircraft move safely through the Nation's skies 24 hours a day, 365 days a year, over nearly 30 million square miles of airspace.

<sup>1</sup>The prepared statement of Ms. Stubblefield appears in the Appendix on page 57.

UAS technology represents the fastest-growing sector in aviation today. In fact, the FAA recently surpassed 1 million UAS registrations. And while UAS technology offers tremendous benefits to the economy and society, we recognize the misuse of this technology poses unique security challenges. I would like to discuss the FAA's work with our security partners to address these threats, our focus on ensuring safety and maintaining airspace efficiency, while supporting national security and law enforcement missions, and taking the next steps in building a robust security framework that supports the full integration of this technology in our aviation system.

Collaborating with our national defense, homeland security, and law enforcement partners is not new to the FAA. Close coordination with our partners to address the UAS security challenge is a natural extension of these time-tested and well-exercised relationships. We have been working together successfully to address manned aircraft risks for decades. We continue to work together to improve the government's ability to respond to threats posed by both manned and unmanned aircraft operations, but more must be done if we are to realize the full benefits of safe and secure UAS integration.

Congress granted the Departments of Defense and Energy counter-UAS authorities in December 2016. Recently the Administration released a legislative proposal to give the Departments of Homeland Security and Justice similar authorities to protect against UAS threats to certain facilities, assets, and operations critical to national security. We support this phased approach, as well as the inclusion of provisions in this Committee's proposal for robust coordination and risk-based assessment which will ensure aviation safety is not compromised.

The FAA's role in counter-UAS is to support our partners' testing and eventual use of these systems while maintaining the safety and overall efficiency of the NAS. The FAA is responsible for balancing the requirements of our security partners' protective missions with the need for operator notification, airspace access, and airspace safety mitigations.

The FAA is currently working with the Department of Defense and the Department of Energy to strike this balance as they deploy counter-UAS technology at sensitive facilities in the United States. We are full partners in their efforts to implement these systems and have received the same commitment from DHS and DOJ should they be granted counter-UAS authority.

In addition to working closely with our Federal partners, FAA is progressing on a host of other actions that support both safe and secure UAS integration, including publishing an Advanced Notice of Proposed Rulemaking (ANPRM) to solicit information on UAS security concerns impacting integration, establishing remote identification requirements for UAS, restricting UAS operations over certain Federal facilities, and appropriately warning operators in proximity to these restricted sites.

Being able to associate a drone in flight with the operator on the ground is crucial to enabling more complex operations and the ability of our law enforcement and national security partners to identify and respond to security risks. Anonymous operations in the na-

tional airspace system are inconsistent with safe and secure integration.

But even as the FAA is working to establish remote ID requirements, challenges remain. In particular, the current exemption for model aircraft, Section 336 of the FAA's 2016 reauthorization, makes it nearly impossible for the FAA to develop new regulatory approaches that facilitate safe and secure UAS integration. This exemption promotes the misperception by many recreational UAS operators that they are not required to follow basic safety rules. To address this challenge, a basic set of requirements, including registration, remote identification, and observance of airspace restrictions, must be applied to all UAS operators. This is essential to ensuring clueless and careless operators fly safely. However, mitigating criminal threats requires our security partners have the counter-UAS authorities and tools central to today's discussion.

There is no question that a robust security framework is critical to advancing the Administration's goal of full UAS integration. By enabling Federal security and law enforcement agencies to detect and mitigate UAS threats, we will continue to lead the world in UAS integration while offering 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 with you to balance safety and innovation with security.

This concludes my statement. I am happy to answer any questions.

Chairman JOHNSON. Thank you, Ms. Stubblefield.

It looks like we have the video ready to go, so if we can just quick play that.

[Video played.]

Senator MCCASKILL. There it goes.

Chairman JOHNSON. It does not need narration.

So, again, that is an ISIS drone. They posted this on YouTube. They let loose a grenade very accurately over the target. So this is not a theoretical threat. This is a threat, and we all know ISIS has their Inspire magazine and other ways of communicating how to do these things.

As is kind of my tradition, I am going to turn the questioning over to other Members to respect their time, but I do want to quickly read a couple of sentences out of a letter I just received today, June 6th, from the American Civil Liberties Union (ACLU)<sup>1</sup> who opposes this piece of legislation. And I want the witnesses to keep that in mind and address it, talk about your viewpoint versus the ACLU's viewpoint.

To quote: "The National Defense Authorization Act for Fiscal Year (FY) 2018 authorized the Department of Defense to take action in cases where drones pose a threat to certain assets and facilities. Given this, there are practical questions regarding whether additional DHS or DOJ authority is needed to protect against the safety threats that could be posed by drones."

Again, I really want you to concentrate, because I was shocked by the fact that we do not have authority to counter this. So if you

<sup>1</sup>The letter referenced by Senator Johnson appears in the Appendix on page 77.

can just kind of keep that in mind as we go through questions by the Committee, and with that, I will turn it over to Senator McCaskill.

Senator MCCASKILL. I will defer and allow other Members to question first also.

Chairman JOHNSON. Then it would be Senator Lankford.

#### OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. Thank you both for deferring to give us time for questions. Thank you for your testimony.

Let me ask a couple of questions. For the FAA, current restrictions right now on registration, a UAS has to be 50 pounds. Is that correct?

Ms. STUBBLEFIELD. It is greater than 0.55 pounds and less—well, first, sir, all aircraft have to be registered.

Senator LANKFORD. Right.

Ms. STUBBLEFIELD. As it pertains to small UAS, if they are greater than 0.55 pounds and less than 55 pounds, they can be registered through the Web-based application. If they are greater than—55 pounds or over, they have to participate in our normal registration process that we use for manned aircraft.

Senator LANKFORD. So when was that weight—the 55 pounds max there, so there is a pretty big spectrum that has happened in the development of the UAS over the past several years where weight is coming down significantly. A 55-pound UAS is fairly rare in the commercial field at this point. So is there a reevaluation that is needed on that as far as the weight base?

Ms. STUBBLEFIELD. Thank you for that question, Senator. The FAA's primary mission and focus being on safety, we evaluate the weight and capabilities based on the potential safety risk that they could pose. So as we look at expanding operations, that is part of the discussion in terms of what are the requirements to ensure safety. With the more weight that the UAS has, the greater requirements for safety mitigations to ensure that it does not pose a safety risk when flying.

Senator LANKFORD. But that is currently under reevaluation or do you think that is not under reevaluation, that 55 is considered the right weight and size?

Ms. STUBBLEFIELD. Senator, the 55-pound distinction is largely around what we consider to be a small UAS, and for the requirements around the Part 107 rule and the requirements that are required for that versus if they are larger than 55 pounds, then there are other certification and operator requirements that are provided. As we move to more complex operations, the requirements are going to be associated with the potential safety risk that particular aircraft pose.

Senator LANKFORD. So is there a size limitation as well, again, with composites and other things coming online now, that they can have very significant size and still be under 55 pounds?

Ms. STUBBLEFIELD. No, sir, and the 55 pounds also includes anything that is attached to or being carried by the UAS as well.

Senator LANKFORD. All right. Let me ask of DHS on this, the difficult question that civil libertarians are going to talk about is who makes the decision, especially when you are talking about an un-

manned aerial system being seized at an event, at a location. So the authorities that we are discussing at this point, who would make the decision on when those authorities go into place, what event, what location you would not be allowed to use a UAS and what time, and then who would grant the seizure authority of that, because that is a key constitutional issue.

Mr. GLAWE. Senator, thank you for the question. And you are actually right, it is a key constitutional question on a Fourth Amendment seizure, how that would work. The legislation allows us to create the policies and procedures and tactics and help develop the technical capability on how to deploy that. To my colleague from the FBI and the national security events and how DHS works that partnered with them, it is clear on that mission in the lines of how we work that and provide that security. This enabling of this new legislation, which is critical to the safety of the homeland, will allow us to start developing those programs and policies and technology on how to deploy it. But the command and control is critical on that once a threat is identified and a reaction is imminent.

I will let my Deputy General Counsel articulate the legal aspect of that as well.

Senator LANKFORD. All right.

Ms. CHANG. Yes, thank you. The decision as to where these technologies will be deployed is going to be made at the highest level. The Secretary and/or the Attorney General will make the initial designation in consultation with the FAA under the bill, and that will be done through a risk-based assessment. So it will be a careful process where we see the highest risk based on one of the—it will need to be connected to one of the missions enumerated in the statute, and then the actions will need to be taken under the bill necessary to mitigate the threat. So it is a fairly limited scope.

And in terms of who will be making those decisions, the personnel have to be with assigned duties of safety or security or protection, so this will not be a broad sweeping investigative tool. They will be protective.

Senator LANKFORD. Just walk me through this. You are trying to make a decision on what is happening in Oklahoma, so there is a Bedlam football game, and half the State is either watching or at the game. Is that a national event or is that a State responsibility to be able to monitor what is happening around that event? Is it different if it is the Super Bowl versus that if it a college football game in a State? When you start talking about authorities and how you are going to be able to monitor this and how you are going to track what events, what locations, that decision has to be made, and we have to provide some clarity to that.

Ms. CHANG. Yes, sir, and currently we have a process in place for handling security at those events, and this would build upon that by adding the C-UAS authority. But, essentially, the homeland security advisers of the States, if it is a State event, will reach out and State and locals or private sector will reach out through their homeland security advisers. The process is in place. The lead is the Secret Service, but the FBI is involved as well, and there is a process for giving each event—if it is not the Super Bowl, they will each have Special Event Assessment Rating (SEAR) rating

events, and based on the threat we will deploy resources as necessary.

Senator LANKFORD. Right. Well, Scott can tell you the Bedlam football game is bigger than the Super Bowl game anytime on a college game. But when we talk about this local FBI engagement, this becomes a key issue on the civil liberties issue. I do not think any of us deny there is a real threat here. The unmanned aerial system to me is kind of like the Internet. It can be used for good or bad. We want to focus on the good aspects of it and be able to broaden the capabilities. But we also want to be aware it can be used for bad and how we are trying to address this. The key issue that we have to address is: What is a national focus? What is a State response and a local focused on that?

Scott, how will the FBI be able to handle that as far as that partnership and that relationship together?

Mr. BRUNNER. Yes, sir. Thank you, Senator, for the question. So from a Federal perspective, we get together and break all these events down into either National Special Security Events (NSSEs), like the political conventions, like the State of the Union address. Those are overseen by the Federal entities. The majority of the other events we break down into—they are called “SEARs.” That is everything from something like the Bedlam football game to the Kentucky Derby to other things that are of national importance but primarily rest with the State and local authorities for responsibility. This law would give us a unique ability to go in at the request of the Governor or the Attorney General and provide the resources that we have in the counter-UAS arena, working extremely closely with our State and local partners, who actually oversee the security of the event. So we would be in addition to them. It would enable us to go in with the technologies that we have provided by the authorities in this bill and support them in protecting those types of events.

Senator LANKFORD. All right. Thank you.

Chairman JOHNSON. I think this would be a good point to really clarify what authorities currently exist and what authorities this bill actually grants. So do you have a list of what those would be? Because, again, this is incredibly limited authority. Currently the Department of Defense has incredibly limited authority over their facilities. Again, whoever can actually lay out here is the authority the Defense Department has, this is the very limited authority prioritized that this bill would grant. This does not give DHS the authority to knock down drones flying around in your backyard. So who could do that? Is that you, Ms. Chang?

Ms. CHANG. Yes, sir, I can answer that. So right now, to address in particular the ACLU’s point about this not being needed because DOD already has the authority, DOD, as you point out, has very limited authority to protect certain critical assets of theirs. It does not cover assets of the Department of Homeland Security or the Department of Justice or these mass gathering events. And so that is what—the Committee’s bill would add DHS and DOJ. It would allow us to cover what are designated as covered facilities or assets by the Secretary or the Attorney General through risk-based assessment, and those could include, based on risk, these special events. But they have to be tied to core missions for us. That is

primarily the Secret Service protecting the President and protectees. The Coast Guard, CBP, DHS is primarily the Marshals and FBI. It also limits how we can do it. It has to be necessary to mitigate the threat, which is a pretty high bar. Generally our use-of-force rules, and DOD is under these as well, operating domestically, are reasonableness. And this would be a higher bar with necessary to mitigate the threat.

And so once that threat is over, our authority ends. We have the authority to disrupt that threat, get that drone down. And then we have also robust protections, both front end and back end, in the statute to limit to protect retention of that data and also oversight of Congress as well as the Executive Branch.

Chairman JOHNSON. And, by the way, State and local authorities have no authority to do this, correct?

Ms. CHANG. That is correct, sir.

Chairman JOHNSON. One of the concerns, I know, as we were drafting the bill, was DHS did not want to assume protective authority over everybody. You simply do not have the resources, so, again, I cannot emphasize enough this is incredibly limited authority. This is just a first step, table stakes authority, with an awful lot of studying, a lot of cooperation with FAA in terms of the complexity of the situation. Senator Hassan.

#### **OPENING STATEMENT OF SENATOR HASSAN**

Senator HASSAN. Thank you, Mr. Chairman and Ranking Member McCaskill, for holding this hearing, and thank you all for being here.

Ms. Chang, I want to follow up a little bit on the discussion we were just having because I would like to better understand the Department's expectations for how this authority is actually going to be implemented. As I understand it, the bill broadly allows DHS or Justice Department personnel under the circumstances you have described to shoot down a drone if the drone threatens the airspace of a covered facility, and we have a whole bunch of criteria about what makes a covered facility.

However, State and local law enforcement will more likely be the first responders to a potential drone threat. In the event that the drone presents an imminent threat, the State and local law enforcement personnel may not have time to wait around for either DHS or the FBI to arrive on the scene to down the drone. Consequently it is possible under the current draft of the legislation for DHS—I guess the question is: Is it possible for DHS or the Justice Department to confer temporarily their authority to a State or local law enforcement officer in order to neutralize an imminent threat?

Ms. CHANG. Thank you, ma'am. This authority is for the Federal Government, and it does provide us the ability to assist our State and local partners. Right now, as the Chairman has pointed out, we do not even have that. We are not able to do anything to counter the threat, but—

Senator HASSAN. I understand that. But what I am interested in, I am a former Governor. I know what these relationships are like, and I know people are stretched, especially at major events. So, what I would ask is: How are we going to practically do this if there is a threat? Suppose there is an imminent threat. The only

people there are State and local law enforcement. What sort of validation, if we decided to have some way that the DOJ or DHS could confer their authority on State or local officials in the right circumstance, what kind of validation would the State and local law enforcement officers be required to provide to DHS or the FBI in order to confer the authority? And should this be something that we think about as a role for fusion centers in connecting DHS personnel with the first responders who have to make really fast decisions in the face of threats like this?

Mr. GLAWE. Senator, thank you for that question. So the fusion centers and the statutory requirement to share intelligence, imminent intelligence and all intelligence, resolves under me as the Under Secretary for Intelligence for DHS.

Senator HASSAN. Yes.

Mr. GLAWE. The requirement that we are going to need to get that information, tactical level, to the first responders and local law enforcement is going to be critical. This bill is a necessary first step to build the process and policies and technology to develop that capability with State and locals. As a former Houston police officer—I started when I was 22—I absolutely understand that local law enforcement is going to be the first line of defense. I run a road race every year in Iowa—I am going to use an example—and myself and my husband, who is an FBI agent, we were there last year. There were 25,000 people in between two buildings in Davenport, Iowa. A wonderful race. And I looked up, and I said, “There are six drones flying above us.” And we said, “I hope they are friendlies,” because we were sitting ducks.

That was a SEAR 4 event. It got a SEAR rating from my fusion center in Iowa, in partnership with the FBI, but it did not raise to the level to have Federal support. That is where we have to have the tactical level intelligence and the countermeasures in place.

What I would say to the Committee as the head of Intelligence for the Department, the sophisticated capability by the terrorist networks and their encrypted communication makes it very difficult to identify those imminent threats. We have to have the capabilities deployed at these events and ready to go if we feel that an adversarial drone is approaching. Thank you, Senator.

Senator HASSAN. Well, thank you, and I would look forward to following up with you on this particular issue.

Under Secretary Glawe, I wanted to move on to another issue. In addition to serving as the Under Secretary for Intelligence and Analysis, do you also concurrently serve as the Counterterrorism Coordinator for the Department of Homeland Security?

Mr. GLAWE. Yes, Senator.

Senator HASSAN. As Counterterrorism Coordinator, are part of your responsibilities to oversee the Department’s efforts to prevent, respond to, and mitigate terrorist threats to the homeland?

Mr. GLAWE. Yes, it is.

Senator HASSAN. The Counterterrorism Coordinator is such a critical position. Can you please outline for us what goals you have accomplished at the Counterterrorism Coordinator over the past year? What will be your goals for the Counterterrorism Coordinator over the next year? And what metrics will you use to measure your effectiveness?

Mr. GLAWE. Thank you for that question. And since my confirmation in August of last year—I have worked as a Special Agent with the FBI, at the Director of National Intelligence (DNI), and as the head of Customs and Border Protection. I was uniquely postured to identify the challenges we have had at the Department. so we have restructured into a counterterrorism mission center approach, bringing all assets—I am head of intelligence for all assets within the Department, Customs and Border Protection, Coast Guard, Immigration and Customs Enforcement (ICE), the Protection Division, as well as mine. Aligning that so we have a common collection posture, so we see the storyboard of the threats as they evolve, as well as increasing my field resources—we had pulled back, and we did not deploy enough resources in the fusion centers, and creating a new structure so we get tactical level terrorism information to the common users, especially at the ports of entry (POEs) and the borders.

Senator HASSAN. So I appreciate that. What I will follow up with you on the record about is that is a lot of activity to get yourselves ready to accomplish certain goals, and I am interested in what goals were set, what has been accomplished, so what the outcomes are, and what metrics you are using. I have one more question, so I am going to move on to that, but that is what I would like to follow up with you about.

Mr. GLAWE. Senator, we will take that back for the record. I would look forward to come back and have a further dialogue regarding our restructuring and how we have put pursuit teams and metrics associated with that.

Senator HASSAN. All right. Thank you.

Another question for you, Under Secretary. Clearly, from our classified briefing yesterday and today's discussion, we know that drones can be used by terrorists to carry out attacks. With that said, it is really important to make sure that we are not confusing the symptoms with the disease. A terrorist with a drone in the United States is clearly a threat. But so are terrorists armed with a car, a bomb, a gun, a pressure cooker, or box cutters. Indeed, any motivated terrorist with a weapon on U.S. soil constitutes a threat to the homeland.

While we must counter the tactics terrorists use to carry out attacks against Americans, it is perhaps even more important to try to stop terrorists from entering the United States and to keep Americans from falling prey to the twisted propaganda that radicalizes them into homegrown terrorists.

On the first point, at one time ISIS had as many as 5,000 recruits from Western countries, including many visa waiver countries. What is your assessment of the number of foreign fighters ISIS was able to recruit from Western countries? And as part of your response, did all of these recruits die on the battlefield? If not, what is DHS' strategy for countering ISIS foreign fighters that may seek to travel back to the United States?

Mr. GLAWE. Senator, thank you for that question, and it is a very diverse and fluid threat right now as the disbursement of the fighters are now leaving Iraq and Syria and going global. We have seen an amount of European foreign fighters and U.S. foreign fighters that are still in Iraq and Syria. There has been disbursement into

North Africa, into Southeast Asia, as well as Europe, as I mentioned.

We have a new U.N. Resolution, 2396, that requires the sharing of Passenger name record (PNR) data to the United States and to European countries and others that signed on. We are developing programs through enhanced screening and vetting in the National Vetting Center to identify those threats and to work with our foreign partners to get that travel data, especially foreign to foreign travel. But developing the systems and the infrastructure to identify that threat globally to prevent that coming into the United States is a priority for the Secretary and for myself, as well as the intelligence community (IC), as well as also the cargo and container security. As we know with the Australia bomb plot, a significant danger, and we have seen that consistently, the threats to aviation continue to morph and expand exponentially, and they are sophisticated. We are developing the programs and infrastructure globally with foreign partners to collect that data and to mitigate the threats.

Senator HASSAN. Well, thank you. And I know we have gone quite a bit over, so I thank the Chair for his indulgence. I also will be following up on the homegrown piece of this and what we are doing at a community level to make sure that we are countering homegrown terrorism.

Thank you.

Mr. GLAWE. Thank you, Senator.

Chairman JOHNSON. Senator Hassan, first of all, I appreciate your questions, particularly when you started talking about local enforcement of this. Again, for purposes of this hearing, I really need to clarify how little authority government at all levels has on this. So the fact of the matter is when I saw the first draft of this bill, I thought, Is this all? Is this really all we are doing? And I pushed my staff and I pushed the Federal partners here to let us make this as expansive as at least the discussion.

Now, in the end we pretty well pared it back to just the initial first step because, again, we are going to have pushback on this. But I think the answer to your question is local authorities would have no authority. Unless DHS or a Federal authority could get there, there is no authority to knock these things down.

Senator HASSAN. And, Mr. Chair, I understand that and I appreciate very much why we are looking at this. What I want people to remember is that just because we give a Federal agency authority does not mean that operationally that is going to result in the kind of action we need to actually take something down. And, I also know from my local and State folks how concerned they are that they may be presented with an imminent threat that they will take action on because they are public safety officers and they are going to protect the people they are sworn to serve. But then what follows is a level of liability for them which is very concerning.

Chairman JOHNSON. Under Title 18.

Senator HASSAN. Yes.

Chairman JOHNSON. Precisely. So, again, I cannot overstate the fact that this is such an important first step, but it is just a minimal first step. It is just minimal. I mean, this is not going to solve

the problem. This puts us on the path to begin to address the problem. So, again, I appreciate your questions. It helped clarify that.

Ms. Stubblefield, I want to go back to registrations versus the number of drones that have actually been purchased. It is all well and good that FAA requires registration, but it does not require registration at the point of purchase. And so any kind of bad actor can purchase a drone and decide not to register it, correct?

Ms. STUBBLEFIELD. That is correct, sir. The regulatory structure and the registration process is made for the compliant, those who want to follow the rules. Certainly we have looked at the point of sale option when we were setting up the registration process initially, and I would like to take you back to that timeframe when we were doing this because I think it helps inform the option and the direction that we took at that time, which was in the middle of 2015; we were facing a projection of significantly high percentage of UAS being under the Christmas trees of folks in the United States, and we were very concerned that we would have a lot of people operating in the airspace who had no understanding of how to do that safely.

So we pulled together an aviation rulemaking committee that was comprised of industry folks, as well as government stakeholders, to look at what is the way that we can most expeditiously register this new group of UAS operators that will be coming into the airspace system. Point of sale was looked at in that context. The concern with that was when people purchase it, it does not necessarily mean they will be the person operating it, and a lot of these were being given as gifts so there was some concern about whether we would actually be capturing the right group of folks.

There is also the concern about people who are ordering them from overseas or are buying them off retail market and how we would capture those folks. And then as we spoke to retailers, they were very concerned about the congestion of having to do that registration at point of sale. There was quite a bit of infrastructure that would need to be built and clearly articulated within the rule, all of which added up to adding significant time to being able to put registration in process.

Chairman JOHNSON. OK. I understand the complexity of it, and, again, particularly for those small toy drones, if you can consider any of them toys, in terms of threat potential. I understand that. But when you start getting into these agriculture use drones and we still do not require registration at the point of purchase, I heard Senator McCaskill say 4 million drones. I heard you say we have registered a million of them. That is a gap of 3 million. That is a significant security risk from my standpoint.

So we can have all the registration rules in place, but we know bad actors are not going to be following the rules. So I do not get a great deal of comfort in terms of registration rules. I will stop right there. Did you want to go before we—

Senator MCCASKILL. Sure.

Chairman JOHNSON. OK.

Senator MCCASKILL. I would like to spend a little bit of time talking about counter-drone technology. I know that Science and Technology (S&T) has been focusing on developing and delivering some counter-drone capability for DHS. Keeping in mind that this

is not a classified setting, discuss what you can about what its capabilities are, and whether the bill gives you the authority to use what is being developed within DHS for counter-drone operations?

Mr. GLAWE. Senator, thank you for the question. The counter-drug technology developments specifically on how we are identifying the different threat vectors. Transnational criminal organizations are incredibly sophisticated, operating much like foreign intelligence services by State-sponsored governments. They are incredibly capable. Specifically, Science and Technology and the two main organizations that do interdictions, Coast Guard and U.S. Customs and Border Protection, have been increasing their capabilities to specifically identify fentanyl. As you know, it is a tremendous threat, and it is causing devastating effects to all of the Senators' communities. It is devastating. With that regard, they have made advances on how to detect that within cargos and containers, and Kevin McAleenan, the Commissioner, has done a fantastic job in leading that effort.

With regard to this legislation and the threat from UASs, specifically Southern and Northern Border, it gives us the opportunity in the Department of Homeland Security to develop tactical techniques and policies and procedures to identify those threats in a foreign country that are trying to come inbound in the United States. It gives us the first start to do that. But as you know, unmanned aerial systems can provide 3 to 5 pounds of payload of pure fentanyl, which is worth thousands and thousands of dollars and can devastate States. It is deadly. This is going to allow us to develop the policies and technology to further that aggressively, because, in my opinion, these sophisticated networks are going to morph and have way outpaced our capabilities on the technology.

Senator MCCASKILL. You may have misunderstood my question. I am obviously always interested in what we are doing to get after the drugs, but I am interested in what we are doing internally versus the commercial counter-UAS technologies. We are aware that some of these companies are touting some pretty amazing technological advances and claim to be able to address the drone threat. And so I have two parts to this question. I want to know what capabilities exist, within S&T through this Theater Air Control Training Information Computer (TACTIC) assessment that you all have done—and that is an acronym for something long; somebody had to write an acronym—versus the commercial technologies available. One of the big things that has occurred, I am very grateful for, in DOD over the last few years is them finally recognizing that sometimes off-the-shelf technology is a much better deal for taxpayers and, frankly, allows us to stay cutting-edge in a more flexible way than investing in a huge, big project to do counter-drone technology that is with request for proposal (RFPs) and changing requirements. So, first I want you to compare and contrast commercially available counter-drone technologies with what is going on within DHS in the Division of S&T. Second, whether or not any of these technologies are ready to be deployed and whether they can be deployed in urban settings.

Mr. GLAWE. So, Senator, I think regarding the surveillance vehicles, I am assuming you were talking about, as far as what would be flown by the Office of Air and Marine and how they patrol spe-

cifically the border environment to look for nefarious activity, that has been an evolving technology that they have looked to advance. Specifically on the commercial use and where they are looking at the testing and procurement, I would have to get back with an answer for the record on the specifics. I want to make sure I am accurate when we answer your question because this is a very costly endeavor and the technology advancements and the cost saving obviously have to be balanced with what—

Senator MCCASKILL. Yes, and that is what I really want to drill down on here. I really need you to get back to me on why we are not buying it off the shelf. What is the reason? If these technologies have been developed and are commercially available, there needs to be a really good excuse why we are not availing ourselves of that technology as opposed to trying to duplicate it in a way that history has told over and over and over again costs three times as much. It does not happen as quickly, there are too many cooks in the kitchen, and we are just not as nimble and flexible as we need to be. And in this particular area, with technologies evolving as quickly as they are, I just want to make sure that we are not missing the opportunity to avail ourselves to the commercial technologies that are available.

Mr. GLAWE. Senator, we will take that back for an answer.

Senator MCCASKILL. Great.

And I really want to know also, when you come back with that, how these technologies can be deployed in urban environments. There is one situation where you can go into a relatively rural area and do the kind of identification, interdiction, and use counter-drone technologies very effectively. Sometimes in an urban setting, it is a whole different set of challenges, both from the flyable space to the interference that there is in terms of the ability to locate them, and obviously the techniques for bringing down are challenged by an urban environment. So I think it is really important that this Committee get a handle on what advancements are being made—and all of you, feel free to weigh in on this, what advancements are being made that would allow us to use these technologies more effectively where it is likely this is going to occur; that is, where bad actors could hope to inflict mass casualty.

Mr. GLAWE. Senator, using UASs for law enforcement purposes to conduct surveillance on criminal suspects, terrorists, foreign intelligence agents is going to be an absolute benefit and how we develop those policies and procedures, I would actually turn it over to the FBI, the Deputy Assistant Director, maybe to touch on that from their use.

Mr. BRUNNER. Yes, Senator, I can speak from experience. I have been in a number of meetings with the Department of Defense, a number of conferences, and with our partners in the industry. There are a significant number of counter-products out there on the market today. The problem we face right now is that we cannot legally use any of those domestically. That is where this legislation comes into play. So the Department of Defense is using some very significant tools overseas. Our partners here within the counter-market are developing some significant technologies that are potentially very useful to us to protect the American public and to re-

spect privacy and civil liberties. But, again, we cannot use any of those right now.

Senator McCASKILL. And our legislation would allow that?

Mr. BRUNNER. Yes, ma'am. It would go a long way in helping us.

Senator McCASKILL. Well, then I want to get a head start on looking at commercially available, off-the-shelf technologies so that we are not back here 5 years from now talking about the 400 million, the 500 million, the billion that was wasted in an acquisition strategy that was never going to be nimble enough to address the threat.

Thank you, Mr. Chairman.

Chairman JOHNSON. Senator Heitkamp.

#### OPENING STATEMENT OF SENATOR HEITKAMP

Senator HEITKAMP. Thank you, Mr. Chairman. And thank you so much for expediting this hearing. I think it is critical, as we talked yesterday, that we have this conversation.

First off, I would just like to acknowledge that North Dakota is very proud of the role that we play in developing technology, and continuing, Senator Hoeven and I brag about this all the time, and you can see our names are prominently featured on this bill because we want this technology to be safe. And so we have great opportunities to expand and to develop what we need for border security, for homeland security, right in North Dakota and right here. And so I just want to submit for the record a statement by Nicholas Flom, who is the executive director of the Northern Plains Unmanned Aircraft Test Site System.<sup>1</sup> Nick is a great leader on UAS, both in North Dakota and the Nation, and he and the North Dakota Test Site I think bring an important perspective on counter-UAS and how to best pursue this initiative. And so—

Chairman JOHNSON. Without objection.

Senator HEITKAMP. Thank you, Mr. Chairman.

First off, it is always dangerous when you are reaching back in the file banks of your memory, but there were companies that developed these techniques overseas for the Department of Defense that came back, and there is a great example in Baltimore where a local agency deployed the same techniques and the same equipment that was used internationally. I do not know. Are you familiar with the Baltimore experience, any of you?

[No response.]

Well, that is a problem, right? Because this is something I know from listening to a podcast, but you guys should know it. And they ran into a number of privacy problems, but I think it was like a Radiolab podcast or maybe a Planet Money podcast, but they talked about tracking the criminal element in the city of Baltimore and using this technique and were able to basically deploy resources almost immediately to conflict points that were very helpful. And it goes to what Claire is talking about, which is, how do we do this, even beyond terrorism threats, even beyond mass casualty threats, these techniques can be very helpful for pursuing safety within communities themselves. And so I would recommend

<sup>1</sup>The statement referenced by Senator Heitkamp appears in the Appendix on page 75.

you guys all get a hold of Baltimore—if it is not Baltimore—I remember it is Baltimore, but get a hold of the other entities.

Mr. BRUNNER. Yes, Senator, we are aware of that. That is a persistent surveillance component. It is slightly different from the counter component that I was—

Senator HEITKAMP. Right, but there is no reason why a persistent could not actually catch a counter-terrorism threat as well, right?

Mr. BRUNNER. I am not—

Senator HEITKAMP. Given the right intel.

Mr. BRUNNER. Potentially, yes.

Senator HEITKAMP. So I think that there is a great example of a public safety utilization of this technology.

I want to continue the dialogue that Claire engaged you all in, in terms of technology. I think that we feel sometimes that we are always behind the eight ball; we are always trying to catch up to what the bad guys are doing or catch up to what is happening and understand the technology. How can we accelerate the development of this technology, especially as it relates to surveillance kind of moving forward? And what are you doing to accelerate the development of this technology or evaluating products, as Claire has talked about, off the shelf that are already available? I would start with you, Mr. Glawe.

Mr. GLAWE. Senator, thank you for the question. I think this legislation allows us the first step to start developing the lanes and the roads of what our authorities will be and how we can deploy it within the homeland. That is going to be unique from a law enforcement and how we use it and how we use that policy and legal framework so when we have officers deployed at the border or at a national security event, that we have the parameters of what we can do and how we can deploy countermeasures. I will turn it over to the Deputy Assistant Director of the FBI, who is really the subject matter expert on this and leads that component down at CIRG, for a little more granularity on it.

Senator HEITKAMP. Mr. Brunner.

Mr. BRUNNER. Yes, Senator, we are working extensively with our private industry partners to evaluate what the market has out there in technology, and we are actually preparing ourselves for when the national airspace opens up, and I could turn that over to Ms. Stubblefield in a moment about that. But we want to be in a position to make the best use of this technology as possible, so we are coordinating with our private entity partners both on the operational surveillance side of the house and on the counter-surveillance side of the house, counter-UAS side of the house, in order to position ourselves and to provide the industry with what we potentially believe we might need to both surveil and counter.

Senator HEITKAMP. One of the things that I would remind you is that this is the Homeland Security Committee but also Government Affairs, and we are charged with efficiencies, we are charged with making sure that we are doing everything that we can to make sure that we are not wasting taxpayer dollars, that we are not re-creating the wheel when the wheel has already been made available. And so I just want to reiterate Claire's point, which is, let us not think that the public fisc is open to every dollar that you

think you may need. Let us try and economize on this. Mr. Brunner.

Mr. BRUNNER. Yes, ma'am, there is a National Capital Region group that gets together on the Federal level—it is chaired primarily by DHS and DOD—that the Department of Justice is now a partner to looking at exactly that. We all believe in this technology. We all know that we are going to need certain components of this technology. Let us be smart about it. Let us do it together. Let us push all of our requirements out at one time so that we do not waste the taxpayers' money.

Senator HEITKAMP. Turning to Mr. Glawe, we are obviously very interested in providing border security on this Committee. I think that we now have gone through a Northern Border study, we have gone through a Southern Border study. How engaged and involved are these technologies in the evaluation of that? We talk about a wall, but we can do a virtual wall if we do this correctly. And so we are very interested in how these technologies will be deployed at the border and whether you believe that you are paying enough attention to the development of these technologies as we look at border security strategies.

Mr. GLAWE. Senator, thank you for the question. I had the good fortune, when I was the head of Intelligence at U.S. Customs and Border Protection, to actually help stand up the Northern Border Coordination Center in Detroit and actually brief you—I believe it was about 3 years ago.

Senator HEITKAMP. I know.

Mr. GLAWE. I am very familiar with the unique environment of collection on the border using unmanned aerial vehicles, and we have done a tremendous amount of testing on the Northern Border. You are very familiar with the challenges with the foliage compared to the Southern Border. We have partnered with the Department of Defense and intelligence looking at capabilities and what we can deploy in an unclassified and classified meeting to look at the coherent change of where those threats are. So if you are unlawfully entering and not going through a port of entry and declaring it, you are essentially illegally entering the United States.

How are we deploying assets on that target to identify what that threat is? That is a layered approach with intelligence, not just air assets but intelligence also in the rear law enforcement and in U.S. intelligence community assets and how we collect that. We are creating new systems in how to do that. This legislation, which also involves a strong research and development (R&D) and reporting requirements to you, will allow us to show you that layered approach and how we are integrating in that intelligence from a classified and unclassified capability on the patrol aspect of it.

Senator HEITKAMP. And I think highlighting, Mr. Chairman, the importance of getting this legislation across the finish line so we can get started. Thank you so much.

Chairman JOHNSON. Thank you. Senator Carper.

#### **OPENING STATEMENT OF SENATOR CARPER**

Senator CARPER. About a Saturday ago, colleagues, I was at the University of Delaware in the football stadium for graduation, and Scott Brunner's name came to mind because if you do a Google

search on Scott Brunner, you will find he is not just a top guy at the FBI. He was our starting quarterback for 3 years.

Senator HOEVEN. Did you graduate?

Senator CARPER. He went on to play for the Giants and for the Broncos.

Senator HOEVEN. Governor, did you graduate?

Senator CARPER. Several times. [Laughter.]

Yes, indeed.

Senator HEITKAMP. Really?

Mr. BRUNNER. No, ma'am. That is not me. It is a different— [Laughter.]

Senator CARPER. But I thought about you when I was there and today. So nice to see you all.

I am going to ask you to think about one question, and then I will ask another one while you think about the one I am going to ask in a minute. The one I am going to ask in a minute is: Each of you, give us a question we ought to be asking that we are not asking yet of you. All right? What should we be asking that so far we have not asked? OK? Think about that.

Here is my question. Given the disparate roles and the responsibilities spread across a bunch of different agencies, I would just like to know what your thoughts are about the degree of coordination and cooperation that are necessary for successful counter-UAS operations. That would be my first question, so let us just start with that. Ms. Stubblefield, do you want to go first?

Ms. STUBBLEFIELD. Thank you, Senator. Both your questions are excellent questions, but I will start with the second one first.

The level of coordination is significant, and we certainly appreciate that this Committee's proposal highlights the need for robust coordination and a risk-based assessment. There are a lot of counter-UAS systems out there, 235 systems available from 155 vendors in 20 countries. There is a plethora of options on the market.

Senator CARPER. I am going to ask you to be succinct because we are—

Ms. STUBBLEFIELD. Yes, sir.

Senator CARPER. Thank you.

Ms. STUBBLEFIELD. However, they have not been tested in the civil environment. Most of them are built on military applications. Therefore, as we are implementing them in the civil environment, as we have been doing with the Department of Defense and Department of Energy, it is critical that we have coordinated processes for notification and reporting for the airspace flight restrictions and mechanisms necessary to ensure we are using this in locations where compliant operators are not operating, to include the spectrum analysis for the impacts that they have on avionics and air navigation systems that are critical to safety of flight. So that coordination, which we have been in lockstep with DOD and DOE, is paramount in the planning up to deployment, through deployment so that we can determine what those impacts are and what mitigations may need to be put in place, and then also post-deployment to understand how the UAS that they are engaging are reacting, because the different UAS platforms actually react differently to different kinds of counter-UAS technology.

Senator CARPER. Great. Thanks.

Same question, Mr. Brunner.

Mr. BRUNNER. Thank you, Senator.

Senator CARPER. And be succinct and brief, please.

Mr. BRUNNER. Yes, sir. Cooperation is imperative in this. I think this group that we have gotten together to work on this legislation with you all exemplifies that, that we recognize the necessity to work together and to cooperate. Yes, we do have our own lanes and our mission sets to protect the American people and to protect their civil liberties and their privacy. But we also need to come together, and we do as this legislation represents in a number of areas where we work together. And that is not just for this Committee. It is the FAA, it is the Federal Communication Commission (FCC), it is the National Telecommunications and Information Administration (NTIA), and then it is all of our State and local partners on top of that. It is imperative that—we cannot do this alone. It is a group effort.

Senator CARPER. All right. Thanks.

Same question, Ms. Chang.

Ms. CHANG. Thank you, Senator. The coordination is extremely robust. I think my partner Ms. Stubblefield said it best when we first started our efforts together, that we should consider this a marriage not a date, and I can say from experience I think I see—

Senator CARPER. Do you say that?

Ms. STUBBLEFIELD. Every day.

Senator CARPER. That is good. I have to use that. [Laughter.]

Ms. CHANG. The statute requires us to coordinate with the Department of Transportation, with the Department of Justice, not only in implementing and doing the risk-based assessment and designating facilities, but also any implementation and guidance that we would issue. And I just wanted to also emphasize that the reason that coordination is so key, we need this bill because right now our research and development is illegal. We cannot even research this technology because it is illegal, and, therefore, we are going to have to build on our counterparts at DOD and build on their efforts in order to hit the ground running if and when we get this authority.

Senator CARPER. Thanks, Ms. Chang. Mr. Glawe.

Mr. GLAWE. Senator, thank you for that question. I would just echo my colleagues. The research and development, the efficient aspect of developing that within the policies and procedures that this legislation allows us to is critical. But I would also foot stomp that we have to move with a sense of urgency. This threat is upon us. It is already here.

Senator CARPER. We have never had a witness' foot stomp before.

Mr. GLAWE. We have to move with a sense of urgency on this, and it has to be developed quickly within the framework of the legislation and reporting requirements back to you all. And then on your follow up question, I will just say quickly—and I think this is going to echo Senator McCaskill's concerns, as well as others—have we gone far enough to allow information and countermeasures to be shared with our State, local, and private sector partners? I am worried about those large venue baseball games,

football games, running events which I attend that do not raise to the level of Federal law enforcement, a SEAR event, and the protections that come with it. So I think in partnership as we move forward, as this first step, do we have the authorities in place as we move out, as the policies and procedures and tactical techniques are built around it.

Senator CARPER. Good. Thank you.

Ms. Chang, what question should we be asking that has not been asked?

Ms. CHANG. Why do we need the broad categorical exemption from Title 18 versus carving out individual sections from the code?

Senator CARPER. OK. Thank you. Mr. Brunner.

Mr. BRUNNER. Senator, my question would be: What are the consequences if we do not take this first step?

Senator CARPER. Ms. Stubblefield.

Ms. STUBBLEFIELD. Why is it that the phased approach is really the most appropriate approach to ensuring that we do not create a safety issue while we are trying to solve a security problem?

Senator CARPER. OK, good. I am going to be asking this question for the record. I do not expect you to respond to it, but the question I will ask for the record goes back to my first question, and that would be: What can we do here in this body, the Legislative Branch, to improve and beyond this branch, working with you, what can we do to improve coordination of counter-UAS activities across Federal agencies? I will ask that for the record.

I have 6 seconds left, but the Chairman is not here. So I will probably ask this one for the record as well.

Senator MCCASKILL [presiding]. You think I am a pushover, don't you? [Laughter.]

Senator CARPER. No one would ever suggest that, least of all me.

I will ask this one for the record as well. Members of the Committee have talked about this legislation being limited in scope regarding authorities being granted. I am going to ask you to share for the record, each of you, your thoughts about potential next steps and what is needed as we move forward.

We thank you for being here today and thank you for your service, and we welcome your presence today, both on and off the grid-iron. Thanks.

Senator MCCASKILL. Senator Hoeven.

#### **OPENING STATEMENT OF SENATOR HOEVEN**

Senator HOEVEN. Thank you, Ranking Member.

To begin with, I want to highlight for the Members of the Committee that the Director of the Northern Plains UAS Test Site, our test site located in Grand Forks, North Dakota, the Director, Nick Flom, submitted a short written statement for the record for this hearing, and he talks about some of the technical challenges and priorities related to development of counter-UAS and strategies, and I would strongly encourage you to read that testimony.

For Ms. Chang, you mentioned in your written statement that Federal law complicates your ability to research, develop, and test counter-UAS technologies. Can you describe the challenges you face in developing and testing counter-UAS technologies and provide examples of technology that would help you counter UAS threats that

you are not currently permitted to test and evaluate? So things that you cannot do that you would like to be able to do.

Ms. CHANG. Thank you, Senator. There are several things that we would like to be able to do that we cannot do currently, and the technology is constantly evolving. But our efforts right now, for example, to detect drones that could pose a threat primarily rely on scanning the radio frequency (RF) spectrum. That raises questions under the Wiretap Act and the Pen/Trap Act for use as well as spending any money on research or testing, because its use is illegal, so testing it and acquiring it is illegal.

The same with any of the disruptive measures that we would use, particularly jamming, raises questions not only under those statutes, but also the Computer Fraud and Abuse Act, potentially the Aircraft Sabotage Act, several others that have been interpreted in new ways because of the development of technology. And because the technology use is illegal, we are not permitted under our rules to spend money to purchase equipment that is illegal to use, and so we cannot test it.

Senator HOEVEN. So you cannot test jamming?

Ms. CHANG. I should say I am aware of only in like a sterile environment we are allowed to test, but we are not allowed to test where there could be any secondary consequences, which is not very realistic if you plan to use it, for example, in Manhattan.

Senator HOEVEN. Well, of course. It is clearly something we have to test and clearly something we have to figure out how we can develop testing for, because, obviously, we are going to need it.

Ms. CHANG. Yes, sir.

Senator HOEVEN. So that is a very good point, a very strong point. Thank you.

Mr. Glawe, your written statement illustrates that we are becoming aware of more and more cases where UASs are being used for illegal purposes. As the commercial UAS industry grows, what additional legal authorities or technical capabilities do you need to track UAS air traffic and separate potential threats from friendlies? How would you benefit from requirements for UAS to identify itself or from the establishment of unmanned traffic management (UTM), networks that might highlight cooperative and noncooperative aircraft?

Mr. GLAWE. Senator, from an investigative standpoint, if you are working a national security investigation or a criminal investigation, the legislation is critical to allow us the procedures and policies and technical capability for identification of those nefarious. This is going to have to be a layered approach with our investigative capabilities which currently exist in—our intelligence capabilities that currently exist. It will be layered into the statutory authorities on how we identify and disrupt threats. But due to the nature of the evolving and the quickness of these threats, this legislation is critically important for us to develop the technical capabilities, as the Deputy General Counsel just mentioned, in that environment of what we can do within the authorities that you all will grant us if this legislation goes forward, which we feel it must.

Senator HOEVEN. So you think this will help get you where you need to go in terms of—I mean, we are going to have to have a system where you have sense and avoid and, UTM that allows not

only the sense and avoid but some ability to make sure that we are detecting the threats.

Mr. GLAWE. Senator, absolutely. As Chairman Johnson stated in his opening remarks, this is a strong first step to allow us the policies and procedures to layer it in with those investigative authorities our law enforcement organizations have, and if it is outside the United States, layered in with the intelligence services and foreign partners of how we are going to mitigate this threat. The threat is very broad, permissive, and significant.

Senator HOEVEN. Ms. Stubblefield, I am pleased to note from your written statement that the FAA is prioritizing ways to both remotely identify UAS aircraft and also development of the UTM system.

Ms. STUBBLEFIELD. Yes.

Senator HOEVEN. So both the systems and the technology, again, that will sort out friendlies and threats. But you are focused on the airspace 400 feet and below, it looks like, so my question is: What about 400 feet and above? Are you looking at that as well for any criminal or terrorist type—any kind of threat activity?

Ms. STUBBLEFIELD. Thank you, Senator Hoeven, for highlighting the remote identification requirement. From the FAA's perspective, we would like to see that requirement for all UAS. As we consider putting together the rulemaking, which we are working on as aggressively as we can right now, we are certainly looking at putting requirements on operators, manufacturers, such that when these come out of the box, there is a capability that is there, which is going to help regardless of where UAS operate, whether it is 400 feet or below or as we move into the middle or even high altitudes. Those UAS that can function at, let us just say to segment it, 18,000 feet and above, so in Class A airspace, those are going to be larger aircraft that will be certified. We will have requirements in that airspace to be communicating with air traffic control.

There is no doubt that we have challenges around the detection of what are generally a low and slow radar cross-section of UAS. However, those larger UAS, we certainly have a much better capability in terms of detection as we stay down into the lower altitudes and, again, not to provide too much information about our security posture, but certainly we think remote identification is going to be key because those who are not cooperating in the environment that will hopefully, as our partners derive the authority to be able to deploy detection, they will stick out, and so we will know who is supposed to be there part of, as you mentioned, the unmanned traffic management, the suite of tools and capabilities that will go with that, we will know who is authorized to be there, who should be operating and is operating compliantly, and those who are outside of that hopefully will be detected by the systems that our partner security agencies will be able to field.

Senator HOEVEN. I am out of time, but, again, I would ask that all the witnesses please take a look at Nick Flom's testimony. I think it is helpful in your endeavors.

Thank you.

Chairman JOHNSON. Thank you, Senator Hoeven.

Ms. Chang, can you describe the inhibitions of Title 18 to non-lawyers? I am one of them. Just talk about why law enforcement is going to be really constrained unless they get this type of waiver.

Ms. CHANG. Certainly, Senator. The primary concern is technology is evolving so rapidly, as you pointed out, and the law is just not keeping up right now. And so we had discussed the detection measures that we try to use, which most of them operate by scanning the RF spectrum. That is naturally going to raise questions under the Wiretap Act that was written in the 1960s, the Pen/Trap Act from the 1980s. They just were not initially written for this, and so what is considered an electronic communication is arguably swept up here, but also our other measures, any effort that we would take to safely bring that device down could potentially raise questions under a whole host of statutes. And it is changing every day. We would not have originally thought that these UASs would be considered—what used to be just model airplanes would be considered aircraft under the Aircraft Sabotage Act and, therefore, bringing it down if it causes damage could create criminal liability for our officers. We would not have believed even recently, until recently, that these would be guided by satellites, implicating provisions about interfering with satellites. And the problem is just changing every day.

And so I cannot say with confidence today how many of these statutes could be implicated as this technology continues to evolve.

Chairman JOHNSON. I think we are all concerned about civil liberties. There is no doubt about that. But, for example, every day law enforcement might be confronted with having to disarm a criminal, correct? They do not need a warrant to take away somebody's gun at that point in time. Why is this that much different? I will go to you, Mr. Brunner.

Mr. BRUNNER. Well, Senator, from a non-lawyer perspective—

Chairman JOHNSON. We will switch over to Ms. Chang afterwards, but somebody with boots on the ground.

Mr. BRUNNER. So the concern for the boots on the ground, Senator, is the way that the Title 18 statute is written right now and some of the other statutes. We are concerned that the individual, the agents on the ground, the officers, however you want to phrase it, would be liable by taking action against these targets, which no one has authority to do right now. So if they were to take action, there is the potential there that the Department of Justice or State or local authorities could bring—

Chairman JOHNSON. I understand, but the analogy really is you have a potential threat now is a drone. You have intelligence, actionable intelligence. You realize this is a problem. First of all, it is temporary restricted airspace. Nobody should be flying a drone. Practically, putting the law aside, is there really a difference between law enforcement disarming somebody without a search warrant or going through any kind of court procedure versus law enforcement acting in that capacity?

Mr. BRUNNER. The difference is on the capabilities that the law enforcement officer or special agent has on hand to mitigate that threat. So downing an aircraft by an agent on the street or a police officer on the street is going to be extremely difficult. So that is the hardest challenge right now. If I am an officer or an agent on the

street and I see a threat, I am going to do whatever I can to mitigate that threat, regardless of what the statute might say at that time, if I feel like I am protecting others. But the issue really for them is they do not have the capabilities nor do we right now without this legislation to actually do that.

Chairman JOHNSON. So, again, I understand the capability. Again, I am just trying to connect the dots in terms of an analogy. We ought to give law enforcement the capability, just as they have the capability of disarming somebody dangerous, without going through a court procedure and getting a warrant, they ought to have that same authority from my standpoint.

Ms. Chang, do you want to comment on this?

Ms. CHANG. Yes, Senator, and I am glad you raised the Fourth Amendment because the Fourth Amendment still applies, and this statute does not change that. And so if, for example, a police officer were breaking up a fight, they would be under the Fourth Amendment. They would be using force. And it would have to be reasonable under the Fourth Amendment. They would be seizing potentially persons or property, and that would have to meet the reasonableness standard under the circumstances.

This statute actually sets a higher bar in that not only would we have to comply with the Fourth Amendment, but also take actions only as necessary to mitigate the threat. And once that threat is over, then our authority under this statute would end. And, again, the normal rules would still apply.

Chairman JOHNSON. Some of the pushback we have gotten from some of the other committees of jurisdiction has to do with the risk-based assessment that is required under the statute. We have left that basically to the agencies to determine what that risk-based assessment would be. I think some of the other committees might be looking for greater detail and more prescriptive language in terms of what that risk assessment is. Can you just address that issue?

Ms. CHANG. Certainly. The reason that we believe that this sets the appropriate balance, there are a number of constraints in the statute governing how we have to coordinate and oversight. But we believe that keeping a somewhat flexible approach because of the developing threat is important. We will be, of course, coordinating with our FAA partners, and every step we take will be with them. But the threat is evolving so quickly that if we are so carefully constrained in statute, we have been asked, for example, if we should define "threat" in the statute. I am only aware of one statute that does that. That is the Cybersecurity Information Sharing Act (CISA) that defines "cybersecurity threat," but typically that is left to the operators because we have the expertise, and like I said, it is developing so fast. We do not want to have to be back here asking Congress for a new law 6 months from now.

Chairman JOHNSON. Which kind of gets me, again, to the very limited nature of this, because I think it is important to pound this point home. This is limited to risk related to the following missions: U.S. Coast Guard and U.S. Border Patrol in terms of their security operations, including security of facilities, aircraft, and vessels; to U.S. Secret Service protection operations; to Federal Protective Services (FPS) protection of DHS facilities; to U.S. Marshals and

DOJ protection of its facilities and court personnel; to the Bureau of Prisons, protection of their high-risk facilities; then security for special events, and there we are talking about visits by the Pope or other special events that are going to be assessed through this risk-based assessment; and then when a State Governor or an Attorney General requests assistance. But, again, the local authorities will have no authority whatsoever to mitigate the threat. Then active Federal law enforcement investigations, emergency responses, security operations carried out by DHS and DOJ, and then just reacting to known national security threats that could involve unlawful use of drones. Again, this is a really narrow authorization.

Who would like to talk—again, to reinforce and clarify, this is just a first step. Maybe, Ms. Stubblefield, you can talk about the first-step nature of the authority given to the Department of Defense, because in our briefing yesterday, it really does sound like those agencies, you are working very closely with them, working through the complexity of this, understanding how difficult this is, but also we are just taking the first steps down that path, even with DOD having this authorization for, what, 2 years? So can you just talk about that?

Ms. STUBBLEFIELD. Yes, sir, Mr. Chairman, and thank you. The complexity, as you cited, of this type of situation is you are taking technologies that have largely been used in conflict zones and the military space and bringing them into the civil environment. And because there have been so few agencies that have the authority that DHS and DOJ are seeking here, it has been extremely challenging for anyone, whether it is Federal, State, or local, to do that testing in the civil airspace, because the technologies that we have, by and large, do have impacts on avionics and air navigation service systems. And so we have been working very closely with DOD in the pre-deployment phase. Part of that risk assessment is determined. What is the airspace around that facility? What does the air traffic look like? What is the appropriate technology? What exactly in that space are you trying to protect? Is it a point defense? Is it an area defense? All of those types of factors go into determining how we appropriately scope any flight restrictions, what the concept of operations (CONOPS) is for the given agency to deploy that system, so that we can then mitigate any of the spillover effects into the civil environment.

As Mr. Brunner articulated earlier, the FCC and NTIA are also involved in that, because those impacts can go beyond just the aviation spectrum.

Chairman JOHNSON. So this has been so far about a 2-year process.

Ms. STUBBLEFIELD. Yes, sir.

Chairman JOHNSON. And you are not at the endpoint, not by a long stretch, right?

Ms. STUBBLEFIELD. As you said, sir, this is an incremental phased approach. As the Department of Defense and the Department of Energy understand what these technologies look like to be deployed by their folks on the ground in the civil environment, they are taking a very measured approach to that as well, because they are also using facilities that have their own constraints, whether

they be a facility that has nuclear weapons or other types of technologies and sensitive materials that may react to the types of technologies they are looking to use to counter. All of those things have to be weighed out, so it is a very slow, methodical approach to ensure that when they get to turning them on operationally, we have done all we can to ensure we are not creating any safety impacts but are, in fact, just focusing on taking down that security risk.

Chairman JOHNSON. And, again, to clarify and respond to the letter I received from the ACLU, DOD only has authority around a very limited number of its facilities, correct?

Ms. STUBBLEFIELD. That is correct, Senator.

Chairman JOHNSON. They have no authority tacked against all the things I just detailed in terms of our bill.

Ms. STUBBLEFIELD. That is correct.

Chairman JOHNSON. The Coast Guard, Secret Service, U.S. Marshals, Bureau of Prisons, special events, DOD has no authority whatsoever.

Ms. STUBBLEFIELD. That is correct, sir.

Chairman JOHNSON. I think it is also important to point out that we did draft this law to pretty well make the authority identical to DOD so that different agencies now working in cooperation are not inhibited by slightly different types of authority which could overly complicate this, correct?

Ms. STUBBLEFIELD. Correct, sir. And it is that mirroring of the coordination and the risk assessment in both of those places as well as the other features that for the FAA who is involved with everyone who is going to deploy this makes it for us a more consistent process as well to ensure we are uniformly looking at the impacts on the airspace and aviation safety.

Chairman JOHNSON. In yesterday's briefing, I think a good line of questioning—I think it was Senator Harris who was talking about, OK, if we have a local authority and they hear and perceive a risk, where is the point of contact going to be? And we are talking about a number of different agencies here in the Federal Government that were providing this authority. Does anybody have an opinion on where that point of contact should be?

Mr. GLAWE. Chairman Johnson, I think developing the policies and procedures around the capability is going to be critical. Under a national security event, we currently have the Critical Incident Response Group along in partnership with the DHS operational equities that are very clarified and defined, very defined, as the Deputy Assistant Director from the FBI will say. But when we are talking about protection of critical infrastructure such as a petrochemical plant in Houston or other critical infrastructure that this statute would allow us to do risk assessments and see if there has to be protection, that is where we are going to have to develop other procedures so we get the intelligence to the operator to make that decision to take whatever countermeasures would be appropriate for that, and we are going to have to change the structure of how we do business in this arena, and this legislation is a key step to getting the policies, procedures, and legal authorities wrapped around it so we can make those decisions, because you are absolutely right, the decision to actually action a UAS is going to

be quick, dynamic, and the threat is going to be evolving fast, and we are going to have to be moving into that space very quickly.

Chairman JOHNSON. So it is just too soon in this process to really start ferreting out points of contact, because it could be points of contact based on the industry, based on the location, and eventually filtering back to somebody. But you have to set up that process.

Mr. GLAWE. Chairman Johnson, you are absolutely right. When we are talking about deploying some sort of a force or a technical capability on an object, which the Deputy General Counsel can explain more from the legal standpoint, we are going to have to have very specific guidelines, procedures, in how that is deployed, what authorities of what organizations are there to deploy it—Coast Guard, Border Patrol, Office of Air and Marine, the FBI, the Secret Service if it is at a protectee's location. Defining that scope and spectrum based on the technological capability is going to be a critical component to that.

Chairman JOHNSON. I have only got one more question for Ms. Stubblefield, but I am going to close this out by asking all of you to respond: Is there anything that we have not talked about that, as we are going through this, you have just been itching to make the point and/or something that really needs to be clarified?

But, first, Ms. Stubblefield, I am going back to registration. Again, I think there is a huge gap there. It is, by and large, voluntary. Correct? It might be required by law, but it is not really required by law at the point of purchase. First, correct me if I am wrong there. And, second, what are the penalties if people do not register? And what is the enforcement of it?

Ms. STUBBLEFIELD. Yes, sir, you are correct that we are dependent upon people complying with the rules, to follow the rules and register their aircraft before they operate them. But that goes across all sectors of aviation, not just the unmanned aircraft.

In terms of the penalties, yes, there are penalties, civil penalties for failing to register aircraft, and I believe there actually may be a criminal aspect to that as well. For the FAA's part, responsible for the civil penalty, if we are made aware that someone has operated an aircraft that is not registered, we conduct an investigation and then determine based on the circumstances whether that is appropriate for enforcement and levying of civil penalties, which the FAA has conducted approximately 73 enforcement cases at this point.

Chairman JOHNSON. So 73 out of about 4 million different drones. In yesterday's briefing, we heard of thousands of problems, correct? I mean per year, thousands of suspected improper use of drones?

Ms. STUBBLEFIELD. And precisely to your point, Mr. Chairman, that is why the FAA has focused firmly and quickly on remote identification. That is going to enable us to identify a drone that is operating with the operator or the owner and be able to then follow up for education, for enforcement, for support to our law enforcement colleagues to be able to actually ascertain what was the intention and what, if any, follow up action needs to be taken, be that, like I said, education, enforcement, or criminal prosecution.

Chairman JOHNSON. Again, I am just trying to lay out the reality. This is how many improper uses of drone we detect, over how many years engaged in 73 enforcement actions. So there is a huge gap between what the reality is and what the vulnerability is, and what we really can do from the standpoint of governmental authority to really address that fact.

Let me start with Mr. Glawe then. Again, anything that just has to be said, needs to be clarified here?

Mr. GLAWE. Chairman Johnson, no, I think we have covered all the threat vectors. I would just say again this threat is significant and it is imminent. It is upon us. Terrorist organizations, foreign intelligence organizations, transnational criminal organizations, criminal actors can use this technology and are using this technology on the homeland and abroad. This legislation is a very strong first step to get the ball rolling on the policies, procedures, technical capabilities, and legal authorities to allow law enforcement officers in the United States to take the actions needed to make the homeland safe.

Chairman JOHNSON. Strong but still minimal, correct? I mean, this is not going overboard. This is just giving you baseline capability that you need as that first step.

Mr. GLAWE. It absolutely is. As a former law enforcement officer, I think we are going to need to revisit this as we know the vulnerabilities will change.

Chairman JOHNSON. I think there would probably be a lot more, first, discussion. We need to really discuss the complexity of this issue. Ms. Chang.

Ms. CHANG. Mr. Chairman, the clarification that I would like to make is about the application of the broad categorical exemption for Title 18. We have been asked several times why we cannot just carve out those statutes that I just listed and say we are exempt from those versus the entire criminal code, and there are three primary reasons for that. The first is the certainty that we have discussed. If we do not have certainty, we have no solution at all because our officers right now cannot move forward, and this technology is just evolving so fast. And that is why the Administration strongly prefers the clear approach in this Committee's bill that is from the same approach given to DOD and DOE in the NDAA. And the second is fairness. We have been told repeatedly that DOD is somehow different, and in their warfighting capacity, they are. But for that authority, they did not need this NDAA authority. The NDAA that we have been discussing, that piece gave them authority to operate domestically, force protection under the Fourth Amendment just like our folks. And if our front-line officers in uniform and out of uniform are treated differently and given less protection, that sends a message they are less valuable than their DOD partners.

And the third is, as you point out, Mr. Chairman, the interoperability. There was a news article this morning in Reuters about a 2017 incident, an Army Black Hawk that a drone collided with it, and this happened at an NSSE. This was a National Security Special Event over the U.N. General Assembly. In that instance, if we did not have the same authority and the same legal regime as DOD, we would not have been able to work together and coordinate

like we do on NSSEs in other areas, and so we need to be able to work together as one team.

Chairman JOHNSON. Those were excellent clarifications. Mr. Brunner.

Mr. BRUNNER. Chairman, I want to start by thanking you very much for holding this hearing today. The Department really appreciates the ability to be here in front of you, so thank you for that.

I also want to emphasize our commitment to implementing this authority in an extremely vigorous manner with respect to privacy and civil liberties. I want to make that point for the record.

And then to a question you asked previously, where do we go from here? We are in extensive conversations with our State and local partners about how we can broaden this authority and how we can bring others into the fold. And we talk to the National Football League (NFL) and we talk to Major League Baseball, and we talk to the Commercial Drone Alliance and the American Modelers Association, just to make sure everybody is on board of where we are going, what we are trying to do, and how we can make this better as we progress.

So thank you again very much for the opportunity today.

Chairman JOHNSON. Well, thank you for your service. Ms. Stubblefield.

Ms. STUBBLEFIELD. Again, thank you very much, Chairman, for the opportunity to participate today. As one clarification, I want it to be crystal clear, sir, that the FAA supports our national security partners in DHS and the Department of Justice gaining this authority. There is a lot to be learned about how to properly use it in the national airspace system and in civil environments, and this authority will give us the opportunity to start to move farther down that road and hopefully provide a road map ahead as we phased-approach move this authority forward.

I would like to mention one thing, though, because there is a concern about what are we doing for our State and local colleagues. Remote identification will be very key to them. In our aviation rulemaking committee, we brought in State and local law enforcement, and they said, "We need to be able to find the guy who is operating that drone," because in many of these situations it is impeding emergency response, police activity, or response to an incident on the highway or something of that nature, where time is of the essence to get critical help into that area. And so that is why we are focusing on remote identification.

The one place we have not talked about today—and you talked about gaps that we have—it is the fact that, unfortunately, right now we do not have the authority to require things like remote identification and basic airspace rules across the totality of all UAS operators. We have an excellent community of aviation enthusiasts who operate models. Unfortunately, we are in a very different place than where we were in 2012 where we have a lot of people who are buying a UAS, do not now understand that they are part of the national airspace system and are injecting safety and security risk into the system. And our inability to ensure that they understand that they have to follow the rules, that nuance has created a lack of compliance. And so that is a space where we still need some assistance in being able to put those minimum requirements across

all operators in the national airspace system, and that will also help with our security partners and their ability to discriminate threat. The more people we can move into that compliant category, the fewer folks that our security partners have to worry about and be focused on.

Thank you, Mr. Chairman.

Chairman JOHNSON. Well, the purpose of this hearing, like the purpose of just about every hearing of this Committee, is the first step in solving a problem, the problem-solving process, it is really gathering the information, identifying the problem, admitting we have one. I think that has been the problem, that we have not just collectively as a society understood that, yes, these drones are great, there is so much promise, and they can be a lot of fun, but they pose a real risk, and our laws just have not kept up with that reality.

It is true that FAA does support this legislation, correct? Go ahead.

Ms. STUBBLEFIELD. Absolutely, Chairman Johnson, it is critical that our partners have the tools they need, because a robust security framework is critical to moving forward with all the promise that you described that UAS bring to our economy and to public safety.

Chairman JOHNSON. Thank you all for your testimony, for your service to this Nation. It would be helpful if, working with your other committees of jurisdiction, if asked to brief Committee Members, Chairmen, that you do so very quickly. We do have a unique opportunity. I did not realize it happened so quickly, but I am going to do everything I believe my Ranking Member is on the same page; I think my cosponsors are as well—about getting this attached to the NDAA so it can become law and this first step can actually be initiated, because I think it is just critical. Within the dysfunction that is the U.S. Congress, I would hate to miss that opportunity, then try and pass this in some way, shape, or form, because, again, we just saw from the ACLU, there will be critics of this, I think completely unjustifiable criticism of it, but this is a really great opportunity. So anything you can do within your agencies to help grease the skids for attachment to NDAA would be very appreciated.

Again, thank you for your testimony, for your service. The hearing record will remain open for 15 days, until June 21st at 5 p.m., for the submission of statements and questions for the record. This hearing is adjourned.

[Whereupon, at 11:49 a.m., the Committee was adjourned.]



## A P P E N D I X

---

**“S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones”  
Opening Statement of Chairman Ron Johnson  
June 6, 2018**

This Committee has a tradition of working together in a bipartisan manner to provide the federal government with the authorities it needs to protect the American people. All too often we pass reactive legislation in the wake of a terrorist attack or other security incident. The purpose of this hearing is to proactively address an emerging threat.

Today’s hearing will focus on the emerging threat that drones in the hands of malicious actors could pose to public safety, and examine bipartisan legislation that Senators McCaskill, Hoeven, Heitkamp, Jones, Cotton, Cassidy, Rubio and I have offered to provide authority to the Department of Homeland Security and the Department of Justice to help protect us from that threat.

Unmanned aircraft systems, or drones, can be used by adversaries in a number of ways to harm or threaten public safety. As is the case when discussing any potential threats, I am wary of providing too much information publicly that could be used by those that want to do us harm. But it should come as no surprise that extremists and criminals both at home and abroad continue to develop drone technology to use for malign purposes. Traffickers use drones to conduct surveillance or smuggle illegal drugs into our country. Criminals use drones to smuggle weapons and other contraband into secure areas including federal prisons. Terrorists use drones to execute their evil attacks against innocent civilians.

The number of drone incidents reported by federal agencies – for example drone flights over sensitive areas or suspicious activities – has skyrocketed from 8 incidents in 2013 to an estimated 1,752 incidents in 2016. The technology is not only constantly evolving, but is getting cheaper and easier to buy off the shelf and manipulate.

I am concerned that the federal government does not have the legal authorities it needs to protect the American public from these kinds of threats. The threats posed by malicious drones are too great to ignore. It is not enough to simply tell operators of unmanned aircraft not to fly in certain areas; we must give federal law enforcement the authority to act if necessary.

S. 2836, the *Preventing Emerging Threats Act of 2018*, would give the Department of Homeland Security and the Department of Justice the authority they need to protect certain assets and facilities where drones would pose an unacceptable security risk to the public. The bill provides these authorities while still protecting recreational drone use. By providing a five-year sunset provision, Congress would have an opportunity to revisit and refine the authorities prior to that sunset.

Thank you to our witnesses from across the administration for joining us today and for the work you all do to keep us safe. We appreciate your dedication to our nation’s security and look forward to working with you to protect the American people against these emerging threats.

**U.S. Senate Homeland Security and Governmental Affairs Committee  
Hearing on  
“S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious  
Drones”**

**June 6, 2018  
Ranking Member Claire McCaskill**

**Opening Statement**

Mr. Chairman, thank you for holding this hearing. As we have seen through the years, it has proven a challenge for the law to keep up with technology. The bill the Chairman and I have introduced – the Preventing Emerging Threats Act of 2018 – has the potential to start addressing that deficit.

The Department of Transportation estimates that there could be as many as 4 million drones owned and operated by recreational and commercial users by 2021 and the FAA estimates that recreational and commercial drone sales will increase to 7 million by 2020.

We know that drones can be used for good and for bad. People fly them for fun and use them to take amazing aerial photos. They are used for crop dusting and newscasting. I understand that drones applications have great potential for precision agriculture.

Drones also play a critical role in public safety – for example we know they are used to support firefighting and search and rescue operations and monitor critical infrastructure.

American industry is constantly innovating, and just a few years from now, drone capabilities and advancements may far exceed our imagination today. Congress must encourage and foster that innovation.

Unfortunately, drones also have the potential to cause harm. Terrorist organizations have used drones overseas. And we expect that terrorists are interested in exploiting those same capabilities in the U.S.

The FBI Director testified that the threat that terrorists will use drones in the U.S. is imminent. As the Director explained to this Committee - drones are easy to acquire and operate, and “quite difficult to disrupt and monitor.” That’s the challenge we all face – how to keep Americans safe in the face of a threat that is impossible to put in a box.

Then-Acting DHS Secretary Elaine Duke testified that drones could be used for surveillance, transporting illicit materials, or for violent purposes and that we lack the “signals” to interdict drones and determine whether they are friend or foe.

Just last month, we heard again from DHS Secretary Nielsen, who expressed concern about drones as a “very serious, looming threat” and said that the Department is “currently unable to effectively counter malicious use of drones because we are hampered by federal laws enacted long before UAS technology was available for commercial and consumer use.”

In November 2017, a drone distributed leaflets over a football stadium in Santa Clara, California. While no one was injured, it demonstrated what a drone might be able to do. My Cardinals play at Busch Stadium – and the average attendance of a regular season game is over 40,000. I know that the FAA imposes flight restrictions, but what happens if a drone just shows up? Besides reporting it to law enforcement, no one’s allowed to do anything about it.

I would really like to hear DHS and DOJ address how they can help owners and operators of critical infrastructure and secure mass gatherings. I understand that you don’t have this authority yet, but if you do get it, I want to know how you intend to leverage your authority to help state and local stakeholders. What do they get out of Congress passing this bill?

I want to thank the DHS, FBI and FAA for working with the Committee closely to develop the language in our bill. This bill was informed by the findings of an interagency group—which I understand you all were a part of—that identified “impediments and gaps” in the federal government’s ability to respond to the threat from drones. This interagency committee concluded that without changes in the law, federal agencies were prevented from developing, testing, and evaluating, and deploying counter drone technologies.

I look forward to hearing from our witnesses today about how the Preventing Emerging Threats Act of 2018 helps you address those gaps and

impediments. I also look forward to hearing from other stakeholders, many of whom I understand will be submitting statements for the record, about ways in which we can ensure that any legitimate concerns are addressed before we move the bill out of Committee. We have a real security need that we must address, and I look forward to working with the Chairman to make sure that our legislative approach is the right one.

Thank you, Mr. Chairman.



**Joint Testimony of**

**The Honorable David J. Glawe  
Under Secretary for Intelligence and Analysis  
U.S. Department of Homeland Security**

**Hayley Chang  
Deputy General Counsel  
U.S. Department of Homeland Security**

**Senate Committee on Homeland Security and Governmental Affairs**

**“S. 2836, the *Preventing Emerging Threats Act of 2018: Countering Malicious Drones*”**

**Wednesday, June 6, 2018**

Chairman Johnson, Ranking Member McCaskill, and distinguished members of the Committee, thank you for inviting DHS to speak with you today. We appreciate the opportunity to discuss the Department of Homeland Security’s (DHS) role in countering threats from small Unmanned Aircraft Systems (UAS) in our National Airspace System (NAS).

**Introduction**

First, we would like to thank the Committee for its attention to this issue and holding this hearing to highlight the critical importance of the interagency efforts to secure the national airspace. We would also specifically thank Chairman Johnson, Ranking Member McCaskill, and the other members of this committee for introducing and cosponsoring a bill that would specifically address our equities in this area – this is a monumental step forward. With enactment of this proposal, Congress would reduce risks to public safety and national security, which will help to accelerate the safe integration of UAS into the NAS and ensure that the United States remains a global leader in UAS innovation.

DHS continues to strongly support the Federal Aviation Administration’s (FAA) UAS integration efforts. As the safe integration of commercial and private UAS into the NAS continues, this technology also presents increasing security challenges that require a layered and parallel government security response from federal partners to protect the public from misuse of this technology. The misuse of this technology poses unique security challenges. Generally,

examples of UAS-related threats include recklessly flying UAS near critical infrastructure, intentionally conducting surveillance and counter surveillance of law enforcement, smuggling contraband, or facilitating kinetic attacks on stationary or mobile, and high consequence targets.

We have already seen transnational criminal actors adopt UAS technology to move drugs across the border. Terrorist groups overseas use drones to conduct attacks on the battlefield and continue to plot to use them in terrorist attacks elsewhere. This is a very serious, looming threat that we are currently unprepared to confront. Today we are unable to effectively counter malicious use of drones because we are hampered by federal laws enacted years before UAS technology was available for commercial and consumer use. Public access to these systems, with their current operational capacity and range were not even conceived of when these laws were adopted.

#### **Lack of Authority for Response**

DHS is in need of legislative authority to counter the growing threat posed by UAS. Specifically, DHS needs Counter-UAS (CUAS) authorities to detect, track, and mitigate threats from small UAS. Without this mandate, DHS is unable to develop and operate many types of CUAS technologies. If enacted, S. 2836, the Preventing Emerging Threats Act of 2018 will provide DHS the ability to develop the necessary technology and deploy it in support of our identified missions to mitigate the range of threats from small UAS similar to the Administration's CUAS legislative proposal.

The potential misuse of UAS presents unique security challenges. In normal security situations, law enforcement personnel can establish protective measures to protect people and property from mobile threats—that is simply not the case with drones as they are able to access areas that people, cars, or other mobile devices cannot. Moreover, the most effective technologies for countering malicious uses of UAS conflict with federal laws enacted long before UAS technology was available for commercial and consumer use.

DHS and our interagency partners identified significant legal challenges to law enforcement's ability to use the most up-to-date technologies to detect, track, and mitigate the threats from small UAS. Our primary concerns with the existing legal uncertainty fall into three critical areas:

- (1) The challenges posed by the rapid technological advancement utilized in UAS;
- (2) Strong concerns for our law enforcement personnel subject to potential criminal liability if they were to take action to mitigate a UAS threat; and,
- (3) The need to have comparable authority with our Department of Defense (DOD) partners when working together on National Security Special Events, Special Event Assessment Rating events, and other domestic security operations.

As a result, DHS and the Department of Justice (DOJ) need relief from Title 18 to allow us to use the most effective technology to counter the threat posed by UAS and to ensure that our law enforcement personnel are not criminally liable for using this technology. As you are aware, Congress provided DOD and the Department of Energy (DOE) with relief from Title 18 when it provided them with the authority to detect, track, and mitigate the threat posed by UAS in the

FY2017 and FY2018 National Defense Authorization Act (P.L. 114-328 and P. L. 115-91). We are asking that DHS and DOJ be provided the exact same relief from Title 18. This bill, sponsored by Chairman Johnson and cosponsored by Ranking Member McCaskill, Senators Hoven, Heitkamp, Jones, Cotton, Cassidy, and Rubio, is a critical step to our front line officers' efforts to mitigate UAS threats.

Additionally, providing relief from Title 18 will allow DHS to have commensurate authorities with our DOD partners when working together domestically, thus ensuring there are no operational authority conflicts to protect certain facilities, assets, and operations critical to national security against threats from UAS. Moreover, due to the rapidly evolving technology and the uncertainty associated with the application of Title 18 to these technologies, it is key to get relief from statutory barriers that were not originally intended for the UAS context.

If enacted, S. 2836 would authorize DHS and DOJ to conduct limited CUAS operations to identify, track, and mitigate drone threats. These authorities would apply to a narrow set of important and prioritized missions, and it would allow DHS and DOJ to protect Americans and our own personnel who perform law enforcement and protective missions.

The proposed legislation mirrors the existing statutory authority granted to DOD and DOE/NNSA in the 2017 NDAA and the 2018 NDAA (P.L. 114-328 and P. L. 115-91, respectively). DOD and DOE/NNSA have been able to use these authorities to protect designated facilities and assets here in the United States. The bill also contains robust measures designed to protect privacy and civil liberties. Specifically, the proposed bill limits the collection and retention of communications to and from the drone and ensures that such collection is undertaken only for the purpose of mitigating the threat caused by the UAS.

We are grateful for the demonstrated leadership from Chairman Johnson, Ranking Member McCaskill and all of the Senators cosponsoring S.2836 for your efforts to move these needed authorities forward. DHS and DOJ need Title 18 relief which this legislation provides to allow our officers access to technologies to counter the nefarious use of UAS. We cannot stress enough how important this is. The technology associated with UAS has and continues to evolve faster than the legal authorities surrounding it, and it is critical to grant our security operators relief from statutory barriers to ensure the Department can keep pace with evolving threats, adaptive enemies, and emboldened adversaries. DHS will continue to work with Congress to ensure the swift passage of this critical legislation to address the significant threat.

### **Threat**

Since the Department was first authorized in the Homeland Security Act of 2002 (P.L.107-296), DHS has been on the frontlines to secure and protect our Nation. But the world has changed since 2002, in geopolitics, technology, and the threats we face. Today a cellphone has the computing power of the world's fastest supercomputers only twenty years ago. Terrorists now communicate through encrypted cell phone apps and social media and are utilizing sophisticated, commercial technologies to conduct attacks —challenges we couldn't foresee in 2002.

To best protect the United States and its citizens, we need updated authorities, updated support, and updated accountability for the world we live in today. It is time to ensure that the 240,000 DHS employees who work tirelessly to protect the nation have the tools they need to carry out our mission. The capability of small UAS's is quickly evolving and more advanced systems are becoming widely available, making the potential threats even more acute. As these capabilities have become available, DHS has worked aggressively with our interagency partners to keep up with the advancement in technology. This work to increase our capability to counter existing threats and anticipate future ones will never stop – but we can't make it operational without the authority to do so.

Overseas, terrorist groups and criminal organizations use commercially available UAS to drop explosive payloads, deliver harmful substances, and conduct illicit surveillance. Illicit actors, including terrorists, have been working to increase the payload capabilities of UAS for a variety of reasons, which presents a growing challenge of scale in mitigating the immediate effects of potential threats.

Domestically, criminals, including Mexican transnational criminal organizations (TCO), are increasingly using UAS to deliver narcotics across the southern border, conduct illicit surveillance, avoid U.S. law enforcement, and interfere with ongoing law enforcement operations.

But the threat goes even beyond that. Malicious actors could utilize UASs in order to wirelessly exploit access points and unsecured networks and devices. This can include using UASs to inject malware, execute malicious code, and perform man-in-the-middle attacks. UASs can also deliver hardware for exploiting unsecured wireless systems. In 2015, researchers in Singapore attached a smartphone holding applications to a UAS to detect printers with unsecured wireless connections. The researchers flew the UAS outside an office building, had the phone pose as the printer, and tricked nearby computers to connect to the phone instead of the printer. When a user sent a document for printing, the phone intercepted the document and sent a copy to the researchers using a 3G or 4G connection. The document was then sent to the real printer so the user would not know the document had been intercepted.<sup>1</sup>

Malicious actors could also exploit vulnerabilities within UAS and UAS supply chains to compromise UAS belonging to critical infrastructure operators and disrupt or interfere with legitimate UAS operations. Since 2012, a DHS review of publicly available reporting indicates that there has been a notable increase in reporting of UAS activity near or over critical

---

<sup>1</sup>Zetter, K. (2015). "Hacking Wireless Printers With Phones and Drones." *Wired* [www.wired.com/2015/10/drones-robot-vacuums-can-spy-office-printer/](http://www.wired.com/2015/10/drones-robot-vacuums-can-spy-office-printer/). Accessed January 2, 2018.

*Cyber Defense Magazine*. (2015). "Hacking enterprise wireless printers with a drone or a vacuum cleaner." [www.cyberdefensemagazine.com/hacking/enterprise-wireless-printers-with-a-drone-or-a-vacuum-cleaner/](http://www.cyberdefensemagazine.com/hacking/enterprise-wireless-printers-with-a-drone-or-a-vacuum-cleaner/). Accessed January 2, 2018.

infrastructure; in 2016, over 2,800 incidents were noted in the national airspace, a 44 percent increase over 2015. We expect the trend to continue across all infrastructure sectors.

### ***CBP***

A vital component of DHS's ability to monitor operational capabilities, CBP Air and Marine Operations (AMO), Air and Marine Operations Center (AMOC) integrates surveillance capabilities and coordinates national security threat response with other CBP operational components, including U.S. Border Patrol (USBP). It works with other federal and international partners in this effort.<sup>2</sup> AMOC helps AMO and its partners predict, detect, identify, classify, respond to, and resolve suspect aviation and maritime activity in the approaches to U.S. borders, at the borders, and within the interior of the United States. AMOC utilizes extensive law enforcement and intelligence databases, communication networks and the Air and Marine Operations Surveillance System (AMOSS). The AMOSS provides a single display capable of processing up to 700 individual sensor feeds and tracking over 50,000 individual targets simultaneously.

From January 2015 through December 2017, CBP's AMOC documented 59 UAS incidents along the Southwest Border, with Yuma, Arizona, and Brownsville, Texas, being the most prevalent areas for drug smuggling.

### ***USCG***

The U.S. maritime domain represents the access point for a majority of commerce, as well as transiting military vessels, hazardous chemical barges, cruise ships, regulated waterfront facilities, and recreational boating. All of these represent potential targets.

The Coast Guard is challenged to conduct its statutory missions over 90,000 square miles of water without the added challenge of UAS interference, either inadvertently or intentionally, with vessels and aircraft. UAS can interfere with many Coast Guard missions, including but not limited to:

- Coast Guard escorts of U.S. Navy high value units (e.g. ballistic missile submarines);
- Coast Guard protection of military outloads and supporting combat operations overseas;
- Active search and rescue operations; and
- Ongoing drug and migrant interdiction.

The Coast Guard is increasingly observing overflights of UAS while performing its missions. In 2017 alone, there were 97 Field Intelligence Reports of known UAS sightings during missions. Recently, a UAS landed on the deck of the Coast Guard Cutter Sea Lion while transiting into San Diego Harbor, a port of strategic military importance to the Nation. The cutter was unable to identify the operator of the device, leaving the crew vulnerable and unable to apply traditional Coast Guard use of force tactics, techniques, or procedures. In March of this year, a Coast Guard

<sup>2</sup> AMOC partners include the Federal Aviation Administration (FAA), the Department of Defense (including the North American Aerospace Defense Command (NORAD)), and the governments of Mexico, Canada, and the Bahamas.

helicopter was forced to take evasive action to avoid a UAS while operating at low altitude. These scenarios are indicative of potential threats our fleet faces daily.

#### ***USSS***

The Secret Service must be able to secure the airspace surrounding locations where a protectee is, or will be in order to provide the greatest level of security possible. The authority to counter malicious UAS is essential to that mission. The ability of a potential attacker to monitor Secret Service preparations for a protectee visit or to monitor protectee movements from the air would give them information that would facilitate planning a future attack. UAS could be used to not only plan but also conduct an attack on a protectee. Already, the Secret Service has had several instances where special agents and Uniformed Division officers were called upon to respond to UAS observed at or near protected locations. The threat presented by these devices is not hypothetical or in the future. It is here and now. The Secret Service needs all available tools, both technological and legal, to counter the threat posed by malicious UAS.

If enacted, S. 2836 will enhance Secret Service capabilities to secure airspace within the NCR, at sites visited by protectees, and at National Special Security Events. These authorities will enhance UAS early warning systems, which provide protective details with vital information in a timely manner so that they may take proactive measures against unknown UAS threats in order to maintain the integrity of a protective site and secure protectees.

#### ***TSA***

UAS encounters near major airports remain a growing concern. As part of the FAA airmen certification process, TSA vets all FAA-certificated remote pilot operators against the Terrorist Screening Database. While we are not currently aware of any specific threat reporting targeting our domestic airports or airport operations, in January 2018, press reports indicated adversaries used bomb-laden drones to attack two Russian military bases in Syria. In light of this information, TSA continues to assess the evolving UAS threats to U.S. airports, as well as how those threats may be mitigated in the future, which requires close analysis and coordination with the Federal Aviation Administration.

#### ***NPPD/FPS & IP***

The Federal Protective Service (FPS) protects more than 9,000 federal facilities across the nation and more than a million people at those facilities each day. Since January 2014, FPS has responded to and investigated 180 UAS incidents. The majority of these incidents have been non-nefarious, although several cases have resulted in criminal charges or other sanctions. Based on this experience, FPS has continuing concern with the following threat and risk vectors:

- Accidental harm or death by out of control drone;
- Unauthorized surveillance of sensitive facilities and operations;
- Disruption of law enforcement activities;
- Disruption of government business/provision of government services to customers;

- Sensor delivery (acoustic, imagery, electromagnetic);
- Contraband/weapons delivery that by-passes security screening; and
- Introduction of chemical/biological/radiological/toxic industrial chemicals into elevated building air intakes.

The Department has been working with critical infrastructure owners and operators to better understand the security risk associated with UAS. In 2018, the National Protection and Programs Directorate (NPPD) formed a joint public-private sector working group under the Critical Infrastructure Partnership Advisory Council framework to better define the risks to critical infrastructure posed by malicious UAS operations. Working group members will consider the effective use of UAS technology to enhance security around the perimeter of a fixed asset and help inform UAS security and resilience priorities. The working group kick-off meeting was conducted in March 2018, in Arlington, VA.

To ensure the working group maintains an active approach, sub-groups will be established to execute various projects, including UAS incident baseline and reporting, nefarious UAS indicators, best practices, and methods for UAS tracking, as well as emergency action plans to address improper use of UASs near a facility or event.

NPPD also informs critical infrastructure owners and operators of the evolving risks associated with UAS through the following resources:

- UAS Website: A website is available for resources on UAS security and response strategies ([www.dhs.gov/uas-ci](http://www.dhs.gov/uas-ci)) and a community of interest is maintained on the Homeland Security Information Network (HSIN-CI).
- Countering-UAS Pocket Card: Provides information on current, non-kinetic actions that security and operations officers can take if a UAS is seen near an infrastructure site. It also contains information regarding the different types of UASs and their respective flight ranges and payload capabilities, along with quick tips on how to properly report UAS-related incidents (<https://www.dhs.gov/uas-ci>).
- Counter-UAS Video Provides information on the threats posed by the nefarious use of UAS, potential implications to critical infrastructure operations, and options for risk mitigation. The video leverages subject matter experts and senior security officials to stress the importance of mitigating the risks associated with this evolving threat (<https://www.dhs.gov/uas-ci>).

#### *National Capital Region Airspace*

Mitigating threats from malicious small UAS operations is a challenge across the entire NAS, but even when the airspace is tightly controlled or heavily restricted, we still face potential threats and are constrained by the same limitations outlined above. One unique challenge is protecting the airspace in the National Capital Region, which is some of the most restricted airspace in the country and is home to the White House, the U.S. Capitol, Congressional office buildings, and a multitude of iconic monuments. This building, your offices, and the safety of millions of visitors to the Capitol Complex are all here. Within this region, the DHS-hosted interagency National Capital Region Coordination Center is the main center for providing coordination across the interagency security enterprise and was created after September 11<sup>th</sup> to

provide real-time information sharing and tactical coordination to address potential airborne threats. The Center has representatives from the military, the FAA, and certain federal civilian law enforcement agencies on duty at all times to speed communication and coordination in the event of an unknown or hostile airborne track of interest.

Following September 11<sup>th</sup>, the dimensions of the restricted flight zones over the National Capital Region changed. The FAA implemented the Special Flight Rules Area (SFRA), which includes within its boundaries the Flight Restricted Zone (FRZ) and Prohibited Area 56 (P-56). The White House and the Vice President's residence are located in the P-56. The United States Secret Service is the DHS agency responsible for approving operations within the P-56 and works closely with FAA, Capitol Police, and U.S. Park Police to enable and protect operations in that airspace. In order to enter the SFRA or the FRZ, an aircraft must have approval from the FAA, and the FRZ remains off limits to UAS operators. Despite this layered security approach, we are still experiencing UAS incidents within the NCR that require an appropriate response— even if they are nuisance or non-compliant operators who disregard the rules. The legislation would help DHS provide detection and mitigation capabilities within the NCR to help identify and isolate UAS threats for appropriate mitigation actions.

#### **CUAS Technology / Limitations**

Legal uncertainty also impedes the Department's ability to research, develop and test CUAS technologies for eventual CUAS operations by our authorized users. Under current legal constraints, only a very small number of technologies can be employed to detect and track UAS and none can be employed to disable/mitigate UAS in our homeland. Examples of legal CUAS measures include RADAR, electro-optical/infrared, acoustic, and non-transmitting radio frequency sensors. While these technologies will continue to improve, they currently have shortfalls in both range and accuracy, especially in urban settings, and we are still unable to even test those systems due to the current legal restrictions. An example of a currently illegal, but highly effective technology is the ability to access signals being transmitted between a nefarious UAS and its ground controller to accurately geolocate and track both without false alarms, and potentially take over the control of the UAS and/or stop its ground operator without the use of kinetic measures.

While there is a wide variety of commercially available CUAS solutions, most were developed for the military and we have not been able to determine their performance and suitability for homeland security missions due to legal restrictions. This authority will enhance our ability to test and evaluate promising technologies in realistic operating conditions, to guide industries and inform our development of regulations governing their deployment, especially as it relates to potential mitigation measures.

#### **DHS CUAS Mission Space**

With approval of this authority, Congress would reduce risks to public safety and national security, which will help to accelerate the safe integration of UAS into the NAS and ensure that the United States remains a global leader in UAS innovation.

We are requesting a narrow grant of authority to protect our highest priority mission space (covered facilities/assets), including:

- Security operations, including securing facilities, aircraft and vessels by the U.S. Coast Guard and CBP;
- Protection operations by the U.S. Secret Service;
- Protection of certain federal facilities by the Federal Protective Service
- Security for Special Events
- Active federal law enforcement investigations, emergency responses, or security operations; and
- Reacting to a known national security threat that could involve unlawful use of a drone.

We also strongly support the additional provision in Chairman Johnson's bill that would allow a state governor or attorney general to request assistance for a mass gathering event that would not otherwise fall into the security for special event category above.

State and local law enforcement are generally responsible for protection of these local events, but neither has authority to use CUAS technologies to counter potential threats. This provision will allow DHS or DOJ to provide assistance, within available resources, when requested by the State Governor or Attorney General. We believe this is an important aspect of our continued coordination with state and local law enforcement partners.

The Administration's proposal, as well as the Chairman's bill, also contains robust measures designed to protect privacy and civil liberties. Specifically, the legislation makes clear that CUAS activities conducted pursuant to the statute will comply with the Fourth Amendment to the Constitution and applicable federal laws. In addition, the proposal limits the collection and retention of communications to and from the drone and only for the purpose of mitigating the threat caused by the UAS. We recognize that deployment of UAS authority could, in certain circumstances, present First Amendment concerns, such as the chilling of protected expression or association. We believe that proper respect for these constitutional limitations can be developed through policy implementing the statutory authority. The DHS Privacy Office and the DHS Office for Civil Rights and Civil Liberties will work with CUAS practitioners, as appropriate, to ensure compliance and oversight of any CUAS activities.

S. 2836 also includes the need for robust coordination and collaborative risk analysis with the FAA to ensure any deployment of CUAS technologies in the NAS is conducted safely and includes fair warning to UAS operators. We have committed to working closely with the FAA to balance our operational security needs with requirements for safe and efficient NAS operations.

### **Closing**

Growth in the UAS market will continue and its adoption for commercial and recreational purposes results in increased UAS encounters over critical infrastructure facilities and large public venues – and those are the non-nefarious actors. UAS technology continues to advance with increased ranges and payload capabilities for a variety of legitimate applications of benefit

to the public – and will continue to evolve toward fully autonomous UAS operations. If we do not want to hinder the positive economic outcome of this technological development, we must advance security measures in parallel.

Although there is no single physical countermeasure to deter or prevent unauthorized UAS encounters, effective deterrence will always include sustained outreach, education, development of safety and training standards, deliberate planning, as well as the integration of technical detection and mitigation capabilities. But right now, we can't test mitigation methods, determine the full scope of the threat, or develop counter measures because of outdated legal restrictions that were not created to cover this issue.

DHS is eager to take the next steps, continue to secure our country against all threats, and prudently act to protect the homeland while respecting privacy and civil liberties. Our dedicated professionals at DHS are on watch 24 hours per day, 365 days per year protecting Americans from threats by land, sea, air, and in cyberspace, while also promoting our Nation's economic prosperity. They take decisive action to protect us all from terrorists, TCOs, rogue nation states, natural disasters, and more. Let us show them we have their backs by working together to secure the authorities and resources they need to do their jobs.

Chairman Johnson, Ranking Member McCaskill, and distinguished Senators of the Committee, thank you again for your attention to this important issue and for the opportunity to discuss our counter UAS efforts.

We look forward to answering your questions.



# Department of Justice

---

STATEMENT OF  
SCOTT BRUNNER  
DEPUTY ASSISTANT DIRECTOR  
CRITICAL INCIDENT RESPONSE GROUP  
FEDERAL BUREAU OF INVESTIGATION

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

AT A HEARING ENTITLED  
"S. 2836, THE PREVENTING EMERGING THREATS ACT OF 2018:  
COUNTERING MALICIOUS DRONES"

PRESENTED

JUNE 6, 2018

**STATEMENT OF  
SCOTT BRUNNER  
DEPUTY ASSISTANT DIRECTOR  
CRITICAL INCIDENT RESPONSE GROUP  
FEDERAL BUREAU OF INVESTIGATION**

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

**AT A HEARING ENTITLED  
“S. 2836, THE PREVENTING EMERGING THREATS ACT OF 2018:  
COUNTERING MALICIOUS DRONES”**

**JUNE 6, 2018**

Good morning Chairman Johnson, Ranking Member McCaskill, and members of the Committee. Thank you for this opportunity to discuss the FBI’s concerns regarding the threat posed by unmanned aircraft systems (“UAS”). On behalf of the men and women of the FBI, let me begin by thanking you for your ongoing support of the Bureau.

Today’s FBI is a global, threat-focused, intelligence-driven organization. Each FBI employee understands that to defeat the key threats facing our nation we must constantly strive to be more efficient and effective, and to look over the horizon. Just as our adversaries continue to evolve, so must the FBI. We live in a time of acute and persistent terrorist and criminal threats to our national security, our economy, and our communities. These diverse threats underscore the complexity and breadth of the FBI’s mission.

We remain focused on protecting the United States against terrorism, foreign intelligence, and cyber threats; upholding and enforcing the criminal laws of the United States; protecting privacy, civil rights and civil liberties; and providing leadership and criminal justice services to Federal, State, tribal, municipal, and international agencies and partners.

**Threat**

Today’s UAS have evolved considerably from the early remote control aircraft of the 20<sup>th</sup> century. UAS now have longer flight durations, larger payloads, and sophisticated maneuverability. The rapid development of UAS technology offers substantial benefits for our society and economy. UAS technology may transform the delivery of goods and the performance of countless services, ranging from the inspection of critical infrastructure to the delivery of life-saving medical devices.

But this technology also raises new risks. The FBI is concerned that criminals and terrorists will exploit UAS in ways that pose a serious threat to the safety of the American people. The UAS threat could take a number of forms, including illicit surveillance,

chemical/biological/radiological attacks, traditional kinetic attacks on large open air venues (concerts, ceremonies, and sporting events), or attacks against government facilities, installations and personnel. Sadly, these threats are not merely hypothetical. For more than two years, the Islamic State of Iraq and ash-Sham (ISIS) has used cheap, commercially available drones to conduct attacks and reconnaissance in Syria and Iraq. As Director Wray testified last year, the FBI is concerned that these deadly tactics—perfected overseas—will be performed in the homeland. That threat could manifest itself imminently.

In addition to national security threats, UAS pose very serious criminal threats. Drug traffickers have used UAS to smuggle narcotics over the U.S. southern border, and criminals have used UAS to deliver contraband inside Federal and State prisons. Similar to national security threat actors, criminal actors have utilized UAS for both surveillance and counter-surveillance in order to evade or impede law enforcement. We have also observed the use of UAS to harass and disrupt law enforcement operations.

UAS technology renders traditional, two-dimensional security measures (such as perimeter fences) ineffective, enabling criminals, spies and terrorists to gain unprecedented, inexpensive, and often unobtrusive degrees of access to previously secure facilities. Finally, the mere presence of UAS in the vicinity of an emergency could impede emergency response operations, especially aviation-based responses, in order to avoid any potential collisions between manned aircraft and UAS.

At present, the FBI and our Federal partners have very limited authority to counter this new threat. Potential conflicts in Federal criminal law limit the use of technologies that would enable the FBI to detect or, if necessary, to mitigate UAS that threaten critical facilities and assets. Absent legislative action, the FBI is unable to effectively protect the U.S. from this growing threat. As you know, the Administration recently proposed Counter-UAS legislation designed to fill this critical gap. That legislation would authorize the Department of Justice and the Department of Homeland Security to conduct Counter-UAS activities notwithstanding potentially problematic provisions in the Federal code. The legislation would extend those authorities within a framework that provides appropriate oversight, protects privacy and civil liberties, and maintains aviation safety.

### **Conclusion**

Chairman Johnson, Ranking Member McCaskill, and members of the Committee, thank you again for this opportunity to discuss the FBI's concerns on the threats posed by UAS. We are grateful for the support you have provided to the FBI. We welcome the introduction of the Preventing Emerging Threats Act of 2018. This legislation would provide the authorities requested in the Administration's proposal, which we believe are necessary to mitigate the national security and criminal threats posed by UAS. I look forward to discussing this important legislation with the Committee today.

STATEMENT OF ANGELA H. STUBBLEFIELD, DEPUTY ASSOCIATE ADMINISTRATOR FOR SECURITY AND HAZARDOUS MATERIALS SAFETY, FEDERAL AVIATION ADMINISTRATION, BEFORE THE SENATE HOMELAND SECURITY AND GOVERNMENT AFFAIRS COMMITTEE, "S. 2836, THE PREVENTING EMERGING THREATS ACT OF 2018: COUNTERING MALICIOUS DRONES," JUNE 6, 2018.

Chairman Johnson, Ranking Member McCaskill, Members of the Committee:

Thank you for inviting me to speak with you today. My name is Angela Stubblefield, 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, and safe air transportation of dangerous goods. This includes ensuring programs and operations are coordinated and integrated with the appropriate external and internal organizations, including the National Security Council (NSC), the Departments of Defense (DOD), 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 has become the focal point within FAA for coordinating Unmanned Aircraft System (UAS) security issues and Counter UAS (C-UAS) policy.

UAS technology represents the fastest growing sector in aviation today. UAS, more commonly referred to as drones, are being used every day to inspect infrastructure, provide emergency response support, survey agriculture, and to go places that are otherwise dangerous for people or other vehicles. Entrepreneurs around the world are exploring innovative ways to use drones in their commercial activities. As of May 21, 2018, the FAA has processed over 1 million UAS registrations. The need for us to fully integrate this technology into the National

Airspace System (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 also acknowledge that potential misuse of this technology poses unique security challenges that enable bad actors to overcome the traditional ground-based security measures in place at most sensitive facilities. Today, I would like to discuss with you the FAA's role in maintaining the safety and efficiency of the NAS, the status of our interagency work with our federal partners to address security challenges posed by UAS, and the next steps in building a robust security framework 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 airspace 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 uses its statutory authority to carry out this mission by issuing and enforcing regulations and standards for the safe operation of aircraft, and by developing procedures to ensure the safe movement of aircraft through the nation's skies. In exercising its authority, the FAA also must consider the public's right of free transit through the navigable airspace. This requires close coordination to balance the needs of our security partners with the right of airspace access for both manned and unmanned aircraft.

*Safety of Small UAS Operations*

Consistent with our mission, in 2016, FAA issued the basic rules for small UAS operations—14 C.F.R. part 107—which set the global standard for integration and provided

small drone operators with unprecedented access to the NAS. The provisions of part 107 are designed to minimize risks to other aircraft, people, and property on the ground. Among other things, the regulations require pilots to keep an unmanned aircraft within visual line-of-sight, and to operate only during daylight, unless the drone has anti-collision lights, which enable twilight use. The regulations also address altitude and speed restrictions, as well as other operational limits, such as prohibiting flights over unprotected people on the ground who are not directly participating in the UAS operation.

Part 107 also creates a new pilot certificate—the Remote Pilot Certificate—which is designed to ensure that a person operating a small UAS has the basic level of knowledge required to safely fly an unmanned aircraft in the NAS. The Transportation Security Administration recurrently vets all FAA certificate holders, including those who hold Remote Pilot Certificates. Additionally, part 107 creates airspace rules specific to small UAS operations. Part 107 allows operation in uncontrolled Class G airspace without the need for approval from the FAA. Operations in controlled airspace—Class B, C, D, and surface area E—require prior approval from air traffic control.

#### *Airspace Management*

One of the biggest challenges for our federal security partners is threat discrimination—knowing who is flying where helps the FAA and our security partners understand what the operator’s intent may be, and is critical to threat assessment and response. In addition to the inherent safety benefits of knowing the location of an unmanned aircraft, remote identification of UAS will provide more accurate and critical data that will allow direct and immediate contact with a UAS operator, education of the operator, or, when necessary, enforcement action against the operator to address a violation of federal regulations. We, along with our security and law

enforcement partners, need to be able to quickly identify unmanned aircraft and their operators in order to discern between the clueless, the careless, and the criminal—including serious threats to national security—and to ensure that all operators conduct compliant operations or face the consequences of introducing a safety or security risk into the NAS.

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. To facilitate airspace approvals for small UAS operators, last November, we deployed the prototype Low Altitude Authorization and Notification Capability (LAANC) at several air traffic facilities to evaluate the feasibility of a fully automated solution enabled by public/private data sharing. Based on the prototype’s success, we began the first phase of a nationwide beta test of LAANC on April 30, 2018, enabling LAANC services at about 80 airports. This rollout will continue incrementally to nearly 300 air traffic facilities covering approximately 500 airports. We expect to complete nationwide deployment in September 2018.

LAANC uses airspace data based on the FAA’s UAS facility maps, which show the maximum altitudes in one square mile areas around airports where UAS may operate safely under part 107. It gives drone operators the ability to request and receive real-time authorization from the FAA, allowing them to quickly plan and execute their flights. LAANC also makes air traffic controllers aware of the locations where planned drone operations will take place, and it can provide information on aircraft that have requested access to a defined airspace.

LAANC is an important step toward implementing UAS Traffic Management (UTM). We view UTM as 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. Our plan for future UTM capabilities includes a number of components—LAANC, remote identification, and dynamic airspace management—that will support the needs of industry, FAA, and our security partners.

Ultimately, UTM will enable UAS operations beyond visual-line-of sight to become routine. As UAS capabilities and their use increase, however, so too does the level of concern among the security and defense communities. DOT and FAA have been working closely with our security partners to better understand these concerns, communicate them to our industry partners, and move forward with opportunities to advance UAS integration while addressing and mitigating security risks.

We are using our existing airspace authority to address concerns about unauthorized drone operations over certain national security-sensitive federal facilities. To date, we have restricted drone flights over military installations, sensitive energy facilities, and iconic landmarks like the Statue of Liberty, Hoover Dam, and Mount Rushmore in the interest of national security. We are also working on additional federal agency requests for restrictions for Federal Bureau of Prisons and U.S. Coast Guard facilities. To ensure the public is aware of these restricted locations, we created an interactive map available on the FAA website, and we have updated our B4UFLY mobile app to include a warning to users in close proximity to these sites. This work is also informing our efforts to determine the most efficient and effective way to implement section 2209 of the FAA Extension, Safety, and Security Act of 2016, which will establish a process for critical infrastructure owners to petition the FAA for UAS-specific flight restrictions over their facilities.

*Interagency Coordination*

Coordination and collaboration with our national defense, homeland security, and law enforcement partners is not new to the FAA. We have been working together successfully to address security risks concerning manned aircraft for decades, such as providing air traffic control support for Operation Noble Eagle, and implementing temporary flight restrictions in support of presidential movements and incident response. Our collaboration with security partners to address the challenges presented by unmanned aircraft is a natural extension of this relationship. We have been able to utilize existing processes, procedures, and lessons learned in working together to improve our ability to assess and respond to threats posed by the malicious use of UAS. However, given the unique security risks presented by malicious UAS, more must be done if we are to realize the benefits of full safe and secure integration of UAS into the NAS.

Drones have been used for illegal, malicious purposes both domestically and internationally. Compared to manned aircraft, drones are widely available and have a significantly lower purchase price. They require minimal training, can be operated from almost anywhere, and offer the capacity to bypass traditional, ground-based security measures. They are also generally difficult, if not impossible, to detect using conventional surveillance technologies like radar. Most also currently lack the on-board equipment typically used by manned aircraft for in-flight identification. These characteristics make UAS an attractive option for terrorists and criminals. Examples of the security threats faced by our federal security and defense partners include: kinetic attacks against high-profile people and locations; the delivery of contraband, such as narcotics, across borders and into correctional facilities; surveillance of critical infrastructure and other sensitive national security sites; cyber crimes; and disruption of law enforcement and emergency response operations.

As Congress recognized in the 2016 FAA Extension, significant legal, policy, and technical challenges exist in countering threats posed by the malicious or errant use of drones. The statute clearly articulates Congress's acknowledgement that these security challenges require a layered and integrated government response. We continue to work with our federal partners to develop policies and procedures that will support protection of critical facilities and assets from UAS-based threats, while increasing regulatory compliance and preserving airspace access and the safety and efficiency of operations in the NAS.

*Counter UAS (C-UAS) Authority*

Congress has provided the DOD and the Department of Energy (DOE) authorities to respond to UAS that pose a threat to designated facilities and assets. FAA has been working in close coordination with DOD and DOE on implementation of these authorities in order to ensure that C-UAS systems are operated safely in the NAS. FAA has worked with DOD and DOE to define what actions constitute a threat, develop a concept of operations for employing C-UAS systems at fixed sites, analyze and mitigate the spectrum impact of selected systems, and draft notification procedures and reporting requirements.

Unlike DOD and DOE, most federal departments and agencies do not have 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. Due in part to potential conflicts with certain federal laws, public and private entities have limited authority to deploy technologies that can detect, track, identify, and, when necessary, mitigate UAS that pose a security threat.

*Legislative Proposal for Additional C-UAS Authorities*

Recently, the Administration released a legislative proposal to enable DOJ and DHS to protect certain facilities, assets, and operations critical to national security, against threats from UAS. The DOT and FAA were heavily involved in developing and supporting the Administration's proposal, which includes relief from Title 18 restrictions. Under this proposal, DOJ and DHS will work closely with FAA to ensure that detection and mitigation technologies are tested, evaluated, and deployed in a manner that minimizes adverse impacts on airspace access, as well as air navigation services, avionics, and other systems that ensure safe and efficient operations in the NAS.

DOT and FAA support the Administration's phased approach to seeking C-UAS authorities, and the mirroring of the requirements and mechanisms established in the FY 17 and FY 18 National Defense Authorization Acts (NDAA) in the Administration's legislative proposal. Many of the currently-available UAS detection, tracking, and mitigation systems utilize radio-frequency based technologies that could interfere with the aviation spectrum, negatively impacting air navigation service and avionics systems critical to the safety of flight. Therefore, extensive coordination before, during, and after deployment is required, and safety impacts must be mitigated, in order to safely deploy these technologies in the NAS.

The FAA's role in supporting our partner agencies' research and eventual use of C-UAS technologies is to ensure that the safety and overall efficiency of the NAS is not compromised. FAA must be involved in deployment of C-UAS technology at each fixed location, and for *ad hoc* or mobile operations. We must conduct specific, data intensive analyses for each potential use of C-UAS 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 FAA nor our partner agencies want to jeopardize safety or interfere with compliant UAS operations.

The FAA is currently working with DOD and DOE to strike that balance as they deploy C-UAS technology at sensitive facilities in the United States. We have forged this new path with DOD and DOE, working through many of the toughest aspects of such deployments in the NAS, such as defining threats, developing concepts of operation, and implementing interagency notification and reporting procedures. We are already sharing these processes and procedures with DHS and DOJ to ensure they benefit from the work we have done with DOD and DOE if they are granted C-UAS authorities and Title 18 relief. We are full partners with DOD and DOE in their efforts to implement this authority, by design of the NDAA, and have received assurances of the same level of commitment to operational collaboration from DHS and DOJ as well.

*C-UAS in the Airport Environment*

We also note that Congress has expressed interest in granting FAA the authority to test and utilize UAS detection technology. Section 2206 of the 2016 Extension required the FAA, working closely with DHS and other relevant federal agencies, to evaluate detection technology at airports. From February 2016 through December 2017, the FAA and our partner agencies assessed or observed UAS detection technologies operating at several domestic airports in Atlantic City, New York City, Denver, and Dallas-Fort Worth.

The FAA is coordinating its report to Congress on the results of this pilot effort. We learned that the airport environment presents several unique challenges to the use of such technologies. The available technology itself is at an early developmental stage for employment at an airport. The technical readiness of the systems, combined with a multitude of other factors,

such as geography, interference, location of majority of reported UAS sightings, and cost of deployment and operation, demonstrate that this technology is not ready for use in domestic civil airport environments.

In view of these results, the FAA suggests that other actions, such as implementation of remote identification requirements, are more effective and cost-efficient to address the concerns related to non-compliant UAS operations on and around airports. Given the likely resulting impact on the safety and efficiency of manned aircraft operations, compliant unmanned aircraft, and the provision of air traffic services, the FAA does not currently endorse the general use of any mitigation technology on or around an airport. In this case, the use of mitigation technology could introduce more disruption and safety risk than its use is intended to counter.

#### *Enforcement*

The interagency work to address the security challenges presented by UAS appropriately has been focused on the risks presented by malicious and criminal operations. To date, however, the FAA and our security partners assess that a preponderance of the non-compliant UAS operations that have occurred are likely errant, not malicious, in nature. These errant operations present a safety concern, which we are addressing in a number of ways. Public education and outreach are key to reducing these incidents. Efforts such as the “Know Before You Fly” information campaign and the small UAS registration process serve as opportunities to ensure UAS operators understand the rules and responsibilities for flying an aircraft in the NAS.

If an operator is unwilling or unable to comply with applicable regulations, or is deliberately flouting the regulations, we will take enforcement action. We have a range of civil enforcement tools available to address a violation of federal regulations—from warning letters to civil penalties, and, in the case of an FAA certificate holder, suspension or revocation of that

certificate. Civil penalties range from a maximum per violation penalty of \$1,437 for individual operators to \$32,666 for large companies. Congress also gave the FAA authority to assess civil penalties of up to \$20,000 for interfering with law enforcement, first responders, or wildfire fighting operations. The FAA may take enforcement action against anyone who conducts an unauthorized UAS operation or who operates a drone in a way that endangers the safety of the NAS.

To date, the FAA has initiated 74 cases for incidents involving unsafe or unauthorized UAS operations. In 2017, 19 incidents resulted in enforcement actions. In 2016, there were 13 such cases. In addition, 23 cases have been initiated citing the FAA's small UAS rule, part 107. All of those cases involved careless or reckless operations.

The FAA is also engaged in extensive outreach with federal, state, local, and tribal law enforcement entities through its Law Enforcement Assistance Program (LEAP). LEAP activities include providing guidance on the FAA's website to assist the law enforcement community in responding to UAS incidents and hosting monthly UAS information webinars. Law enforcement officials are often in the best position to detect and deter unsafe and unauthorized drone operations and we rely heavily on their reports to provide us with actionable information concerning these incidents. Accordingly, the FAA works closely with these agencies to provide them with information regarding the evidence needed by the FAA to take enforcement, as well as to provide a communications link where these law enforcement agencies can pass along reports in a timely manner.

The challenge the FAA continues to encounter in both education and enforcement is the misperception by many recreational UAS operators that they are not required to follow the basic rules of UAS operation because they fit under the statutory exemption for model aircraft

operated under the programming of a community-based organization. These unknowing operators present risks to both manned and unmanned compliant operators. In our view, widely-applicable requirements for remote identification are critical to enabling education and, when necessary, enforcement action when operators conduct non-compliant UAS activity. The current exemption for model aircraft—Section 336 of the FAA Modernization and Reform Act of 2012—makes it difficult for the FAA to develop new regulatory approaches that will help expand and facilitate the greater use of UAS in the NAS. Education, civil enforcement, and a set of basic requirements for all UAS operators are essential to bringing the clueless and careless into compliance; however, our security partners still need the authorities and tools to counter threats from criminals.

*Next Steps*

As Congress has recognized, remote identification of UAS is a critical step on the path to full integration of UAS technology. In order to ensure that our airspace remains the safest in the world, and to enable our law enforcement and national security partners to identify and respond to security risks, we need to know who is operating in the airspace. Effective integration and threat discrimination will continue to be a challenge until all aircraft in the NAS—manned and unmanned—are able to be identified. Anonymous operations are inconsistent with safe and secure integration.

We recently published the report and recommendations prepared by the summer 2017 UAS Identification and Tracking Aviation Rulemaking Committee (ARC). The ARC's 74 members represented a diverse array of stakeholders, including the aviation community and industry member organizations, law enforcement agencies and public safety organizations, manufacturers, researchers, and standards entities involved with UAS. The ARC's

recommendations cover issues related to existing and emerging technologies, law enforcement and national security, and how to implement remote identification and tracking. Although some recommendations were not unanimous, the group reached general agreement on most issues. The FAA is reviewing the technical data and recommendations in the ARC report to support the development of the FAA's remote ID requirements. We are currently working on a proposed rule to implement these requirements as quickly as possible.

As listed in the Administration's Spring 2018 Unified Agenda of Regulatory and Deregulatory Actions, we have also drafted a security-focused Advance Notice of Proposed Rulemaking (ANPRM) to gain additional information related to the security concerns that impact the advancement of UAS integration. Once issued, the ANPRM will seek information from the public to inform possible rulemaking proposals for reducing risks to public safety and national security as UAS are integrated into the NAS. Consistent with our statutory authority, the FAA seeks to ensure UAS operations will neither create a hazard to users of the NAS or the public at large, nor pose a threat to national security.

On May 9, 2018, the Secretary of Transportation announced that 10 state, local, and tribal governments were selected to participate in the Administration's UAS Integration Pilot Program. Each of the participants will partner with private sector entities to evaluate operational concepts and provide DOT and FAA with actionable information that will accelerate safe UAS integration. The goals of the program are to: identify ways to balance local and national interests; improve communications with local, state, and tribal jurisdictions; address security and privacy risks; accelerate the approval of operations that currently require special authorizations; and collect data to support the regulatory development steps needed to allow more complex, routine low-altitude operations. We are working with each of the participants to identify the

specific operational concepts that the participants will undertake. A list of the participants and each of their proposed operational concepts can be found at: [https://www.faa.gov/uas/programs\\_partnerships/uas\\_integration\\_pilot\\_program/awardees/](https://www.faa.gov/uas/programs_partnerships/uas_integration_pilot_program/awardees/). We have included, and will continue to engage, our federal security partners in this pilot program.

*Conclusion*

There is no question that a robust security framework is critical to advancing the Administration's goal to fully integrate UAS into the NAS. By enabling federal security and law enforcement agencies to detect and mitigate UAS threats and risks posed by errant or malicious UAS operations, the United States will continue to lead the way in UAS innovation, and offer the safest and most efficient aviation system in the world. Working together, we are confident we can balance safety and security with innovation. We thank the Committee for its leadership on this issue, and we look forward to working with you as we continue to safely, securely, and efficiently integrate UAS into the NAS and solidify America's role as the global leader in aviation.

This concludes my statement. I will be happy to answer your questions at this time.



Testimony before Senate Homeland Security Committee 6/6/2018

Chairman Johnson, Ranking Member McCaskill, Senators and Members of the committee, thank you for opportunity to provide testimony for the record on a topic of great concern to myself, the St. Louis Cardinals and my colleagues in Major League Baseball (MLB).

I'm originally from New York City, live in Illinois and I work in Missouri. I've lived in Texas, Colorado, Kentucky, Georgia, North and South Carolina, almost every country in Central and South America and a country formerly known as West Germany. I'm a retired US Army Special Forces Green Beret and former security professional with the National Geospatial-Intelligence Agency. So I have a diverse perspective of cultures and security.

My career with the St. Louis Cardinals began in January of 2017, at which time I was given a mandate by ownership and senior management of the Cardinals to make Busch Stadium, in St. Louis, the safest place to enjoy baseball or any event. Part of my responsibilities was to work with the Department of Homeland Security (DHS) in achieving our SAFETY (Support Anti-Terrorism by Fostering Effective Technologies) Act Designation, which we earned in December of last year. As part of this endeavor, we received support from the Ranking Member of the committee, Senator McCaskill. Senator McCaskill's interest in the security of Busch Stadium has been greatly appreciated and has started an ongoing dialogue on stadium security in general. As a result, the St. Louis Cardinals are only the fourth team in MLB to achieve the SAFETY Act distinction. This year, we will be submitting our application with DHS for full Certification under the SAFETY Act.

We, the St. Louis Cardinals, and Major League Baseball take security seriously. Baseball is an institution and part of the fabric of the United States of America. The security professionals within Major League Baseball are 100% committed to the preservation of baseball as an institution and are intimately familiar with the impact a terrorist act would have on any baseball stadium. The negative shock wave would be nationwide regardless of the target. We spend millions of dollars, work countless hours and dedicate ourselves to the goal of keeping our guests, fans, teams and employees safe. After the 9/11 attack, baseball was a unifying factor for many Americans and the resumption of games, and the singing of God Bless America at baseball games became a rallying cry for our citizens following that horrific event.

Major League Baseball has made SAFETY Act recognition a goal for all 30 of the teams. To help reach that pinnacle of excellence, we have to be able to identify the threats and vulnerabilities we face, and then determine a means to mitigate the threat and decrease the vulnerability. Last year, the St. Louis Cardinals had over 3.4 million guests attend Busch Stadium for baseball games. In fact, more than 3 million guests have attended regular season Cardinals baseball games each and every year since the current Busch Stadium opened in 2006, and the average attendance of all regular season Cardinals baseball games has exceeded 40,000 guests per game since the facility opened in 2006. One threat, for which there is currently no mitigation, is the topic of discussion for today; Drones and Unmanned Aircraft Systems (UAS).

Drones pose a multi-faceted threat to any open stadium because of the range they can span and the potential for the dangerous payload they can carry. That could vary from an explosive, a heavy object, a chemical or biological agent or even the drone itself being used as the weapon. All of these threats are real and capable of being deployed by a bad actor utilizing a drone. In fact, small commercial drones have already been used in the Middle East by Al Qaeda and ISIS to deploy explosives with great accuracy. Imagine the possibility of a drone being used in such a manner against a stadium filled with 40,000+ targets. The results could be catastrophic. Technology has moved much faster than our laws, and, unfortunately, there is nothing in our current laws that would authorize or permit any stadium operator or any governmental authority to interdict, disable or commandeer a drone or otherwise to safely deal with the threat of a drone attack. Under the current laws, the stadium operator and the occupants of the stadium are rendered completely helpless to the threat of a drone attack.

There is technology that can alert a stadium to the presence of a drone, but that falls far short from any kind of realistic mitigation strategy. There is technology that utilizes other drones to intercept a drone with netting. However, the current law does not authorize or permit us (or any governmental authority) to intercept a drone.

The proposed Senate bill represents a step in the right direction to help address the risk of a drone attack on certain facilities by granting DHS and DOJ UAS authorities. However, as stadium operators we know that more has to be done to fully address and mitigate such risks and strengthen our capabilities to prevent the potentially horrific consequences from a drone attack on a publicly televised event in a facility with more than 40,000 occupants. Expanding the scope of the definition under Special Events Assessment Rating Events to include regular season games would greatly help security. As currently written, the proposed bill provides stadiums protection for regular season games only if they work through their governors or state's attorneys generals for assistance. This adds a layer of bureaucracy when the wording

in the bill can be adjusted to include regular season games as a qualifying 'Special Event'. The defining of 'Special Events' as written, splits hairs about the title of the event without consideration of the target itself. For example, an All-Star Game is captured under the proposed language and there may be only a few thousand more people at the event by comparison to a regular season game. This seems short-sighted and neglects thousands of games and millions of Americans as potential targets.

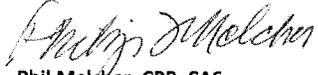
The other main issue that stands out in the proposed bill is that there is still no authority for a private entity to protect itself from a drone threat. We can pay tens of thousands of dollars to purchase technology to monitor a drone as it flies into our airspace and watch it as it deploys an explosive or chemical onto our guests and employees. We have no choice but to watch it happen. We still have no legal authority, under the proposed bill, to intercept or interdict a drone. We are completely dependent on the federal government to change this because even a local ordinance is unenforceable because the federal law and jurisdiction preempts any state or local law or jurisdiction when it comes to airspace. This legal authority for a stadium operator to intercept a drone has to be a critical part of any legislation that deals with drones as a threat. No government entity can be everywhere to protect its citizens, so allowing sports venues to take positive measures to protect millions of guests makes good sense.

The St. Louis Cardinals and the other teams in Major League Baseball work very closely with our local, state and federal government partners to assess threats, mitigate vulnerabilities and protect our guests. We already partner with government entities to make informed decisions about protective measures and to ensure the safety of all events. In St. Louis, the FBI and DHS are active participants in all of our Risk and Threat Assessment meetings and the Cardinals are members of the St. Louis FBI Field Office's Drone Working Group. This group is made up of both government and non-government entities which discuss UAS and drone threats and possible ways to mitigate those threats within the existing boundaries. By providing venues like ours the capability to proactively protect our stadiums internally, we would be avoiding additional burdens on government agencies, eliminate greater bureaucracy and make our stadiums and millions of Americans safer.

We ask that you please consider these measures as part of any drone legislation and not delay a response to the very real and immediate threat that we currently face in our rapidly changing world. There is no mystery in the capability of the threat drones pose and there should be no hesitation in our capability to identify and negate that threat.

Thank you for your consideration.

Respectfully,

A handwritten signature in cursive script that reads "Phil Melcher".

Phil Melcher, CPP, CAS  
Director, Security and Special Operations  
St. Louis Cardinals, LLC



NORTHERN PLAINS UNMANNED AIRCRAFT SYSTEMS TEST SITE  
4149 University Ave  
Grand Forks, ND 58202



**“S. 2836, the Preventing Emerging Threats Act of 2018: Counter Malicious Drones”**

**Testimony of Nicholas Flom**

**Senate Committee on Homeland Security and Government Affairs**

**Wednesday, June 6, 2018**

Chairman Ron Johnson, and Ranking Member Claire McCaskill, thank you for the opportunity to present my views on Unmanned Aerial Systems (UAS) and the emerging threats these systems may pose to aviation safety and national security. I'd also like to thank my senators, Senator John Hoeven and Senator Heidi Heitkamp, for having joined you on sponsoring S. 2836. My name is Nicholas Flom, and I am the Executive Director of Northern Plains UAS Test Site (NP UAS TS). The NP UAS TS is one of seven sites designated by the Federal Aviation Administration (FAA) to conduct critical research on the certification and operational requirements necessary to safely integrate UAS into the National Airspace System (NAS). With an eye toward UAS emerging threats, North Dakota's Governor Doug Burgum formed the UAS Detection and Counter-UAS Task Force in 2017. As co-chair of the UAS Detection and Counter-UAS Task Force, we are exploring government, business and research opportunities in the rapidly evolving field, while also working to accommodate UAS operators who want to test UAS detection and counter measures in North Dakota.

There are three major steps that must be conducted when countering a UAS. First and foremost, new use of existing technologies and a new way of thinking must be used to detect the presence of a UAS. Detection of UAS can be conducted in various ways including using radars, optics, and radio frequency (RF). Once the UAS has been detected, it must be determine if the UAS is a friend or foe. Without the requirements of remote identification and tracking, or the requirement to determine the owner/operator of the UAS, determining friend or foe can be a bit of a challenge, or near impossible. But once the detected UAS has been determined to be a threat, the UAS can be defeated. Just like detecting a UAS, there are multiple ways to defeat a UAS including kinetic, GPS jamming or manipulating RF signal.

*North Dakota*



NORTHERN PLAINS UNMANNED AIRCRAFT SYSTEMS TEST SITE

4149 University Ave  
Grand Forks, ND 58202



Through existing agreements and waivers with the FAA, the NP UAS TS has the exclusive ability to test detection systems anywhere in the country. For example, in 2016, the NP UAS TS obtained FAA airspace approval to fly UAS up against detection systems at Denver's International Airport in support of FAA. I assure you, the NP UAS TS has the ability to obtain FAA airspace approvals that ensure detection systems are fully tested, evaluated, capabilities proven or disproven and industry and government limitations stressed. Currently, federal regulation forbid UAS from flying above 400 feet, but that does not inhibit malicious activity well above that set altitude. Therefore, I strongly suggest the committee consider encouraging the testing of UAS counter measures in multiple classes of airspace.

Additionally, defending, or countering, UAS is much more challenging under the current NAS regulations. Due to a thicket of laws buried in Title 18 Federal Code, it is illegal to counter a UAS. Please be aware North Dakota does have permissible airspace access, in partnership with North Dakota's Army National Guard at Camp Grafton, where testing of counter UAS systems is available. Currently, Minot Air Force Base is testing UAS detection and counter systems at the Camp Grafton.

Because of our rich UAS history with Department of Defense, Department of Homeland Security, Department of Transportation and FAA, North Dakota is uniquely positioned to fully support testing missions for detecting and countering UAS. Although the challenges may seem daunting, we are well ahead of most in testing counter-UAS technologies and evaluating specific UAS emerging threats. The NP UAS TS fully supports your and the committee's efforts to enable counter-UAS efforts through the Preventing Emerging Threats Act of 2018. Again, thank you for allowing me to present my viewpoint on UAS emerging threats and how best to counter those threats.

*North Dakota*

June 6, 2018

Re: ACLU opposes S. 2836

Dear Senator,

On behalf of the American Civil Liberties Union (ACLU), we submit this letter for the record in connection with the Senate Homeland Security and Government Affairs Committee hearing on June 6, 2018 titled, "S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones." **The ACLU opposes S. 2836.**

**While the potential security threat posed by drones is real and the need to protect certain facilities is legitimate, strong checks and balances to protect property, privacy, and First Amendment rights are vital. S. 2836 lacks such measures. The bill amounts to an enormous unchecked grant of authority to the government to forcefully remove drones from the sky in nebulous security circumstances.**

S. 2836 would empower the Department of Homeland Security (DHS) and Department of Justice (DOJ) to intercept, surveil, destroy, or seize drones in a wide array of circumstances – including in cases they are operated by a non-malicious actor like a hobbyist, commercial entity, or journalist. The bill contains insufficient protections to ensure that such authority is not used arbitrarily, abusively, or unnecessarily, and would permit conduct that raises privacy and due process concerns.

The National Defense Authorization Act for Fiscal Year 2018<sup>(1)</sup> authorized the Department of Defense to take action in cases where drones pose a threat to certain assets and facilities. Given this, there are practical questions regarding whether additional DHS or DOJ authority is needed to protect against the safety threats that could be posed by drones. There are also serious questions regarding whether DHS and DOJ have the expertise to carry out such a mission safely and effectively.

Nevertheless, S. 2836 would empower DHS or DOJ to take actions – including seizure, interception of communications, or use of force to destroy a drone – in any case where it is necessary to "mitigate the threat" that a drone may pose to the "safety or security of a covered asset or facility." Among the civil rights and civil liberties concerns posed by the bill are the following:

**The bill would allow DHS and DOJ to take extreme actions when it may not be necessary.** The bill permits DOJ and DHS to use force to destroy or disable a drone, intercept private communications, seize a drone, or take other significant actions. However, the bill's language fails to make clear that such measures may only be employed in a true emergency when there is a threat to life or safety. Instead, the bill permits such extreme measures – which in and of themselves may implicate public safety – simply to "mitigate the threat" to the safety or security of a covered

facility. Such language is broad and fails to ensure that the extreme measures contemplated by the bill are only used in a true emergency.

**The bill would allow the government to seize private property without adequate due process or any showing of wrongdoing.** The bill permits DHS and DOJ to seize private drones (which are then subject to forfeiture) without prior or post-hoc judicial authorization of any kind. The lack of judicial oversight fails to provide an adequate check on DHS or DOJ in cases where exercise of their authority under the bill is abusive, improper, or without appropriate cause. Moreover, it permits the punitive measure of seizing or forfeiting of private property without any due process, showing of wrongdoing, or necessity.

**The bill's broad definition of what constitutes a "covered facility or asset" is vague, applies to areas where there may not be a temporary flight restriction in place, and may raise First Amendment concerns as applied.** The bill's definition of "covered asset or facility" is vague and broad – including, for example, areas related to an "active Federal law enforcement investigations, emergency responses, or security operations." This definition is far more expansive than the authority that has been granted to the Department of Defense.<sup>[2]</sup> As applied, the broad definition in S. 2836 could implicate areas where there is a strong public interest in drone use by the media – such as reporting on the response to a national disaster like Hurricane Harvey – implicating First Amendment concerns. Additionally, this definition could apply in places where there is not a temporary flight restriction in place.<sup>[3]</sup> Thus, there is a significant risk that a drone operator may not be aware of where a prohibited area is or may enter into such an area only inadvertently, yet nonetheless be subject to actions including surveillance or seizure of their private property.

**The bill fails to include oversight and accountability measures to prevent DHS and DOJ from abusing or misusing their authority.** The bill permits DOJ and DHS to take significant actions without sufficient oversight or accountability mechanisms. Interception of communications, seizure, or use of force to destroy or disable a drone would not require judicial authorization or post-hoc review to ensure that it is appropriate or consistent with the law. Additionally, the bill does not contain provisions requiring sufficient transparency or reporting so that the public is aware of how the agencies are exercising their authority. Such protections are critical to prevent abuse or misuse of DHS and DOJ authority.

**The bill exempts DHS and DOJ actions from restrictions in the Wiretap Act, Stored Communications Act, and other provisions in title 18, permitting collection of private information without a warrant or other privacy protections.** The bill permits DHS or DOJ to intercept or interfere with wire, oral, electronic, or radio communications used to communicate with a drone without a warrant from a judge, notice, or other protections that may be required under current law. Such an exception is unnecessary given that existing laws provide ample opportunity for the government to act quickly in an emergency. For example, the Wiretap Act permits the government to intercept communications in an emergency without judicial authorization, and seek

approval after-the-fact. Moreover, once collected, the bill permits information that is collected to be used and disseminated for purposes unrelated to averting an imminent threat, raising additional Fourth Amendment concerns.

The ACLU urges you to oppose S. 2836. If you have questions, please contact Neema Singh Guliani at [nguliani@aclu.org](mailto:nguliani@aclu.org).

Sincerely,

Faiz Shakir  
National Political Director

Secretary  
U.S. Department of Homeland Security  
Washington, DC 20528



Homeland  
Security

June 6, 2018

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

Dear Chairman Johnson:

I want to take this opportunity to thank you and this Committee for leading efforts in Congress to help the Department of Homeland Security (DHS) address security threats from small Unmanned Aircraft Systems (UAS or drones). My Department is committed to working with you and others in Congress to close this identified security gap. We appreciate the opportunity today to discuss DHS's role in defending our country against such dangers and what more we need to protect Americans.

The bipartisan legislation you co-sponsored, S.2836, *Preventing Emerging Threats Act of 2018*, represents a critical step in enabling the Department to address this threat. We are grateful for your leadership, and we strongly support your bill. Once enacted, the legislation will provide DHS the necessary legal authorities to detect, track, and mitigate threats from small UAS. Additionally, the bill will provide DHS the specific authority to develop, test, and deploy within the United States the most advanced and effective counter-UAS technology to mitigate threatening or malicious drones.

The threat is real. We are witnessing a constant evolution in the danger posed by drones as the technology expands and as increasingly advanced drones become more available and affordable worldwide. Commercially available drones can be employed by terrorists and criminals to drop explosive payloads, deliver harmful substances, disrupt communications, and conduct illicit surveillance both domestically and internationally against U.S. citizens, our assets and interests, and those of our allied partners. This technology also presents a growing risk to our Department's law enforcement officers and personnel in the field as they execute our homeland security missions.

The laws on the books today were not written with weaponized drones in mind. As a result, the technology has outpaced our ability to respond to it. Our hands are tied when it comes to guarding Americans against these threats, and if we tried to, our officers and agents could be at risk of criminal liability for simply doing their jobs to protect the public. Providing statutory relief from these barriers will enable our teams to quickly test and deploy effective counter-UAS

The Honorable Ron Johnson  
Page 2

technologies that were previously unavailable to us. With enactment of S.2836, we will be able to further execute our highest priority missions, including ensuring the safety of our coasts, the security of our borders, and the protection of large crowds at special events.

As I have previously stated, immediately obtaining this authority is necessary to ensure we have a robust security framework in place to support the Administration's goal of advancing UAS integration in the National Airspace System, including the Presidentially-directed "Drone Integration Pilot Program" that is being administered by the Federal Aviation Administration (FAA). The Department acknowledges the economic and social benefit that drones provide to this country, but we cannot ignore the homeland security concerns that have emerged from misuse, careless use, or malicious use of this technology. I applaud your introduction of S.2836, which acknowledges the need for flexibility to address this issue and will provide us the additional authority and tools needed to safely and successfully perform our mission while respecting the privacy and civil liberties of those we seek to protect and ensuring that safety is not compromised in the National Airspace System.

Thank you again for your attention to this important matter, and for your continued support of the men and women at DHS committed to protecting this Nation. Your cosigner, Ranking Member McCaskill, will receive a separate, identical response.

Best Regards,



Kirstjen M. Nielsen  
Secretary



June 6, 2018

Chairman Ron Johnson  
U.S. Senate  
Committee on Homeland Security &  
Government Affairs  
340 Dirksen Senate Office Building  
Washington, D.C. 20510

Ranking Member Claire McCaskill  
U.S. Senate  
Committee on Homeland Security &  
Government Affairs  
340 Dirksen Senate Office Building  
Washington, D.C. 20510

Dear Chairman Johnson and Ranking Member McCaskill:

On behalf of the Security Industry Association (SIA), I would like to express our strong support for S. 2836, the *Preventing Emerging Threats Act of 2018*, bipartisan legislation which grants new authorities to the U.S. Department of Homeland Security (DHS) and Department of Justice (DOJ) to administer a counter unmanned aerial systems (UAS) program to protect certain assets and perform critical missions. SIA is an international trade association representing nearly 900 security solutions providers, many of which provide public safety technology vital to homeland security.

Our member companies have made significant investments in effective counter-UAS technologies; however, updates to federal laws and regulations are required to allow the responsible integration of counter-UAS capabilities into the overall security infrastructure. Your legislation takes the important step of expanding the Federal government's capabilities to protect critical assets against the threat posed by unauthorized UAS seeking to cause serious damage against critical infrastructure.

Furthermore, we urge you to consider the pressing need for enabling the appropriate state and local government and private sector entities to utilize counter-UAS technology for public safety and critical infrastructure protection purposes. We are hopeful that the establishment of a counter-UAS program called for under S. 2836 will not only enhance the ability of covered agencies to carry out their missions, but also help provide a model and path forward for effective use of counter-UAS technologies by appropriate non-federal entities.

SIA looks forward to working with you to ensure swift passage of *Preventing Emerging Threats Act* this Congress. Thank you for your leadership and attention to this important matter.

Sincerely,

A handwritten signature in black ink that reads "Don Erickson". The signature is written in a cursive style.

Don Erickson  
CEO  
Security Industry Association



**Cathy L. Lanier  
Senior Vice President of Security  
National Football League**

**Statement for the Record  
S. 2836, Preventing Emerging Threats Act of 2018: Countering Malicious Drones  
Committee on Homeland Security and Governmental Affairs  
United States Senate**

**June 6, 2018**

Chairman Johnson and Senator McCaskill, thank you for the opportunity to submit this testimony for the record in the Committee's hearing on S. 2836, the Preventing Emerging Threats Act of 2018. I appreciate the opportunity to address issues related to threats posed by malicious operators using unmanned aerial vehicles, or drones. As you may know, I joined the National Football League in September 2016 after more than 25 years in local law enforcement in the District of Columbia. At the NFL, I oversee the security policies and procedures that protect the 1,700 professional players, the hundreds of coaches and other staff associated with our 32 clubs, and the 17 million fans who attend our games each year. Club security officials and I work closely with local law enforcement officials, federal authorities, stadium owners, and many others to provide a safe and secure environment for our fans to enjoy the games.

In the two years that I have been at the NFL, we have observed a dramatic increase in the number of threats, incidents, and incursions by drones. Most notably, in November 2017, a drone operator was arrested after using a drone to distribute leaflets over NFL stadiums during two games. Although this action violated a number of laws and regulations, the operator fortunately only dropped leaflets. The incident, however, demonstrated dramatically the threat that drones can pose to teams and crowds gathered in NFL stadiums.

The Federal Aviation Administration and Congress have long recognized that stadium crowds are an enticing target for malicious actors. Following the terrorist attacks of September 11, 2001, the Federal Aviation Administration established flight restrictions over stadiums and other large gatherings. Congress subsequently strengthened and codified these requirements. The current version of the flight restrictions prohibits all aircraft operators over certain sporting events for one hour before until one hour after the event, from ground level to 3,000 feet, and within a radius of three nautical miles. In addition to NFL games, this flight restriction applies to Major League Baseball games, NCAA Division One football games, and NASCAR Sprint Cup, Indy Car, and Champ Series races. The flight restrictions designate the airspace as National Defense

Airspace, and any operator who knowingly or willfully violates the flight restriction may be subject to criminal penalties.

The temporary flight restriction above stadiums and other sporting events apply broadly to all aircraft operations, including both general aviation and commercial aircraft, and flight under both visual flight rules and instrument flight rules. Importantly, the flight restrictions apply to *all* aircraft, whether manned or unmanned. The Federal Aviation Administration has worked extensively to educate the aviation community about the flight restrictions. Air traffic control towers and centers, and licensed pilots have worked cooperatively to respect this protected airspace. As a result, the temporary flight restrictions over sports events have largely worked as intended, keeping commercial and civil aircraft away from stadiums during games.

Unfortunately, drones present an entirely different challenge. Unlike traditional aircraft, unregulated drones can be acquired easily and cheaply by anyone, anywhere, anytime. Highly sophisticated drones are widely available at retail stores and online. Drones are sold to the general population for use by unlicensed individuals, often with no awareness of airspace rules, flight restrictions, or many other regulatory requirements related to aircraft. Drones are sold broadly without regard to applicable flight restrictions. For example, although drone flights are prohibited throughout Washington, D.C., numerous electronics stores and other retailers market drones in the city without notifying customers that a local flight would break the law. Unlike licensed pilots who must undergo specific training and are required to check for flight restrictions before each flight, many drone operators are untrained and simply unaware of the flight restrictions that apply to stadiums.

Drones also present a unique threat by the nature of their operations. Drones are small and easily portable. Unlike manned aircraft, drones can be launched quickly and in close proximity to a stadium, such as from a stadium parking lot. The FAA established the three-mile radius of the stadium flight restriction to allow authorities to have some warning about an aircraft that was purposefully violating the airspace, hopefully before the aircraft was in a position to threaten the stadium and fans. This three-mile buffer zone is completely irrelevant to a drone because a drone can take off immediately adjacent to a stadium. Additionally, as drones become increasingly powerful and capable, drones are able to carry payloads rivaling some small aircraft.

These threats are not merely hypothetical. In 2018, the NFL recorded about a dozen intrusions by drones at stadiums during games. In an NFL season that is only 17 weeks, the frequency of drone incursions is quite alarming. Some of these incursions have been high profile and highlight the security risks related to NFL games.

As a result of these events, the NFL has increasingly engaged the FAA and other policymakers on the development of new policies, procedures, and approaches related to reducing the threat posed by drones. We support the aims of S. 2836, the Preventing Emerging Threats Act of 2018, which expands the authority to interdict potentially malicious attacks by drones and drone operators. Under the legislation, the interdiction authority that Congress had

previously granted to the Department of Defense and the Department of Energy would be extended to the Department of Homeland Security and the Department of Justice.

Consequently, federal law enforcement officials at these agencies would have the authority to take the necessary steps to mitigate and counteract the threat posed by drones in certain circumstances. Such circumstances include when a State's governor or attorney general requests that federal law enforcement officials provide support for state, local, or tribal law enforcement to ensure the security of mass gatherings. This specific provision recognizes and reflects the fact that local law enforcement officers stand at the frontlines and are primarily responsible for providing safety and security at most locations where drones may present risks, including at the vast majority of large-scale amateur and professional sporting events, such as NFL games. With 256 regular season games played across the country, we believe that the legislation under consideration is an important first step, but more must be done to provide local law enforcement officials with the authority they need to protect our games.

The NFL therefore strongly encourages Congress to consider additional reforms that will provide authorities to local law enforcement officers, with appropriate training and expertise, to detect and intercept drones that pose a known and identifiable threat to an NFL game in violation of the flight restrictions that Congress and the FAA have established.

In parallel, the NFL believes that the Federal Aviation Administration must rapidly adopt and implement a remote identification requirement for all, or nearly all, drones sold or operated in the United States. Federal officials, air traffic control operators, and local law enforcement officers need a simple and easy method to identify a drone and its operator when a device is spotted in a dangerous location or in violation of an established flight restriction. Any class of drones excluded from such a requirement must be very narrow and limited to drones that do not present any possible security threat to a large gathering of people. To implement a robust remote identification requirement, Congress must also revise the hobbyist exemption in section 336 of the FAA Modernization and Reform Act of 2012. Although this provision was undoubtedly well intentioned at the time it was adopted, it is far too broad for today's environment. The current hobbyist exemption permits far too many drones to be flown by far too many unlicensed and untrained pilots.

On behalf of the National Football League, I look forward to working with Congress and the Federal Aviation Administration on our shared goal of ensuring the safety and security of the players, coaches, fans, and others who attend our games. Thank you for the opportunity to submit this testimony for the record. The National Football League would be pleased to answer any questions that you may have about our efforts to protect fans from the increasing threat of malicious attacks by drones and drone operators.

**Post-Hearing Questions for the Record  
Submitted to Hon. David Glawe and Haley Chang  
From Senator Claire McCaskill**

**“S. 2836 – the Preventing Emerging Threats Act of 2018: Countering Malicious Drones”**

**June 6, 2018**

<b>Question#:</b>	1
<b>Topic:</b>	Drone Threat
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Based on where terrorists and malicious actors have used drones for overseas, what is the probability that drones will be used by terrorists in the U.S. in the next few years?

How imminent is the threat and why must the Department of Homeland Security (DHS) gain counter-drone authorities now?

**Response:** We assess with high confidence that terrorists overseas will continue to use small UAS in order to advance nefarious activities and exploit physical protective measures. While there has been no known malicious use of UAS by these adversaries in the United States, we cannot rule out that such encounters may occur in the near future—perhaps imminently--due to their legal retail availability, general ease of use, and prior use overseas.

Reports of UAS encounters by law enforcement and security officials in the Homeland already occur with alarming frequency. We assess with high confidence that reports of UAS encounters within the United States will continue to rise as these systems continue to gain popularity with recreational and commercial users. Since 2012, there has been a notable increase in reporting of UAS operations near or over critical infrastructure based on a review of data from federal, state, local, private and open source reporting.

Lack of effective, technology-based countermeasures will hinder the ability of DHS to disrupt malicious activities and prevent an attack using an UAS within the Homeland Security Environment. According to internal DHS data involving UAS reports since 2012, operators are not identified in 85% of all reports received from State, local, private and Federal partners involving unauthorized operations of UAS over or near critical infrastructure.

<b>Question#:</b>	2
<b>Topic:</b>	Drones Used
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Please provide examples of where drones have been used by terrorists in the 18 months in theater and efforts to use drones within the U.S., the type of drones used, locations and targets, and the availability to the general public of the drone technology used.

**Response:** We can assess with confidence that terrorists overseas will continue to use small unmanned aircraft systems (UAS) in order to advance their nefarious activities and exploit physical protective measures. Overseas, terrorist groups and criminal organizations have used commercially available UAS to drop explosives, deliver harmful substances, and conduct illicit surveillance. While there has been no demonstrated use of a weaponized UAS by these adversaries to conduct attacks within the inside the United States, we cannot rule out that such events may occur in the future due to their legal retail availability and general ease of use. Some examples of UAS threats can include: recklessly flying UAS near major airports and critical infrastructure; intentionally flying drones over special events where mass gatherings are occurring; intentionally conducting surveillance and counter surveillance of law enforcement; and facilitating kinetic attacks on stationary or mobile, high-consequence targets.

Domestically, criminals, including transnational criminal organizations, are increasingly using UAS to deliver narcotics across the southern border, conduct illicit surveillance, avoid U.S. law enforcement, and interfere with ongoing law enforcement operations. The United States Coast Guard is also increasingly observing overflights of UAS while performing its missions. In 2017 alone, there were 97 Field Intelligence Reports of known UAS sightings during missions. Recently, a UAS landed on the deck of the Coast Guard Cutter Sea Lion while transiting into San Diego Harbor, a port of strategic military importance to the Nation. The cutter was unable to identify the operator of the device, leaving the crew vulnerable and unable to apply traditional Coast Guard use of force tactics, techniques, or procedures. In March of this year, a Coast Guard helicopter was forced to take evasive action to avoid a UAS while operating at low altitude. These scenarios are indicative of potential threats our fleet faces daily. We believe that reports of UAS encounters within the United States will continue to rise as these systems continue to gain popularity with recreational and commercial users.

Since 2012, there has been a notable increase in reporting of UAS operations near or over critical infrastructure based on a review of publically available data from federal, state, local, private, and open source reporting. Further, there are numerous incidents in which drones have been encountered flying over major events and mass gatherings in spite of the establishment of “No Drone Zones” and temporary flight restrictions. Most notably a

<b>Question#:</b>	2
<b>Topic:</b>	Drones Used
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

2017 incident in which drones were used to drop leaflets over two NFL stadiums. This activity, whether malicious or not, poses a very significant public safety risk.

<b>Question#:</b>	3
<b>Topic:</b>	Missions Impeded
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Provide a few clear examples where drones have impeded your ability to carry out your critical missions and instances in which you would have used counter drone authority if you had had it.

How many incidents have you documented of unauthorized drones posing a threat to DHS-related missions?

**Response:** Domestically, criminals, including transnational criminal organizations, are increasingly using unmanned aircraft systems (UAS) to deliver narcotics across the southern border, conduct illicit surveillance, avoid U.S. law enforcement, and interfere with ongoing law enforcement operations. UAS also present a challenge for critical infrastructure owners to protect against evolving threats due to their ability to easily overcome traditional perimeter defenses. These threats require new authorities and associated counter UAS technologies to mitigate the threat. DHS and DOJ federal law enforcement officers need the proper authorities and the right tools and technologies to make the safest determination when responding to a UAS threat.

From January 2015 through December 2017, CBP's Air and Marine Operations Center documented 59 UAS incidents along the Southwest Border, with Yuma, Arizona, and Brownsville, Texas, being the most prevalent areas for drug smuggling.

The United States Coast Guard is increasingly observing overflights of UAS while performing its missions. In 2017 alone, there were 97 Field Intelligence Reports of known UAS sightings during missions. Recently, a UAS landed on the deck of the Coast Guard Cutter Sea Lion while transiting into San Diego Harbor, a port of strategic military importance to the Nation. The cutter was unable to identify the operator of the device, leaving the crew vulnerable and unable to apply traditional Coast Guard use of force tactics, techniques, or procedures. In March of this year, a Coast Guard helicopter was forced to take evasive action to avoid a UAS while operating at low altitude. These scenarios are indicative of potential threats our fleet faces daily. Additionally, in September 2017, during the United Nations General Assembly in New York City, an illegally operated UAS slammed into one of the main rotors of a U.S. Army helicopter performing a patrol mission, despite the fact that was a temporary flight restriction in place for that airspace.

But the threat goes even beyond that. Malicious actors could utilize UAS in order to wirelessly exploit access points and unsecured networks and devices. This can include

<b>Question#:</b>	3
<b>Topic:</b>	Missions Impeded
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

using UAS to inject malware, execute malicious code, and perform man-in-the-middle attacks. UAS can also deliver hardware for exploiting unsecured wireless systems.

Malicious actors could also exploit vulnerabilities within UAS owned by critical infrastructure operators and interfere with legitimate UAS operations. Since 2012, a DHS review of publicly available reporting indicates that there has been a notable increase in reporting of UAS activity near or over critical infrastructure; in 2016, over 2,800 incidents were noted in the national airspace, a 44 percent increase over 2015. The Federal Protective Service (FPS) protects more than 9,000 federal facilities across the Nation and more than a million people at those facilities each day. Since January 2014, FPS has responded to and investigated 180 UAS incidents. The majority of these incidents have been non-nefarious, although several cases have resulted in criminal charges or other sanctions. DHS expects the trend to continue across all infrastructure sectors.

Drones have been seen repeatedly in the airspace over and around major special events. These events include parades, marathons and Super Bowl ancillary events. To date these incursions have been non-malicious. However, should this same technology be used as a delivery mechanism for an improvised explosive device, the potential impact could be devastating.

<b>Question#:</b>	4
<b>Topic:</b>	Taking Down a Drone
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Besides the violation of federal law, please explain the concerns attached to simply taking down a drone.

**Response:** DHS is in need of legislative authority to counter the growing threat posed by unmanned aircraft systems (UAS). Specifically, DHS needs Counter-UAS (CUAS) authorities to detect, track, and mitigate threats from small UAS. Without this mandate, DHS is unable to develop and operate many types of CUAS technologies. S. 2836, *the Preventing Emerging Threats Act of 2018*, would provide DHS the ability to develop the necessary technology and deploy it in support of our identified missions to mitigate the range of threats from small UAS. With approval of this authority, Congress would reduce risks to public safety and national security, will help to accelerate the safe integration of UAS into the National Airspace System (NAS) and ensure that the United States remains a global leader in UAS innovation.

The potential misuse of UAS presents unique security challenges. In normal security situations, law enforcement personnel can establish protective measures to protect people and property from mobile threats—that is simply not the case with drones as they are able to access areas that people, cars, or other mobile devices cannot. Moreover, the most effective technologies for countering malicious uses of UAS conflict with federal laws enacted long before UAS technology was available for commercial and consumer use.

Additionally, state and local law enforcement are generally responsible for protection of local events and mass gatherings, but neither has authority to use CUAS technologies to counter potential threats. A provision included in S. 2836 would allow DHS or DOJ to provide assistance, within available resources, when requested by the State Governor or Attorney General. We believe this is an important aspect of our continued coordination with state and local law enforcement partners.

The Administration's proposal, as well as the Chairman's bill, also contains robust measures designed to protect privacy and civil liberties. Specifically, the legislation makes clear that CUAS activities conducted pursuant to the statute will comply with the Fourth Amendment to the Constitution and applicable federal laws. In addition, the proposal limits the collection and retention of communications to and from the drone and only for the purpose of mitigating the threat caused by the UAS. We believe that proper respect for constitutional limitations can be developed through policy implementing the statutory authority. Also, both the Administration's proposal and S. 2836 identify the need for robust coordination and collaborative risk analysis with the Federal Aviation Administration (FAA) to ensure any deployment of CUAS technologies in the NAS is

<b>Question#:</b>	4
<b>Topic:</b>	Taking Down a Drone
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

conducted safely and includes fair warning to UAS operators. DHS has committed to working closely with the FAA to balance our operational security needs with requirements for safe and efficient NAS operations.

<b>Question#:</b>	5
<b>Topic:</b>	Waiving Title 18
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The DHS Deputy General Counsel testified that a critical piece of the bill is the language waiving Title 18.

Understanding that technology is constantly evolving and Department employees need legal certainty, please explain in detail why a complete waiver of Title 18 is necessary rather than inventorying Title 18, and waiving specific statutes.

What are the consequences of DHS not having counter drone authority?

**Response:** Consistent with the authorities exercised by the Department of Defense (DOD) and Department of Energy (DOE), under the proposed draft legislation, DHS and Department of Justice (DOJ) officers would be exempt from potential criminal penalties for performing their duties to protect the homeland pursuant to the authorities granted in this legislation. In order for the legislation to be effective, it must remove uncertainty found in existing law that could place operators of this capability in legal jeopardy. That is why the Administration favors a clear approach that would completely eliminate uncertainty by covering specific provisions of Title 18 and one provision of Title 49. Congress took that approach in each of the last two NDAA's with respect to DOD and DOE's employment of Counter-UAS (CUAS) activity.

This approach ensures that security personnel in DOJ and DHS do not receive fewer protections than their colleagues in DOD and DOE while performing the same type of activity. DHS and DOJ personnel deserve the same protections as their DOD and DOE counterparts. Providing different protections for DOJ and DHS could also make joint operations more difficult. This approach helps to avoid a negative inference: i.e., if one law has a categorical exclusion, and another does not, a court could interpret that as Congressional intent to open up liability for some provisions.

Operationally, differing authorities and CUAS technologies may lead to security gaps in areas of joint responsibility. Not only could an authority gap cause different capabilities, but also significantly impair our ability to create a common operating picture where we can share critical threat data among participants in joint operations or joint areas of responsibility. The DOD legislation limits the personnel authorized to exercise this authority to employees with assigned duties that include safety, security, or protection of personnel, facilities, or assets. The proposed legislation contains this same limitation. As a result, both provide for the same ability for the appropriate personnel to conduct force protection/security operations, utilizing unique capabilities, to counter threats posed by unmanned aircraft systems (UAS). The legal framework governing any peacetime

<b>Question#:</b>	5
<b>Topic:</b>	Waiving Title 18
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

domestic use of force to counter a nefarious UAS must comply with the Fourth Amendment's prohibition against unreasonable searches and seizures, regardless of whether the use of force is by DOD, DHS, or DOJ. Thus, any federal effort to counter UAS that involves or requires a "seizure" of property or persons must adhere to the Fourth Amendment's general reasonableness requirement.

The purpose of the legislative proposal is to close the existing loophole that prevents federal law enforcement from addressing the current UAS threat. To that end, the legislation is narrowly tailored to authorize only enumerated actions ("detect, identify, monitor," etc.) toward a UAS that are "necessary to mitigate the threat" posed by that UAS. This does not remove liability for independent criminal acts. It protects only CUAS operators acting in the course of their assigned duties to protect their teams and the public

Since the hearing, the Department has worked closely with this committee, the Judiciary Committee, and the Commerce, Science, and Transportation Committee on the Title 18 waiver provision to narrow the applicable provisions. The Department has agreed to narrow the breadth of the waiver.

<b>Question#:</b>	6
<b>Topic:</b>	Listing Facilities
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** S. 2836 authorizes DHS to take certain actions necessary to mitigate the threat posed by drones to a covered facility or asset. A covered facility or asset is to be identified by the Secretary through a risk based assessment and must be directly related to certain mission sets. The bill allows the Secretary to make this designation.

Please explain why you are unable to list out the covered facilities and assets you would like the counter drone authority to apply to?

**Response:** As described in the Administration's proposal and the draft bill, covered facilities and assets are those (1) within the United States; (2) that are identified by DHS and DOJ through a risk-based assessment conducted in coordination with the DOT/FAA; and (3) that directly relate to one of the following missions:

- United States Coast Guard and U.S. Customs and Border Protection security operations, including securing facilities, aircraft and vessels;
- United States Secret Service protection operations;
- Federal Protective Service protection of federal facilities;
- U.S. Marshals/DOJ protection of its facilities and court personnel;
- Bureau of Prisons protection of its high-risk facilities;
- Security for Special Events: National Special Security Events designated by the President at the request of the Secretary of DHS; or Special Event Assessment Rating Events
- When a state governor or attorney general requests assistance for a mass gathering event that would not otherwise fall into the security for special event category above;
- Active federal law enforcement investigations, emergency responses, or security operations carried out by DHS or DOJ; and
- Reacting to a known national security threat that could involve unlawful use of a drone.

DHS and DOJ will be required to assess what covered assets and facilities within the above authorized mission sets will be prioritized to receive CUAS protections – and not all DHS or DOJ covered assets and facilities will require counter-unmanned aircraft systems (CUAS) protections. Additionally, until we have completed the necessary threat and risk assessments of the prioritized assets, in coordination with DOT/FAA, we will not have a final list. Further, the list of covered assets and facilities could change over time and must adapt to the evolving threat. Therefore, a static list is unlikely to remain

<b>Question#:</b>	6
<b>Topic:</b>	Listing Facilities
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

current and will constantly need to be evaluated against the threats we face from malicious use of UAS.

Regarding special events, the list of Special Events Assessment Rating events is not static and varies dependent on: 1) risk; 2) threat; and 3) data submission from the state and local authorities each year. The event risk assessment process is executed each year and is dependent on state and local authorities to provide their event information to DHS for inclusion in the process. The federal interagency uses this data set for awareness of non-NSSE special events occurring across the nation.

<b>Question#:</b>	7
<b>Topic:</b>	Risk Based Assessment
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Explain how designating covered assets and facilities through a risk based assessment would work. Is this risk based designation process similar to anything DHS has done before in other areas?

How does requiring that the designation be "risk based" limit the number of assets or facilities covered? In your estimation how many DHS facilities do you anticipate would be included in covered asset and facility?

**Response:** The required risk-based assessment is a critical component to prioritizing how DHS and DOJ will protect our most important assets, facilities and personnel within the context of the authorized mission sets. The risk assessments will also be coordinated with the Department of Transportation (DOT) and will include a number of important factors, including but not limited to: 1) potential impacts to the national airspace system, including potential effects on manned aircraft and unmanned aircraft systems, airport operations, infrastructure, and air navigation services; 2) options for mitigating any identified impacts to the national airspace system related to the use of any system or technology, including minimizing disruptions to the transmission of radio or electronic signals; 3) the ability to provide reasonable advance notice to aircraft operators when possible; 4) the location of a covered facility or asset, including whether it is located in a populated area or near other structures, open to the public, and any potential for injury or damage to persons or property; 5) potential consequences to national security, public safety, or law enforcement if threats posed by unmanned aircraft systems are not mitigated or defeated. Several DHS offices and components will be involved in the development of each risk assessment, to include I&A for specific assistance with the threat context and NPPD to assist in evaluating and assessing the risk factors.

Currently DHS manages the very mature, robust, Special Events Assessment Rating Methodology to assess risk to state and local events occurring across the nation. This subjected system of risk analysis has been in use for approximately 15 years and is recognized across the US Government and nationally as a reliable accurate mechanism for determining special event risk. This methodology considers threat (using up to date "High Income Nation" attack trends), vulnerability (event venue type and access restrictions), and consequences of a successful attack (crowd density vs attack type). The Methodology uses data voluntarily submitted by state and local government authorities.

Additionally, S&T will assist in evaluating the potential use of technology systems, including their effectiveness to mitigate UAS threats and their impact on the airspace and surrounding environment. DHS will also benefit from the assessments that DOD has

<b>Question#:</b>	7
<b>Topic:</b>	Risk Based Assessment
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

already completed with DOT and we will look to leverage that work into our complement of risk assessments. DHS will not be able to provide CUAS protections to every covered asset or facility, and that was not our intention when seeking this authority. Instead we are proposing to use this new authority judiciously and to protect our most prioritized assets within the defined mission sets, as described in the draft legislation. The specific number of covered assets and facilities has not yet been determined, as our Components have not yet completed their risk assessments nor coordinated those assessments with DOT.

<b>Question#:</b>	8
<b>Topic:</b>	S. 2836 Mission Sets
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** DHS use of counter-drone authority to secure a covered asset or facility from the threat posed by a drone must be directly linked to a mission set listed in S. 2836.

Explain if DHS is able to list out in additional detail the specific missions in which counter drone authority should apply and why DHS would prefer the current bill formulation.

Please review any concerns attached to a more limited description of mission sets.

**Response:** As described in the Administration's proposal and the draft bill, covered facilities and assets are those (1) within the United States; (2) that are identified by DHS and DOJ through a risk-based assessment in coordination with DOT; and (3) that directly relate to one of the following missions:

- United States Coast Guard and U.S. Customs and Border Protection security operations, including securing facilities, aircraft and vessels;
- United States Secret Service protection operations;
- Federal Protective Service protection of federal facilities;
- U.S. Marshals/DOJ protection of its facilities and court personnel;
- Bureau of Prisons protection of its high-risk facilities;
- Security for Special Events: National Special Security Events designated by the President at the request of the Secretary of DHS; or Special Event Assessment Rating Events
- When a state governor or attorney general requests assistance for a mass gathering event that would not otherwise fall into the security for special event category above;
- Active federal law enforcement investigations, emergency responses, or security operations carried out by DHS or DOJ; and
- Reacting to a known national security threat that could involve unlawful use of a drone.

These are the most important and prioritized mission sets that require immediate protections from unmanned aircraft system (UAS) threats. DHS and DOJ have limited resources, and we will only be able to utilize the counter-UAS (or "CUAS") authorities in this legislation when they deem the risk significant enough to warrant it and after conducting a risk assessment in coordination with DOT.

<b>Question#:</b>	9
<b>Topic:</b>	Technology Research
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Please state the extent of your authority to research, develop and operationally test counter-drone technologies.

**Response:** With appropriate protocols and permissions it is currently possible for DHS to research, develop, and operationally test most (not all) technologies used to detect and track drones. This precludes certain type of detection technology deemed most effective in urban settings to precisely geo-locate both drones and ground controllers. All mitigation technologies to stop or take over the control of drones, such as jammers/interceptors can only be developed and tested at facilities that permit these activities, typically controlled airspace in military test ranges that do not reflect operational civil environments for homeland security.

**Question:** Specifically, what counter drone capabilities has the DHS Science and Technology Directorate (S&T) been focusing on developing and delivering to operating components given current limitations?

**Response:** DHS S&T focuses on testing and evaluating commercially available off-the-shelf solutions for drone detection and tracking. Typically these include radars, optical/infrared, acoustic and radio frequency detection systems or combinations thereof. We are also working on upgrading current CUAS capabilities for the U.S. Secret Service which has limited mitigation authority; specifics are classified.

**Question:** What more would you like to do that you are prohibited from doing now?

**Response:** We need to be able to research, develop, test and evaluate full capability systems (including detection, tracking, and mitigation) in actual operational environments including urban cities, within the US.

<b>Question#:</b>	10
<b>Topic:</b>	Existing Technologies
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** S&T through the Technical Assessment of Counter UAS Technologies in Cities (TACTIC) assessed the performance and suitability of commercial counter-UAS solutions in homeland security settings. There is a large market for commercial counter drone technologies and many vendors claim to have technologies that will address the threat posed by drones.

What did the TACTIC assessments reveal about existing counter drone technologies?

**Response:** Due to current legal constraints, TACTIC only focused on systems for detection and tracking of drones. TACTIC results indicate that current commercial solutions are capable of detecting and tracking drones in simulated urban environments but with less accuracy and a higher false alarm rate as compared to their performance in wide open areas. Furthermore, these systems require constant manning and significant operator training. Single sensor types generally have shortfalls, hence solutions offering integrated multi-sensor systems together with intelligent fusion of the data would be most desirable, although few currently exist in the marketplace.

**Question:** Were any of the counter drone technologies ready for deployment?

**Response:** For detection and tracking only, several systems have demonstrated useful capabilities and could likely be deployed to address immediate needs, pending further user evaluation in actual operational conditions. These included radar, passive RF detection, and Electro-Optic systems. Most of these systems are fairly expensive, costing hundreds of thousands to millions of dollars and cannot mitigate drone threats.

**Question:** Which technologies looked the most promising?

**Response:** TACTIC was limited to drone detection and tracking systems in simulated urban settings; for this setting, several technologies appear useful. Radar has the capability to detect and accurately track nearly all types of drones at ranges of 1 kilometer or more, albeit with high false alarm rates. Systems that detect the radio traffic to and from the drone (without reading the messages themselves in order to stay within legal boundaries) can detect many types of drones and some systems can provide tracking data, although typically not as accurately as radar tracking. Optical systems operating in the visible or infrared spectra (EO/IR systems) can be used to resolve false alarms from radar when used in combination a secondary means of confirmation. Today, this usually requires a human operator but this is increasingly becoming automated. In addition,

<b>Question#:</b>	10
<b>Topic:</b>	Existing Technologies
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

small video cameras have shown some promise as local sensors for detection of below-rooftop drone flights. Since each of the sensor types listed above has advantages and disadvantages, the most promising solutions are those that utilize a combination of different sensor types all integrated into an overall capability with intelligent data fusion. These systems are emerging.

None of the commercial solutions for drone mitigation was tested nor were active RF capabilities for detection assessed to violate Title 18.

<b>Question#:</b>	11
<b>Topic:</b>	Performance Data
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Have any counter drone technologies been subjected to testing in urban environments? And what performance data are you able to access of capabilities in an urban environment?

**Response:** Within the US, there has been very limited testing in actual urban areas. There was a test of detection and tracking systems conducted by the US Army in New Orleans in April 2017 with limited quantifiable data obtained. DHS has yet to perform any testing in actual cities. Through our international collaborations, DHS was given qualitative briefs on a March 2017 test in London, UK and a November 2017 test in Tel Aviv, Israel. We are aware of tests performed in other cities, such as Seoul but cannot obtain further information. In addition, the DHS S&T-sponsored TACTIC tests collected quantitative data from a variety of detection and tracking systems in a simulated urban environment at a military training facility during August and December 2017. This data is being assessed and is providing insights regarding performance of these systems in urban environments, however true urban environments will provide additional complexities.

**Question:** What are some of the challenges and impediments associated with deploying these technologies?

**Response:** Several challenges exist regarding the development and delivering of drone capabilities to operational components. First, most agencies do not have the authority to use any sort of countermeasure against drones, whether electronic or kinetic; the testing of mitigation countermeasures is highly restrictive and can only be done in controlled, unrealistic settings. Countermeasure technologies also pose problems of their own, such as unintentional interference with electronic systems or collateral damage due to drone downing. This further speaks to the need to be able to test them in realistic operational conditions to better understand their collateral effects; then in turn develop proper regulations for their use while researching on ways to control/reduce their collateral effects, as well as closely coordinate with FAA to ensure collateral impacts can be adequately mitigated if/when used. Second, most detection and tracking systems today require constant operator supervision to assess whether a detection is a drone or something else such as a bird, and whether the drone poses a threat. Also, drones flying below rooftop level in urban areas are difficult to detect.

**Question:** What kind of threat does counter drone technology pose to other types of critical technologies already in use in avionics and other areas?

<b>Question#:</b>	11
<b>Topic:</b>	Performance Data
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Response:** Depending on the specific technology used, detection and tracking technologies generally do not pose large difficulties. Mitigation and neutralization technologies pose greater problems. Jamming of the radio command link of the drone may result in unintentional interference with other communication signals or uncontrolled flight by the target drone. Jamming of the GPS link causes interference with other systems that use GPS signals for navigation or timing. Net projectiles may fall into undesired areas, or may bring the threat drone down in undesired areas. Automated interceptor drones with tethered net guns appear to hold promise but have yet to be sufficiently matured. Interfering with the RF communications between a drone and its ground controller to take over the control of the drone is the least disruptive among all countermeasures but will not be effective against non-transmitting drones.

<b>Question#:</b>	12
<b>Topic:</b>	Securing Mass Gatherings
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** There is real concern about the private sector's ability to secure critical infrastructure and soft targets, such as mass gatherings of people. The St. Louis Cardinals are just one example of a group concerned about the safety of their game attendees. Despite temporary flight restrictions, private entities cannot mitigate drone threats.

Explain how DHS gaining authority to counter drones will help owners of critical infrastructure, state and local law enforcement and mass gathering venue operators.

Review what DHS is doing in the interim to support the private sector in their effort to protect critical infrastructure and the American public at mass gatherings.

**Response:** The security of the nation's critical infrastructure generally, and soft targets-crowded places specifically, is a top priority for DHS. Terrorists and other violent extremist actors have demonstrated an explicit interest in attacking areas that are inherently open to the general public, and by nature of their purpose do not incorporate strict security measures. This is further complicated by the increased use of low sophistication attack methods that exhibit minimal identifiable indicators. Understanding that no one entity can mitigate all risks independently, DHS – in partnership with other federal agencies, state and local governments, and the private sector – has developed a multitude of resources and capabilities that support the critical infrastructure community in enhancing security. These are executed through programs such as the Protective Security Advisory, Active Shooter Preparedness, Bombing Prevention, SAFETY Act, Special Events, and others.

Unlike other attack vectors (e.g., vehicle ramming, active shooter, bombing, bladed weapons, etc.), the potential threats posed by unmanned aircraft systems (UAS) are unique as they can have both physical and cyber implications. Moreover, the critical infrastructure community is significantly limited in the actions it can take to thwart potential nefarious use. The current legal landscape, whether determined by federal and/or state/local laws, restrict countermeasures. Although a temporary flight restriction will lessen overflight from hobbyists and those who use UAS for commercial purposes, it will not preclude a terrorist or other violent extremist actor from leveraging the technology to inflict harm during games in stadiums, special events in parks, or during other mass gathering events.

To support the critical infrastructure community in understanding the threats posed by this technology, potential resulting disruptions to operations, and the limited actions that

<b>Question#:</b>	12
<b>Topic:</b>	Securing Mass Gatherings
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

can be taken to mitigate risks, DHS developed several resources intended for owners/operators and event coordinators:

- “UAS and Critical Infrastructure – Understanding the Risk” – an instructional video that contains information on the threats posed by the nefarious use of UAS, potential implications to critical infrastructure operations, and options for risk mitigation.
- “Tips in Responding to a UAS Incident” – a pocket card that provides information on actions that security and operations officers can take if a UAS is seen operating near an infrastructure. It also contains information regarding the different types of UAS and their respective flight ranges and payload capabilities, along with quick tips on how to properly report an UAS-related incident.
- “Technology Trends in Small Unmanned Aircraft Systems and Counter UAS: A Five Year Outlook” – provides results from research pertaining to the future evolution of the technology and countermeasures.
- “UAS Frequently Asked Questions” – contains responses to the most common inquiries, ranging from how to submit for flight restrictions to whether a UAS is required to be registered.
- Website – provides access to information regarding the threat, and resources available to better inform potential risk mitigation solutions.

DHS also established a working group comprised of public and private sector partners to identify innovative methods to mitigate the risks posed by this emerging threat to critical infrastructure. Ultimately, the working group aims to advance capabilities and practices for countering the malicious use of the technology, and reduce security and public safety risk.

Using the risk based Special Events Assessment rating process DHS is able to identify the highest risk events. This risk based ranking enables the US Government to focus its efforts on those highest risk events and inform policy decisions. For all of the Level 1 and select Level 2 events the Secretary of DHS appoints a Federal Coordinator to serve as their personal representative for those events. The Federal Coordinator’s role, among others, is to assist the state and local officials fill significant capabilities shortfalls. In this capacity our Federal Coordinators are in direct contact with state and local government authorities, who are responsible for special event security, who routinely express great concern about the threat posed from drones. The existence of a special event Federal Coordinator provides a mechanism through which CUAS capabilities could be accessed and implemented.

<b>Question#:</b>	12
<b>Topic:</b>	Securing Mass Gatherings
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

While DHS's current authorities are primarily focused on informing potential risk mitigation solutions for use by the private sector, the proposed legislation would provide DHS with additional operational authorities that allow some of its law enforcement entities to more directly counter a potential threat posed by a UAS. Most pertinently, DHS would have the ability to detect, identify, track and mitigate UAS threats to covered facilities.

<b>Question#:</b>	13
<b>Topic:</b>	Special Event Designation
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Explain whether the threat posed by drones warrants the consideration of regular season games as "special events" and what issues, if any, are raised by such a designation.

**Response:** "Regular season games", if submitted to or entered by DHS, are designated special events and are assessed a Special Events Assessment Rating (SEAR). A SEAR event is defined as:

*Preplanned special events not designated as NSSEs, which have been submitted via the National Special Events Data Call. The majority of these events are state and local events that may require augmentation from the Federal Government. (PPD 8, Protection, Federal Interagency Operations Plan)*

DHS uses the risk-based Special Event Assessment Rating Methodology, a sophisticated, risk-based approach, to determine the risk of terrorist attacks on special events. Drones, as explosive device delivery systems, pose a risk to special events and are accounted for in our special event risk assessments.

Unlike other methods of attack that are assessed using the methodology where we can collaborate with federal, state and local law enforcement and security partners to employ threat mitigation capabilities, we all currently lack the authority to employ counter-drone capabilities. A provision included in S. 2836 would allow DHS or DOJ to provide assistance to state and local law enforcement, within available resources, when requested by the State Governor or Attorney General.

<b>Question#:</b>	14
<b>Topic:</b>	Private Sector Deployment
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** At this time, what are your specific concerns about the consequences of the private sector deploying counter-drone technologies?

**Response:** The private sector lacks counter-unmanned aircraft system (CUAS) authorities, just as DHS and DOJ lack these authorities. Further, we are requesting an incremental approach to countering this threat, starting with the DOD and then moving forward with federal law enforcement agencies. The inability to fully and completely evaluate the performance and impacts of available CUAS technology in the civil domestic environment continues to hinder the U.S. Government's ability to appropriately assess these impacts to ensure the consequences of their use can be mitigated or accepted. The bill's will enable DHS and DOJ to conduct testing and evaluation of technology that will inform the circumstances under which it can be safely used, in turn informing discussion of allowing additional entities—both governmental and private sector—CUAS authorities.

Growth in the unmanned aircraft system (UAS) market will continue and its adoption for commercial and recreational purposes, in the absence of additional regulatory measures, results in increased UAS encounters over critical infrastructure facilities and large public venues – and those are the non-nefarious actors. UAS technology continues to advance with increased ranges and payload capabilities for a variety of legitimate applications of benefit to the public – and will continue to evolve toward fully autonomous UAS operations. If we do not want to hinder the positive economic outcome of this technological development, we must advance security and regulatory measures in parallel.

As a result of a rapid market growth and existing legal restrictions for product testing in the United States, CUAS product development is occurring largely in foreign countries. Most CUAS technologies developed in the United States are not tested outside of a controlled laboratory environment or remote rural locations, making their capabilities in urban environments unknown. Foreign countries have ongoing and extensive testing being performed without any restrictions, and some U.S. companies are going overseas to test their products. Today, most CUAS systems are based on countering the Commercial-Off-the-Shelf (COTS) UAS that are widely known or studied, whereas custom-built UAS can easily defeat currently available systems. Customized UAS could include altered communications channels, blocking equipment, stealth designs, etc. and could be more difficult to detect and mitigate without additional research and development.

<b>Question#:</b>	15
<b>Topic:</b>	Counter Drone Authority
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The Department of Homeland Security (DHS) is the lead coordinator for National Special Security Events (NSSEs) and works with federal, state and local law enforcement to provide security. These include the Republican and Democratic National Conventions and the State of the Union. The Department of Defense (DoD) and the Department of Justice (DOJ) are partners in that effort. Counter drone authority seems critical to ensuring security at these types of events.

Since the National Defense Authorization Act for Fiscal Years 2017 and 2018 provided the DoD with counter drone authorities, explain why DOJ and DHS need these same authorities. Why isn't the authority provided to the DoD sufficient?

**Response:** In general, the DOD authorities already in statute are specific to their mission sets and operations and cannot be conferred to other Departments and Agencies.

<b>Question#:</b>	16
<b>Topic:</b>	Privacy Protections
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** There is a perception that if DHS were granted this authority that it would provide DHS with roving and ongoing authority to access stored data on the drones or some other personal device.

**Response:** Section 210G(b)(1)(A) expressly limits DHS ability to access only those communications that are used to control the unmanned aircraft. This bill is about mitigating a threat from a UAS. Mitigating the immediate threat is very different from any post-event investigation that may follow. During the identification, tracking, and mitigation process it may be necessary to access the command and control communications, but it is difficult to imagine (and the bill does not allow) collecting other types of data. After duly authorized and fully trained officers seize control, disable, redirect, interfere with, or destroy the UAS a law enforcement investigation will likely follow. During the investigation law enforcement officers would likely seek other types of data (not related to command and control), but accessing such data would be covered by the Fourth Amendment and other laws relevant to criminal investigations.

**Question:** Please review the privacy protections in S. 2836, how DHS would implement those protections and limitations to DHS infringements on privacy.

**Response:** Before a single step is taken to implement this new authority, the DHS Chief Privacy Officer will “assure that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information,” as stipulated in Section 222 of the Homeland Security Act of 2002. To do so, the authorized CUAS component operators would file a Privacy Threshold Assessment (PTA)—which is required for operating any technology or system that may have privacy implications—with the DHS Privacy Office. A privacy analyst would then determine if a new Privacy Impact Assessment (PIA) is necessary to mitigate any possible privacy risks. In addition, the privacy analyst would also determine whether an existing Privacy Act System of Records Notice (SORN) applies or if a new SORN must be drafted. The DHS Chief Privacy Officer may require privacy protections beyond those required by S. 2836 if he or she believes additional measures are necessary to protect individuals’ privacy.

Review by the DHS Privacy Office is not a one-time event, but instead part of the lifecycle of the program or technology. Privacy Office analysts review all SORNs biennially and review all PIAs triennially. Furthermore, the Privacy Office routinely conducts Privacy Compliance Reviews to ensure that DHS programs operate in a manner consistent with applicable SORNs and PIAs, and to examine whether mitigation

<b>Question#:</b>	16
<b>Topic:</b>	Privacy Protections
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

strategies that have been developed at the inception of a program work in operation or practice. Finally, anyone who believes that DHS has violated his or her privacy rights may submit a complaint to the Chief Privacy Officer, who has broad investigative authority to investigate issues, even when the OIG has declined to investigate.

All of these authorities, processes, and procedures apply beyond the privacy requirements of S. 2836. The bill's requirement that intercepting, acquiring, or accessing communications between the UAS and the controller are only allowed when it is necessary to support a function of DHS mirrors existing DHS privacy policy, which stipulates that DHS must follow the Fair Information Practice Principles at all times. In terms of data retention, DHS already limits retention of data acquired during UAS operations to 180 days and would similarly restrict data retention in CUAS privacy compliance documentation.

DHS's Office of General Counsel and the Office for Civil Rights and Civil Liberties also exercise oversight authorities that would apply to DHS use of CUAS technologies. The DHS Privacy Office routinely works with these offices to ensure that DHS abides by the Constitution, the law, and DHS policy when conducting its missions.

**Question:** Please explain how DHS interprets the transparency requirements in the bill.

**Response:** DHS will make available to the public all applicable Privacy Impact Assessments, Systems of Record Notices, and privacy guidance related to CUAS without disclosing classified or operationally sensitive information. In addition, the DHS Privacy Office would include in the required semi-annual reports all outreach efforts specific to the privacy implications of DHS use of its CUAS authorities, instances of alleged violations of individuals' privacy, and any subsequent steps taken to ensure that DHS's CUAS operation stands by its commitments to privacy.

**Question:** Please outline your interpretation of the limitations on the interception and use of electronic communications in S. 2836?

**Response:** S. 2836 restricts the interception of electronic communications to only those communications between the controller and the aircraft used to control the aircraft and only to the extent necessary to mitigate the threat posed by that aircraft to the safety or security of covered facilities and assets. The bill does not authorize DHS to collect or access any other communications to or from the controller for any reason.

<b>Question#:</b>	17
<b>Topic:</b>	Operator Intent
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** FAA testimony mentioned the need to identify drones and their operators in order to differentiate between "the clueless, the careless, and the criminal."

Does DHS believe that drone operator intent needs to be determined prior to conducting any counter drone activity?

Does DHS consider determination of a drone operator's intent as a key factor in its actions concerning management of drone safety risks?

**Response:** Operator intent is a very important factor when determining if there is a need to mitigate an unmanned aircraft system (UAS) threat, as well as how that threat can be mitigated using our authorized authorities and capabilities. While it is important to understand the operator's intent, it would not be explicitly necessary before our authorized officers and agents utilized counter-UAS capabilities to mitigate a threat. Once authorized DHS and DOJ personnel have determined that there is a threat from a UAS, those authorized personnel would be permitted to use the necessary force to mitigate that threat.

One area of significant concern is the inherent public safety risk of drone operation above or around special events and mass gatherings. The unauthorized operation of UA, above a large crowd, could pose a public safety risk to individuals should the UAS crash into the crowd due to operator error or manufacturing defects that are not yet regulated.

<b>Question#:</b>	18
<b>Topic:</b>	Discerning
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** How do you plan to discern authorized drones from unauthorized drones in real time, in the absence of a comprehensive remote identification requirement?

**Response:** Currently, unlike manned aviation, there is no remote identification requirement for unmanned aircraft systems (UAS), nor is there a UAS traffic management system in place. The Federal Aviation Administration is pursuing both capabilities to help integrate UAS into the National Airspace System (NAS), and DHS supports both concepts to make it easier for law enforcement personnel to discern legitimate and commercial UAS traffic in the NAS. In the absence of these capabilities, law enforcement personnel are left with few options to discern what is legitimate and what is unauthorized. Under the current legal construct, if a UAS is determined to be a threat, then DHS and DOJ personnel can act to ensure that threat is appropriately mitigated using conventional law enforcement methods and techniques. With the authorities requested in the Administration's proposal and the introduced bill, DHS would be able to utilize counter-UAS technologies that can detect, track and, if necessary, help mitigate a threat from a malicious or unauthorized UAS.

<b>Question#:</b>	19
<b>Topic:</b>	Repealing Section 336
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** To that end, do you support the repeal of Section 336 of the FAA Modernization and Reform Act so that you can require remote identification for all drones over a certain weight threshold?

**Response:** DHS is supportive of the efforts to ensure there is a level playing field for all UAS operators in the National Airspace System (NAS), to include the registration, operation, and identification of all unmanned aircraft systems (UAS) flown for commercial and recreational purposes.

**Post-Hearing Questions for the Record  
Submitted to Hon. David Glawe and Haley Chang  
From Senator Rand Paul**

**“S. 2836 – the Preventing Emerging Threats Act of 2018: Countering Malicious Drones”**

**June 6, 2018**

<b>Question#:</b>	20
<b>Topic:</b>	Determining a Threat
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Rand Paul
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** S. 2836 authorizes the Secretary of Homeland Security and the Attorney General to empower select DHS and Department of Justice (DOJ) personnel to "mitigate the threat" posed by unmanned aircraft systems (UAS) or unmanned aircraft.

Does the bill's language in any way limit or prohibit the Secretary of DHS or the Attorney General from determining that all UAS or unmanned aircraft pose a potential threat?

**Response:** The draft legislation specifically authorizes DHS and DOJ personnel to take only necessary actions to mitigate the threat from UAS. While we understand that not all UAS flying in the national airspace are threatening and many will continue to operate for legitimate commercial purpose, the draft legislation allows both Departments to take necessary actions to protect the American public from UAS threats. The threat definition and scope will be defined by DHS and DOJ in coordination with DOT, and will include a number of factors, such as: the potential for bodily harm or loss of human life; the potential loss or compromise of sensitive national security information; or the potential severe economic damage resulting from use of a UAS in the vicinity of a covered facility or asset. The final definition of threat will be determined and approved by the Secretary once the necessary consultation with DOT has been completed.

<b>Question#:</b>	21
<b>Topic:</b>	Limiting Coverage
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Rand Paul
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** S. 2836 authorizes the Secretary of Homeland Security and the Attorney General to define "covered facility or asset" through a risk-based assessment process.

Does the bill's language in any way limit or prohibit the Secretary of DHS or the Attorney General from identifying every DHS or DOJ facility (including every federal courthouse, corrections facility and/or port of entry) as a covered facility or asset?

**Response:** The legislation requires a risk based approach, and evaluation of which covered facility assets requires protection, and requires consultation with the DOT. Also, due to the cost of these capabilities and other limited resources, the Department could not practically or operationally include every federal facility associated with the Department.

**Question:** Does the bill's language in any way limit or prohibit the Secretary of DHS from identifying the entire 100-mile "border zone" as a covered facility or asset?

**Response:** DHS and DOJ will be required to assess what covered assets and facilities within the bill's authorized mission sets will be prioritized to receive counter-unmanned aircraft system (CUAS) protections. Not all DHS or DOJ covered assets and facilities will require CUAS protections, which includes the entire U.S. borders. Determination of what would be covered will be done based upon the threat and risk UAS pose to certain facilities and assets. Further, both Departments have limited resources and we would not be in a position to apply CUAS protections for every DHS or DOJ owned asset or facility. Decisions will be based on threat and risk assessment, which will evolve over time and we will constantly need to address the threat to our covered assets and facilities to ensure we are adapting to counter the threat from malicious use of UAS.

<b>Question#:</b>	22
<b>Topic:</b>	Assessing the Harm
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Rand Paul
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** S. 2836 authorizes the Secretary of Homeland Security and the Attorney General to "[u]se reasonable force to disable, damage, or destroy the unmanned aircraft system or unmanned aircraft."

Does the bill's language in any way require DHS or DOJ personnel, before downing or destroying a UAS or unmanned aircraft, to assess the potential harm such actions may cause to life and property in the vicinity of the target or on the ground below?

**Response:** DOJ and DHS will make every effort to avoid any such harm to life and property when mitigating a threat from an unmanned aircraft system (UAS) via the utilization of counter-UAS (CUAS) authorities. The Administration's legislative proposal and this bill permits these activities within a highly regulated framework with oversight from multiple federal departments, including DOJ, DHS, and DOT. While this authority does provide for relief from Title 18 provisions that might otherwise constrict legitimate activity, it is not a blank check for conducting CUAS operations. It is important to remember that bill exempts activities "necessary to mitigate the threat" from Title 18. If the operator's actions were not necessary to mitigate the threat, one would imagine that (s)he could still be prosecuted for involuntary manslaughter, if it were otherwise appropriate under the circumstances. DOJ and DHS take seriously the obligation to comply with the Constitution and with the ordinary rules of tort liability. The legislative proposal reflects that core commitment. But like any other law enforcement or protective activity of DHS and DOJ, there is always the possibility that actions could be unreasonable under the circumstances.

...

<b>Question#:</b>	23
<b>Topic:</b>	Judicial Review
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Rand Paul
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** S. 2836 authorizes the Secretary of Homeland Security and the Attorney General to "[u]se reasonable force to disable, damage, or destroy the unmanned aircraft system or unmanned aircraft."

Does the bill's language contemplate any process by which the actions of DHS or DOJ personnel may be subject to judicial review?

Does the bill's language contemplate any process by which a UAS or unmanned aircraft operator might challenge the lawfulness or appropriateness of the actions taken by DHS or DOJ personnel?

**Response:** DHS and DOJ take seriously the obligation to uphold Constitutional protections. That obligation would apply to every activity conducted under this proposal. As a practical matter, before operating this capability in a particular location, the Departments will work with DOT to ensure appropriate notice is provided to unmanned aircraft system (UAS) operators. Notice will reduce the risk of unauthorized UAS activity in a protected airspace. Moreover, the proposed statutory framework contains a number of protections designed to protect privacy and civil liberties. Additionally, the proposed legislation only authorizes actions "necessary to mitigate" a threat to the safety or security of a covered facility or asset. Lawfully conducted news gathering activities in lawfully accessible airspace would not pose such a threat to the safety or security of a protected facility or asset. Finally, all law enforcement actions authorized in the proposed bill must comply with traditional Fourth Amendment principles.

<b>Question#:</b>	24
<b>Topic:</b>	Seizing Property
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Rand Paul
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** S. 2836 authorizes the Secretary of Homeland Security and the Attorney General to “seize or otherwise confiscate the unmanned aircraft system or unmanned aircraft” as well as to “[u]se reasonable force to disable, damage, or destroy the unmanned aircraft system or unmanned aircraft.”

Would the seizure or destruction of private property under this Act by DHS or DOJ violate the Fifth Amendment to the U.S. Constitution? Why or why not?

**Response:** Due process, particularly where property is destroyed, would ordinarily require a hearing or some other procedure before a person is deprived of property. However, case law recognizes that in exigent circumstances (such as those presented by UAS activities falling within the scope of S. 2386), the government may act first and provide sufficient post-deprivation process to satisfy Fifth Amendment requirements. Because, as explained below, nothing in S. 2836 purports to limit any available remedies to UAS owners who challenge or seek compensation for a seizure or other deprivation of property under this provision, the seizure or destruction of property in exigent circumstances under S. 2836 would not violate due process requirements.

**Question:** S. 2836 authorizes the Secretary of Homeland Security and the Attorney General to seize and control “unmanned aircraft systems” without a warrant. These systems include “communication links and the components that control the unmanned aircraft.”

Would smartphones and personal computers that control unmanned aircraft be considered “unmanned aircraft systems”?

**Response:** Although a smartphone or a computer may be considered a part of the unmanned aircraft system, the authority under S. 2836 is limited to interception of communications between the drone and its controlling device that is necessary to mitigate the threat. As noted below, any “seizure” of property or persons must adhere to the Fourth Amendment’s general reasonableness requirement.

**Question:** Would the DHS or DOJ be able to seize and control such devices without a warrant under this Act?

**Response:** Any federal effort to counter UAS that involves or requires a “seizure” of property or persons must adhere to the Fourth Amendment’s general reasonableness

<b>Question#:</b>	24
<b>Topic:</b>	Seizing Property
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Rand Paul
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

requirement. All of the limits on unlawful searches and seizures still apply (as emphasized in subsection on “Privacy Protection.”).

**Question:** Could records of communication to or from such a device or other data collected with authority under this Act be used to support warrants, arrests, or indictments unrelated to threats presented by unmanned aircraft?

**Response:** S. 2386 only authorizes DHS and DOJ to intercept communications between the drone and its controlling device, not data stored on the device. Additionally, that interception is authorized only to the extent necessary to mitigate the threat. To collect any data after the immediate threat is over would require separate, standard processes in place in existing law (e.g. warrant, court order). Finally, under provisions of S. 2386, records cannot be retained for more than 180 days unless there are extenuating circumstances (enumerated exceptions set forth in the bill). As is the case in all law enforcement investigations, the very limited data that is collected between the drone and the controlling device can be used for other law enforcement purposes and need not be ignored if relevant to other potential violations of law.

**Question:** S. 2836 gives the Secretary of Homeland Security and the Attorney General broad authority to seize and control expensive personal property. The American people have an interest in understanding how government will invoke this authority.

What recourse will the public have if DHS or DOJ mistakenly seizes, controls, or destroys a system not related to unmanned aircraft, perhaps due misattribution of a controlling device or misidentification of wire, oral, electronic, or radio communications protocols?

**Response:** Congress has provided generally applicable rules and procedures for lawful forfeiture actions in Title 18, Section 983. Those rules would apply to forfeitures that take place under this proposal. That statute entitles those whose property was seized to challenge the action in court. It also requires the government to follow certain procedures, such as providing notice of a seizure. Under those rules and procedures, the burden is always on the government to prove (1) a crime occurred and (2) that property is connected to that crime. The government needs probable cause to seize property – the same standard the Constitution requires to arrest someone. We also note that the legislative proposal makes on attempts to shield liability that would otherwise be appropriate under the Federal Tort Claims Act.

<b>Question#:</b>	25
<b>Topic:</b>	Rights of Private Citizens
<b>Hearing:</b>	S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones
<b>Primary:</b>	The Honorable Rand Paul
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** S. 2836 authorizes the Secretary of Homeland Security and the Attorney General to “[u]se reasonable force to disable, damage, or destroy the unmanned aircraft system or unmanned aircraft.” The Department of Defense and the Department of Energy enjoy similar authorities.

What course or courses of action are available to private U.S. citizens to mitigate the threat posed by an unknown UAS or unmanned aircraft on their property, if that UAS or unmanned aircraft presents a threat to the individual’s life, property, or privacy?

**Response:** Federal law may subject citizens who willfully damage or disable a drone to criminal sanctions of the Aircraft Sabotage Act. A person who perceives that a drone presents a threat, should contact law enforcement or the FAA.



U.S. Department of Justice

Office of Legislative Affairs

---

Office of the Assistant Attorney General

Washington, D.C. 20530

SEP 19 2018

The Honorable Ron Johnson  
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 FBI Assistant Director Scott Brunner before the Committee on June 6, 2018, at a hearing entitled "S. 2836 — the Preventing Emerging Threats Act of 2018: Countering Malicious Drones."

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

Sincerely,

A handwritten signature in cursive script that reads "Prim Escalona".

Prim F. Escalona  
Principal Deputy Assistant Attorney General

Enclosure

cc: The Honorable Claire McCaskill  
Ranking Member

RESPONSE OF  
SCOTT BRUNNER  
DEPUTY ASSISTANT DIRECTOR  
FEDERAL BUREAU OF INVESTIGATION  
DEPARTMENT OF JUSTICE

TO QUESTIONS FOR THE RECORD  
ARISING FROM A HEARING ENTITLED  
“S. 2836 – THE PREVENTING EMERGING THREATS ACT OF 2018: COUNTERING MALICIOUS  
DRONES”

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

JUNE 6, 2018

Questions from Senator Paul

1. S. 2836 authorizes the Secretary of Homeland Security and the Attorney General to empower select Department of Homeland Security (DHS) and DOJ personnel to “mitigate the threat” posed by unmanned aircraft systems (UAS) or unmanned aircraft.

**Question:** Does the bill’s language in any way limit or prohibit the Secretary of DHS or the Attorney General from determining that all UAS or unmanned aircraft pose a potential threat?

**Response:** Yes. Recognizing that many UAS are flown for legitimate recreational or commercial uses, the bill narrowly tailors the government’s use of counter-UAS (C-UAS) technologies to detect and mitigate UAS operations that pose a threat to the safety or security of a covered facility or asset. First, the bill places significant limitations on DOJ and DHS to ensure the Departments prioritize only the most sensitive and essential government facilities and assets for protection. Each covered facility or asset must relate to a specified mission set of the Department and pass through a rigorous risk-based assessment conducted by the Attorney General or the Secretary of Homeland Security in consultation with the Secretary of Transportation.

Second, DHS and DOJ personnel may take only those actions “necessary to mitigate” the threat posed by a particular UAS under the circumstances. DOJ and DHS must coordinate the definition of “threat” with DOT, which will likely be influenced by a number of factors, such as: the potential for bodily harm or loss of human life; the potential loss or compromise of sensitive national security information; the potential loss or compromise of a sensitive government investigative, intelligence collection capability

or evidence in the investigation or prosecution of a significant case to the public safety or national security; or the potential severe economic damage resulting from the malicious or reckless use of a UAS in the vicinity of a covered facility or asset. Assessing whether a particular UAS poses a threat to a covered facility or asset does *not* permit a blanket determination that all UAS in proximity present a threat; rather, it requires a case-by-case determination made by federal law enforcement officers at the scene based on the totality of the circumstances.

Third, the bill requires DHS and DOJ to coordinate with the Secretary of Transportation and the Administrator of the Federal Aviation Administration before issuing any guidance, or otherwise implementing the authorities, if such guidance or implementation “*might* affect aviation safety, civilian aviation and aerospace operations, aircraft worthiness, or the use of airspace.” That broad-based requirement to coordinate implementation activities with DOT and FAA ensures that the authority will facilitate—rather than impede—the safety and efficiency of the national airspace system.

Finally, the bill ensures constrained use of the authority by mandating the issuance of guidance and providing for robust congressional oversight. Among other things, DOJ and DHS are required to brief the appropriate committees of jurisdiction, with DOT, every six months on instances in which C-UAS action has been taken, as well as policies and procedures that affect privacy, civil rights, or civil liberties.

2. S. 2836 authorizes the Secretary of Homeland Security and the Attorney General to define “covered facility or asset” through a risk-based assessment process.

**Question:** Does the bill’s language in any way limit or prohibit the Secretary of DHS or the Attorney General from identifying every DHS or DOJ facility (including every federal courthouse, corrections facility and/or port of entry) as a covered facility or asset?

**Response:** Yes. The bill does *not* permit the Secretary or Attorney General to identify for protection every DHS or DOJ facility or asset—far from it. The facilities or assets eligible for protection must be tied to a specific DHS or DOJ mission authorized by the bill, and be conducted consistent with governing statutes, regulations, and orders for the agencies concerned. In many cases, the particular mission set or facility must also be assessed to be high-risk or a target for unlawful unmanned aircraft activity.

Importantly, the legislation also requires the Secretary or Attorney General to conduct a rigorous risk-based assessment with the Secretary of Transportation in the course of identifying a particular facility for protection. As part of this assessment, the bill requires a careful evaluation of multiple factors with respect to potential impacts on the safety and efficiency of the national airspace before a facility or asset can be designated for C-UAS protection. These limitations ensure that DHS and DOJ will deploy the authority incrementally and on a risk-based basis.

3. S. 2836 authorizes the Secretary of Homeland Security and the Attorney General to identify “active Federal law enforcement investigations, emergency responses, or security operations” as a “covered facility or asset.” The U.S. Border Patrol and the U.S. Coast Guard conduct security operations around-the-clock.

**Question:** Does the bill’s language in any way limit or prohibit the Secretary of DHS from identifying the entire 100-mile “border zone” as a covered facility or asset?

**Response:** The FBI defers this question to DHS because Customs and Border Protection is a DHS component.

4. S. 2836 authorizes the Secretary of Homeland Security and the Attorney General to “[u]se reasonable force to disable, damage, or destroy the unmanned aircraft system or unmanned aircraft.”

**Question:** Does the bill’s language in any way require DHS or DOJ personnel, before downing or destroying a UAS or unmanned aircraft, to assess the potential harm such actions may cause to life and property in the vicinity of the target or on the ground below?

**Response:** Before a facility or asset is even designated for protection, the Secretary or Attorney General must evaluate—in coordination with DOT—the potential consequences of the impacts of any C-UAS action taken to the national airspace system and infrastructure, as well as the setting and character of any covered facility or asset, including whether it is located in a populated area or near other structures. DOT, and specifically the FAA, will identify aviation safety risks and work with DHS and DOJ to mitigate those risks and ensure compliant aircraft are not impacted. The bill also expressly requires any use of force by DOJ or DHS to be “necessary.” Such actions are also governed by the Fourth Amendment to the United States Constitution and by case law, which requires the use of force to be “reasonable,” assessed under the totality of the circumstances. Use of force encounters require an assessment by the officer or agent of the potential collateral impact of the use of force on bystanders, and this bill does not change that requirement.

In accordance with our Constitutional obligations, and consistent with the duty we have as law enforcement to protect and defend the American people, DOJ and DHS will make every effort to avoid any inadvertent harm to life or property when mitigating a threat from an unmanned aircraft system (UAS), as the purpose of this bill is not just to counter UAS but to protect life and property threatened by UAS.

Moreover, this legislation does not protect operators from civil liability resulting from harm to persons or property. DOJ and DHS take seriously the obligation to comply with the Constitution and with the ordinary rules of tort liability. The legislative proposal reflects that core commitment.

5. S. 2836 authorizes the Secretary of Homeland Security and the Attorney General to “[u]se reasonable force to disable, damage, or destroy the unmanned aircraft system or unmanned aircraft.”

**Question:** Does the bill’s language contemplate any process by which the actions of DHS or DOJ personnel may be subject to judicial review?

**Question:** Does the bill’s language contemplate any process by which a UAS or unmanned aircraft operator might challenge the lawfulness or appropriateness of the actions taken by DHS or DOJ personnel?

**Response:** While this authority does provide for relief from Title 18 provisions that might otherwise constrict legitimate activity, it by no means a blank check for conducting C-UAS operations. It is important to remember that the bill exempts from Title 18 only those activities “necessary to mitigate the threat.” If the operator’s actions were not “necessary,” the operator could potentially be held criminally liable for her actions.

In addition, this legislation does not protect operators from civil liability that would otherwise be appropriate resulting from harm to persons or property. DOJ and DHS take seriously the obligation to comply with the Constitution and with the ordinary rules of tort liability. Moreover, this proposal does not excuse operators from complying with the Constitution or from complying with federal statutes not listed in Section (a) of the bill.

6. S. 2836 authorizes the Secretary of Homeland Security and the Attorney General to “seize or otherwise confiscate the unmanned aircraft system or unmanned aircraft” as well as to “[u]se reasonable force to disable, damage, or destroy the unmanned aircraft system or unmanned aircraft.”

**Question:** Would the seizure or destruction of private property under this Act by DHS or DOJ violate the Fifth Amendment to the U.S. Constitution? Why or why not?

**Response:** It would not, because the seizure is authorized by the statute only as “necessary to mitigate the threat . . . that an unmanned aircraft system or unmanned aircraft poses to the safety or security of a covered facility or asset.” The government’s urgent need to mitigate the threat posed by a UAS in those specific circumstances make before-the-fact due process practically impossible, and the Constitution does not require that before-the-fact process when the exigency is present.

7. S. 2836 authorizes the Secretary of Homeland Security and the Attorney General to seize and control “unmanned aircraft systems” without a warrant. These systems include “communication links and the components that control the unmanned aircraft.”

**Question:** Would smartphones and personal computers that control unmanned aircraft be considered “unmanned aircraft systems”?

**Response:** Although a smartphone or a computer may in certain cases be considered part of the unmanned aircraft system, the authority under S. 2836 is limited to interception of communications between the drone and its controlling device—not data stored on the device—that is necessary to mitigate the threat. The statute provides that any data intercepted must be deleted after six months, unless an exception applies. Further, because the bill only provides authority “necessary to mitigate the threat,” DOJ and DHS may not rely on this authority to conduct further investigation once the threat has been mitigated. As noted below, any “seizure” of property must adhere with the Fourth Amendment, including the warrant requirement.

**Question:** Would the DHS or DOJ be able to seize and control such devices without a warrant under this Act?

**Response:** No. This Act would not change the law governing whether the government can seize and control such devices. Any federal effort to counter UAS that involves or requires a “seizure” of property must comply with the Fourth Amendment. Clearly, a statute cannot authorize the government to do something that the Fourth Amendment prohibits.

**Question:** Could records of communication to or from such a device or other data collected with authority under this Act be used to support warrants, arrests, or indictments unrelated to threats presented by unmanned aircraft?

S. 2386 only authorizes DHS and DOJ to intercept communications between the drone and its controlling device, not data stored on the device. Additionally, interception is authorized only to the extent “necessary” to mitigate the threat. Finally, records of communications cannot be retained for more than 180 days, unless an exception applies. As is the case in all law enforcement investigations, the very limited data that is collected between the drone and the controlling device can be used for other law enforcement purposes and need not be ignored if relevant to other potential violations of law.

8. S. 2836 gives the Secretary of Homeland Security and the Attorney General broad authority to seize and control expensive personal property. The American people have an interest in understanding how government will invoke this authority.

**Question:** What recourse will the public have if DHS or DOJ mistakenly seizes, controls, or destroys a system not related to unmanned aircraft, perhaps due misattribution of a controlling device or misidentification of wire, oral, electronic, or radio communications protocols?

**Response:** The bill leaves in place remedies that any person would have when their property is unlawfully seized or destroyed by the federal government, including the Federal Tort Claims Act. Precisely what remedies would be available in a given situation is a fact-specific inquiry.

9. S. 2836 authorizes the Secretary of Homeland Security and the Attorney General to “[u]se reasonable force to disable, damage, or destroy the unmanned aircraft system or unmanned aircraft.” The Department of Defense and the Department of Energy enjoy similar authorities.

**Question:** What course or courses of action are available to private U.S. citizens to mitigate the threat posed by an unknown UAS or unmanned aircraft on their property, if that UAS or unmanned aircraft presents a threat to the individual’s life, property, or privacy?

**Response:** Landowners have legal rights to privacy and to enjoy their property free from nuisance, trespass, or interference. Currently, however, if a landowner were to defend their property from threats posed by UAS, they could conceivably face criminal or civil penalties.

#### Questions from Senator McCaskill

*Please feel free to provide responses in a separate classified submission where necessary.*

#### The Threat Posed By Drones

- i. Based on where terrorists and malicious actors have used drones for overseas, what is the probability that drones will be used by terrorists in the U.S. in the next few years?

**Response:** We assess with high confidence that terrorists overseas will continue to use small UAS to advance nefarious activities and exploit physical protective measures. While there has been no *successful* malicious use of UAS by terrorists in the United States to date, terrorist groups could easily export their battlefield experiences to use weaponized UAS outside the conflict zone. We have seen repeated and dedicated efforts not only by terrorist organizations, such as ISIS and Al Qa’ida, but also transnational criminal organizations such as MS-13 and Mexican drug cartels, which may encourage use of this technique in the United States to conduct attacks. FBI analysts assess with high confidence that, given their retail availability, lack of verified identification requirement to procure, general ease of use, and prior use overseas that UAS will be used to facilitate an attack in the United States, most likely against a mass gathering. This risk has only increased in light of the publicity associated with the apparent attempted assassination of President Maduro using explosives-laden UAS.

It is important to note that we have already disrupted a plan in the United States to use a drone to attack the Pentagon and the Capitol. On November 1, 2012, Rezwan Ferdaus was sentenced to 17 years in prison for attempting to conduct a terrorist attack and providing support to al-Qa'ida. Among his various plans, Ferdaus desired to use a remote-controlled, jet powered model fixed-wing aircraft, fill it with explosives, and send the unmanned aircraft into the Pentagon or Capitol using a built-in GPS system. The FBI was fortunate to have interrupted the plot by learning of it and deploying an undercover agent.

Additionally, reports of suspicious UAS encounters near sensitive locations, critical infrastructure, mass gatherings, and in close proximity to active law enforcement operations occur with alarming and rapidly increasing frequency. We assess with high confidence that reports of UAS encounters within the United States will continue to rise as these systems continue to gain popularity with recreational and commercial users. Since 2012, there has been a notable increase in reporting of UAS operations near or over critical infrastructure based on a review of data from federal, state, local, private and open source reporting.

2. How imminent is the threat and why must the Department of Justice (DOJ) gain counter drone authorities now?

**Response:** In addition to the information provided in question 1 above, the malicious use of drones presents a grave and growing threat to national security and public safety. That threat manifests itself in three primary areas: counterterrorism, counterintelligence, and criminal activity.

Overseas, ISIS and other terrorist groups use commercially available UAS to drop explosive payloads and conduct illicit surveillance. In Japan, drones were successfully used to place radioactive material on the roof of the Prime Minister's office without detection. Precision agricultural spraying drones are easily obtained domestically and provide an ideal delivery vehicle for a chemical, biological or radiological attack.

We have seen that the use of UAS by terrorists and criminals is no longer confined to the Middle East—the threat is marching closer to our own shores. Last fall, from a counterterrorism perspective, two incidents occurred that caused grave concern. First, an individual in the San Francisco Bay area was able to overfly two NFL games, notwithstanding the Temporary Flight Restrictions in place, and use commercially available UAS to drop leaflets over the crowds. While they were only leaflets, if a terrorist replaced the payload with an explosive, a WMD, or even baby powder instead of leaflets, it could have caused mass panic or resulted in a devastating attack against the soft target of a mass gathering of people. Second, an Army Blackhawk helicopter supporting a National Security Special Event, also with a Temporary Flight Restriction in place, was struck by a drone, causing hundreds of thousands of dollars in damage and forcing an emergency landing. The recent apparent, attempted assassination of President

Maduro in Venezuela using weaponized UAS, and a number of instances of weaponized UAS being used by drug cartels in Mexico, cause us concern that those tactics will be replicated in the US.

The FBI's Counterintelligence Division also assesses with high confidence that there is a significant risk that foreign adversaries will take advantage of the permissive domestic environment to conduct espionage against US persons and sensitive facilities with UAS. There is open source reporting that researchers have successfully used drones to hack into air-gapped computers, as well as "Internet of Things" devices. Malicious actors could utilize UAS in order to wirelessly exploit access points and unsecured networks and devices. This can include using UAS to inject malware, execute malicious code, and perform man-in-the-middle attacks. UAS can also deliver hardware for exploiting unsecured wireless systems. UAS are uniquely able to easily overcome traditional perimeter defenses. In normal security situations, law enforcement personnel can establish protective measures, such as physical security and access controls, to protect sensitive locations and assets. But that is simply not the case with drones, which are able to successfully avoid or defeat traditional physical security and area denial measures to access areas that people, cars, or other mobile devices cannot.

The potential criminal use of UAS also presents serious challenges. For instance, criminals are currently using UAS to drop contraband inside federal prisons and deliver narcotics across the southern border. As access to drones and understanding of their capabilities continue to increase, DOJ expects those threats to increase. The FBI has also experienced criminals using UAS to both conduct counter-surveillance against FBI personnel, and to interfere with FBI tactical operations.

3. Please provide examples of where drones have been used by terrorists in the past 18 months overseas and efforts to use drones within the U.S., the type of drones used, locations and targets, and the availability to the general public of the drone technology used.

**Response:** Some examples of recent UAS risks include: recklessly flying UAS near major airports and critical infrastructure; intentionally flying drones over special events where mass gatherings are occurring; intentionally conducting surveillance and counter surveillance of law enforcement; and facilitating kinetic attacks on stationary or mobile, high-consequence targets.

Domestically, criminals, including Mexican transnational criminal organizations, are increasingly using UAS to deliver narcotics across the United States' southern border, conduct illicit surveillance, avoid U.S. law enforcement, introduce dangerous contraband into federal prisons, and interfere with ongoing law enforcement operations. In addition, reports of the weaponization of UASs in Mexico are cause for concern. In July 2018, for example, a UAS carrying two grenades landed on the property of a Mexico state security chief in an attack likely conducted by Mexican organized crime elements, and likely meant as a warning to the security chief. While the grenade safety pins were still in place

and there was no additional means to activate the grenades, this incident demonstrated how UAS can be used to target and access specific individuals or public figures while evading traditional perimeter and physical security measures. On August 5, 2018, in Venezuela, two DJI Matrice 600 platforms were used in an apparent attempted assassination of President Maduro at an open air assembly and parade where multiple bystanders on the ground were injured.

In September 2017, a DJI Phantom 4 drone crashed into the main rotor of a New York Army National Guard Black Hawk helicopter that was providing security support for the UN General Assembly meeting, a National Security Special Event with a Temporary Flight Restriction in place. While not connected to a terrorist intent, the UAS nevertheless caused hundreds of thousands of dollars in damage to the Black Hawk, and reduced the air support capability of the UNGA security force.

In November 2017, a DJI Mavic was used to drop leaflets over two NFL stadiums (San Francisco and Oakland, CA) during games. This kind of activity, whether malicious or not, poses a very significant public safety risk. Had the operator decided to drop explosives or WMD instead of leaflets (or even a suspicious-looking white powder), numerous people could have been killed or injured.

4. Provide a few clear examples where drones have impeded your ability to carry out your critical missions and instances in which you would have used counter-drone authority if you had had it.

**Response:** As discussed above, criminals are currently using UAS to drop contraband inside federal prisons and deliver narcotics across the southern border. Criminals have also used UAS to conduct counter-surveillance against FBI personnel and use that information to interfere with FBI tactical operations. In one particularly egregious situation, defendants used a commercial drone as a counter-surveillance platform to collect intelligence on the FBI's elite Hostage Rescue Team (HRT), which was preparing to conduct a high-risk, high-threat tactical entry. The individuals used the drones and video footage to identify HRT agents in observation posts and frustrate their activities. Additionally, a hobbyist used a UAS to film FBI personnel staging outside the location, and posted the video on YouTube.

UAS also present a threat to DOJ and FBI facilities. For instance, every FBI field office has reported suspicious UAS activity in the vicinity of the field office, including UAS flying along the building line to look inside windows, or overflying sensitive areas that designed to protect sensitive assets from public view, including parking areas for undercover or covert vehicles, and training areas for our Hostage Rescue Team.

The proposed legislation is necessary to enable DOJ and FBI to provide protection from UAS used to threaten the security of sensitive facilities and operations.

5. How many incidents have you documented of unauthorized drones posing a threat to DOJ related missions?

**Response:** At this time, the FBI is not able to provide detailed statistics specific to DOJ missions due to the nature of the UAS threat, and the challenges in detecting UAS with the unaided senses, given the current legal limitations. Against that backdrop, there are concerns that any current data is under-inclusive and incomplete.

6. Besides the violation of federal law, please explain the concerns attached to simply taking down a drone.

**Response:** DOJ and DHS require urgent legislative authority to counter the growing threat posed by unmanned aircraft systems (UAS). Specifically, DOJ and DHS need a tailored grant of Counter-UAS (CUAS) authority to detect, track, and mitigate threats posed by UAS to the security of sensitive facilities and assets. Without this mandate, DOJ and DHS are unable to develop and operate many of the most effective CUAS technologies.

S. 2836/H.R. 6401 would provide DOJ and DHS the ability to develop the necessary technology and deploy it in support of certain, narrow missions to mitigate the range of threats from small UAS. With approval of this authority, which resembles the authority Congress granted DOD and DOE, Congress would reduce risks to public safety and national security, help to accelerate the safe integration of UAS into the National Airspace System (NAS), and ensure the United States remains a global leader in UAS innovation.

Further, any legislative proposal must contain robust measures designed to protect privacy and civil liberties, as S. 2836/H.R. 6401 does. The legislation makes clear that CUAS activities must comply with the Fourth Amendment to the Constitution and applicable federal laws. In addition, the legislation requires DOJ and DHS to issue guidance that, among other things, limits the collection and acquisition of communications to and from the drone only to the extent necessary to mitigate the threat posed by the UAS.

S. 2836 requires close coordination and collaborative risk analysis with the Federal Aviation Administration (FAA) to ensure any deployment of CUAS technologies in the NAS is conducted safely, minimizes the potential for interference with aircraft operations, and includes fair warning to UAS operators. DOJ is committed to working closely with the FAA to balance our operational security needs with requirements for safe and efficient NAS operations.

Authorities Needed to Counter Drones

The Department of Homeland Security (DHS) Deputy General Counsel testified that a critical piece of the bill is the language waiving Title 18.

7. Understanding that technology is constantly evolving and employees deployment counter drone technologies need legal certainty, please explain in detail why a complete waiver of Title 18 is necessary rather than inventorying Title 18, and waiving specific statutes.

**Response:** In order for the legislation to be effective, it must remove uncertainty found in existing law that could place operators of CUAS capabilities in legal jeopardy for taking actions necessary to mitigate a threat. At the time of the hearing, the Administration requested a clear approach that would remove uncertainty by exempting Title 18 and one provision of Title 49. Congress took that approach in each of the last two NDAs with respect to DOD and DOE's employment of Counter-UAS (CUAS) activity.

That approach would ensure that personnel assigned CUAS duties in DOJ and DHS do not receive fewer protections, or face more potential for legal exposure, than their colleagues in DOD and DOE while performing the same type of activity. DOJ and DHS personnel deserve the same protections as their DOD and DOE counterparts. Providing different protections for DOJ and DHS could also make joint operations more difficult. That approach would also help to avoid a negative inference: i.e., if one law has a categorical exclusion, and another does not, a court could interpret that as Congressional intent to open up liability for some provisions.

Operationally, differing authorities and CUAS technologies may lead to security gaps in areas of joint responsibility. Not only could an authority gap cause different capabilities, but also significantly impair our ability to create a common operating picture where we can share critical threat data among participants in joint operations or joint areas of responsibility.

The legislative proposal provides affirmative authority and removes legal uncertainty that currently prevents federal law enforcement from addressing the UAS threat. The proposal is narrowly tailored to authorize only enumerated actions ("detect, identify, monitor," etc.) that are "necessary to mitigate the threat" posed by the UAS. Importantly, the proposal does not remove liability for independent criminal acts, nor does it shield the United States government from liability under the Federal Tort Claims Act.

Since the hearing, the Department has worked closely with this committee, the Judiciary Committee, and the Commerce, Science, and Transportation Committee to narrow the scope of the Title 18 waiver. Although a full waiver from Title 18 would be preferable for the reasons stated above, the Department has agreed to narrow the breadth of the

waiver to the statutes most likely to be implicated by the use of currently available CUAS technologies.

8. What are the consequences of DOJ not having counter drone authority?

**Response:** In short, the Department would be unable to effectively counter the serious and growing threats identified in the above responses to questions 1, 2, 3, and 4.

S. 2836 authorizes DOJ to take certain actions necessary to mitigate the threat posed by drones to a covered facility or asset. A covered facility or asset is to be identified by the Attorney General through a risk based assessment and must be directly related to certain mission sets. The bill allows the Attorney General to make this designation.

9. Please explain why you are unable to list out the covered facilities and assets you would like the counter drone authority to apply to?

**Response:** S. 2836 carefully and narrowly defines the scope of facilities and assets capable of protection. In essence, covered facilities and assets must be (1) within the United States; (2) identified by DOJ and DHS through a sophisticated risk-based assessment conducted in consultation with DOT; (3) and directly related to one of the following missions:

- United States Coast Guard and U.S. Customs and Border Protection security operations, including securing facilities, aircraft and vessels;
- United States Secret Service protection operations;
- Federal Protective Service protection of federal facilities;
- Federal Bureau of Investigation and U.S. Marshals Service personnel protective operations;
- Bureau of Prisons protection of its high-risk facilities and operations;
- Protection of DOJ buildings and grounds considered to be high-risk;
- Security for Special Events: National Special Security Events designated by the President at the request of the Secretary of DHS; or Special Event Assessment Rating Events;
- When a state governor or attorney general requests assistance for a mass gathering event that would not otherwise fall into the security for special event category above;
- Active federal law enforcement investigations, emergency responses, or security operations carried out by DOJ or DHS; and
- Reacting to a known national security threat that could involve unlawful use of a drone.

Specific locations cannot practically be listed in the statute for a variety of reasons. The Government must be able to react to evolving threats in a nimble and effective manner. Adopting a static list of facilities in statute would prevent DOJ and DHS from changing

their security posture based on changes in threat reporting. New facilities may need to be added based upon the threat, while facilities that are initially listed may need to be removed, also based on changes in threat reporting. A static, statutory list is unlikely to remain current, is difficult, cumbersome and time intensive to change, and will constantly need to be evaluated against the threats we face from UAS. Lastly, posting a list of facilities would telegraph to malicious actors precisely where the federal government has and, more importantly, does not have effective countermeasures in place.

Regarding special events, the list of Special Events Assessment Rating events is not static and varies depending on: (1) risk; (2) threat; and (3) data submissions from the state and local authorities each year.

10. Explain how designating covered assets and facilities through a risk based assessment would work. Is this risk based designation process similar to anything DOJ has done before in other areas?

**Response:** The required risk-based assessment is a critical component of prioritizing facilities and assets for protection within the context of the authorized mission sets. Each risk assessment will be conducted in consultation with the Department of Transportation (DOT), and will evaluate a number of important factors identified in the statute, including but not limited to: (1) potential impacts to the national airspace system, including potential effects on manned aircraft and unmanned aircraft systems, airport operations, infrastructure, and air navigation services; (2) options for mitigating any identified impacts to the national airspace system related to the use of any system or technology, including minimizing when possible the use of technology that disrupts the transmission of radio or electronic signals; (3) the ability to provide reasonable advance notice to aircraft operators, consistent with the needs of law enforcement; (4) the location of a covered facility or asset, including whether it is located in a populated area or near other structures, open to the public, and any potential for injury or damage to persons or property; and (5) potential consequences to national security, public safety, or law enforcement if threats posed by unmanned aircraft systems are not mitigated or defeated.

Within the context of the legislation, the risk-based assessment with DOT serves to ensure that DOJ and DHS appropriately consider the full-range of risks before deploying CUAS capabilities in a particular location. Importantly, DOT has performed this risk-based assessment many times with DOD and DOE in the context of their separate CUAS authority. DOJ and DHS would follow that general process when implementing S. 2836.

As a member of the Intelligence Community, FBI has extensive experience with risk-assessments. A significant number of analysts support functions related to risk assessment. Furthermore, DOJ's law enforcement components routinely engage in risk assessments with respect to threats in their areas of responsibility. DOJ participates in the mature and sophisticated National Security Special Event and Special Events Assessment Rating Methodology to assess risk to state and local events across the nation.

This system of risk analysis has been in use for approximately 15 years and is recognized across the US Government and nationally as a reliable and accurate mechanism for determining special-event risk. This methodology considers the threat, vulnerability (e.g., event venue type and access restrictions), and consequences of a successful attack (e.g., crowd density vs attack type).

11. How does requiring that the designation be “risk based” limit the number of assets or facilities covered? In your estimation how many DOJ facilities do you anticipate would be included in covered asset and facility?

**Response:** Please see the above answers to questions 9 and 10.

DOJ use of counter drones authority to secure a covered asset or facility from the threat posed by a drone must be directly linked to a mission set listed in S. 2836.

12. Explain if DOJ is able to list out in additional detail the specific missions in which counter drone authority should apply and why DOJ would prefer the current bill formulation.

**Response:** S. 2836 carefully and narrowly defines the scope of facilities and assets capable of protection. In essence, covered facilities and assets must be (1) within the United States; (2) identified by DOJ and DHS through a sophisticated risk-based assessment conducted in consultation with DOT; (3) and directly related to one of the following missions:

- United States Coast Guard and U.S. Customs and Border Protection security operations, including securing facilities, aircraft and vessels, considered to be high-risk;
- United States Secret Service protection operations considered to be high-risk;
- Federal Protective Service protection of federal facilities considered to be high-risk;
- Federal Bureau of Investigation and U.S. Marshals Service personnel protective operations;
- Bureau of Prisons protection of its high-risk facilities and operations;
- DOJ’s buildings and grounds considered to be high-risk;
- Security for Special Events: National Special Security Events designated by the President at the request of the Secretary of DHS; or Special Event Assessment Rating Events;
- When a state governor or attorney general requests assistance for a mass gathering event that would not otherwise fall into the security for special event category above;
- Active federal law enforcement investigations, emergency responses, or security operations carried out by DOJ or DHS; and
- Reacting to a known national security threat that could involve unlawful use of a drone.

The language above captures the most critical missions performed by DOJ and DHS that will, in some instances, based on our law enforcement and emergency response experience, require protection from UAS threats. DOJ and DHS are committed to implementing this authority in a rigorous and responsible manner, and will only be protecting those facilities and assets significant enough to warrant the use of CUAS capabilities, following a thorough risk-based assessment conducted in consultation with DOT.

13. Please review any concerns attached to a more limited description of mission sets.

**Response:** As discussed above, the FBI has significant concerns about the multitude of drone threats we face, and our inability to use the most effective capabilities to counter those threats. Within the federal government, the FBI is the lead investigative agency in the investigation and prevention of terrorist and significant cyber incidents in the United States, and is also the lead intelligence community agency responsible for counterintelligence activity in the United States. UAS provide an attractive tool for terrorists, nation-states, and criminals to conduct these activities.

As the lead agency for these important functions, we take exceptionally seriously our solemn obligation to protect the American people. Should the mission sets be further narrowed, we have grave concerns about our ability to execute our lead agency responsibilities and to keep the American people safe. The threat is clear, and the repercussions of a potential attack grave -- lives lost, people injured, public confidence in their ability to safely attend a mass gathering outdoors diminished, and the economy impacted. Given the potential consequences, we believe the proposed legislation is a reasonable first step, and urge Congress to approve S. 2389/H.R. 6401.

#### Research, Development and Operational Testing

14. Please state the extent of your authority to research, develop and operationally test counter drone technologies.

**Response:** The FBI has limited authority under 42 U.S.C. §3771 to “develop new or improved approaches, techniques, systems, equipment, and devices to improve and strengthen criminal justice,” which enables the FBI to conduct some forms of CUAS testing. However, like DHS, we must constrain our testing to approved NTIA test ranges where we will not interfere with other aircraft. That constraint precludes real-world testing and validation of promising technologies.

15. What more would you like to do that you are prohibited from doing now?

**Response:** DOJ needs the authority to conduct real-world testing and validation of CUAS systems, and to implement those technologies once they are validated, in coordination with DOT/FAA and NTIA.

#### Securing Mass Gatherings

There is real concern about the private sector's ability to secure critical infrastructure and soft targets, such as mass gatherings of people. The St. Louis Cardinals are just one example of a group concerned about the safety of their game attendees. Despite temporary flight restrictions, private entities cannot mitigate drone threats.

16. Explain how DOJ gaining authority to counter drones will help owners of critical infrastructure, state and local law enforcement and mass gathering venue operators.

**Response:** The security of the nation's critical infrastructure, and soft targets like open air mass gatherings, is of primary concern to DOJ, and in particular, the FBI, given our lead agency responsibility in preventing and investigating terrorism and criminal mass casualty events. As recognized by Chairman Johnson during the committee hearing on S. 2836, this legislation is a much-needed initial step in protecting the United States from the UAS threat. The Administration has endorsed a sequenced approach to CUAS, in which DOD and DOE first obtained authority to protect national defense assets. In this next phase, the Administration has proposed legislation to enable DOJ and DHS to protect sensitive facilities and assets within their purview.

Provided DOJ and DHS receive these authorities, both departments could develop best practices that could be exported to other federal/state/ local/tribal/territorial (FSLTT) law enforcement, should Congress decide to expand CUAS to those actors at some point in the future. In addition, the testing, evaluation, and use of CUAS in the National Airspace System will provide critical information for assessing the performance and impacts on aviation safety, NAS systems, and civil communication systems, which will also assist if/when Congress expands CUAS authority to other federal, state, and/or local entities.

In the meantime, S. 2836 would authorize DOJ and DHS to protect certain scenarios involving mass gatherings. In particular, DOJ and DHS could protect NSSE or SEAR events, provided that the Secretary or Attorney General designated them for protection following a risk-based assessment conducted in consultation with DOT. DOJ and DHS could also protect mass gatherings upon the request of a state governor or attorney general.

17. Review what DOJ doing in the interim to support the private sector in their effort to protect critical infrastructure and the American public at mass gatherings.

**Response:** Please see the response to question 16. Additionally, the FBI has been meeting with representatives of private sector entities, including outdoor entertainment venue operators, major sports leagues, colleges, power generation entities, and others to share information about these threats and discuss best practices for responding in a manner consistent with federal law.

18. Explain whether the threat posed by drones warrants the consideration of regular season games as “special events” and what issues, if any, are raised by such a designation.

**Response:** The FBI defers this question to DHS because DHS is responsible for management of the NSSE and SEAR process.

19. At this time, what are your specific concerns about the consequences of the private sector deploying counter-drone technologies?

**Response:** The growing use of capable and inexpensive UAS for commercial and recreational purposes has resulted in increased UAS encounters over critical infrastructure facilities and large public venues. UAS technology continues to advance with increased range and payload capabilities, enabling a variety of applications that benefit the public. This technology will continue to evolve toward fully autonomous UAS operations. If we do not want to hinder the positive economic potential of this technology, we must advance security measures in parallel.

As a general matter, the use of technologies capable of detecting and mitigating UAS presents similar legal risks for the private sector as it does for the federal sector. Aside from the legal concerns, should private sector entities begin operating their own CUAS equipment in an unregulated and uncoordinated manner, it could result in the “balkanization” of the airspace, effectively closing the skies above private sector facilities for use by civil aviation operators or law enforcement and public safety aviation assets. In addition, the FAA has identified aviation safety impacts associated with the use of some types of CUAS technologies in the National Airspace System. Those impacts must be identified and mitigated through coordination with the FAA and execution of a risk-based assessment. Further, the federal government has a vested interest in ensuring that the private sector uses CUAS technology in a manner protective of privacy and civil liberties. Thus, while we acknowledge the growing need for the private sector to be able to engage in CUAS activities, separate legislation may be necessary to alleviate legal concerns in Title 18 and ensure the activity is carried out in a responsible way.

#### Privacy

There is a perception that if DOJ were granted this authority that it would provide DOJ with roving and ongoing authority to access stored data on the drones or some other personal device.

20. Please outline the privacy protections in S. 2836 and how DOJ would implement those protections.

**Response:** First and foremost, it is important to understand that this legislation is not a new surveillance authority. This legislation merely seeks to provide a clear grant of authority to DOJ and DHS to conduct protective CUAS activities.

This legislation does not provide DHS with roving and ongoing authority to access stored data on drones or other personal devices. In particular, this bill cannot and does not alter the Constitution's prohibition of unreasonable searches and seizures. This bill creates a narrow exception to certain statutes in the federal criminal law, an exception that is limited by purpose, actor, and scope. This legislation authorizes DOJ and DHS to take action to detect or disrupt a UAS only when such action is "necessary." That requirement constitutes the cornerstone of the statutory scheme.

The immediate threat is very different from any post-event investigation that may follow. During the identification, tracking, and mitigation process it may be necessary to access the command and control communications, but it is difficult to imagine (and the bill does not allow) collecting other types of data. After duly authorized and fully trained officers seize control, disable, redirect, interfere with, or destroy the UAS, a law enforcement investigation will likely follow. During the investigation, law enforcement officers could seek other types of data (not related to command and control) through procedures consistent with the Fourth Amendment and laws and policies, such as a search warrant granted by a federal judge.

The text of the bill contains significant and overlapping privacy protections. Specifically, the legislation makes clear that CUAS activities conducted pursuant to the statute must comply with the Fourth Amendment to the Constitution and applicable federal laws. In addition, the bill requires the issuance of guidance that limits the collection, retention, and dissemination of communications to and from the drone. For example, such guidance must limit the interception of communications to or from a UAS only to the extent necessary to support an action authorized by the legislation (e.g., to detect, track, or mitigate a UAS that threatens a covered facility or asset). Records of such communications may be maintained only so long as necessary and, in any event, no longer than 180 days, unless the Secretary or Attorney General determine that an exception applies. The legislation further prohibits the dissemination of communications outside of the relevant department unless one of three exceptions is satisfied.

S. 2836 also requires robust coordination and collaborative risk analysis with the Federal Aviation Administration (FAA) to ensure any deployment of CUAS technologies in the national airspace system (NAS) is conducted safely, minimizes the potential for interference with aircraft operations, and includes fair warning to UAS operators. DOJ is fully committed to working closely with the FAA to balance our operational security needs with the safe and efficient operation of the NAS.

Depending on the operation of the system, DOJ's Chief Privacy and Civil Liberties Officer would work with component Privacy Offices to determine if a Privacy Impact Assessment (PIA) were required, and if so, to identify and mitigate any privacy risks. In addition, a review would take place to determine whether the Privacy Act would apply and if so, whether an existing Privacy Act System of Records Notice (SORN) would apply or a new SORN would be necessary. DOJ's Chief Privacy and Civil Liberties Officer and Senior Component Official for Privacy may decide as a matter of policy to put in place additional privacy protections beyond those required by S. 2836 if he or she believes additional measures would be appropriate.

The involvement of the DOJ privacy program is not a one-time endeavor, but extends throughout the lifecycle of the program or technology. In addition, privacy officials might need to conduct a separate assessment to address any significant changes to the program or the technology.

21. Please explain how DOJ interprets the transparency requirements in the bill.

**Response:** DOJ will make available to the public all Privacy Impact Assessments, when practicable, and Systems of Record Notices, as well as privacy guidance related to CUAS without disclosing classified or operationally sensitive information.

22. Please outline your interpretation of the limitations on the interception and use of electronic communications in S 2836?

**Response:** S. 2836 strictly limits the interception and use of electronic communications. In particular, the legislation limits the interception of electronic communications only to those communications transmitted between the controller and the aircraft, and only to the extent necessary to mitigate the threat posed by that aircraft to the safety or security of covered facilities and assets. Records of such communications may be maintained only so long as necessary and, in any event, no longer than 180 days, unless the Secretary or Attorney General determine that an exception applies. The legislation further prohibits the dissemination of communications outside of the relevant department unless one of three exception is satisfied.

DOJ is committed to interpreting this authority in a manner fully protective of privacy and civil liberties.

#### Counter Drone Authorities

The Department of Homeland Security (DHS) is the lead coordinator for National Special Security Events (NSSEs) and works with federal, state and local law enforcement to provide security. These include the Republican and Democratic National Conventions and the State of the Union. The Department of Justice (DOJ) and the Department of Defense (DoD) are partners

in that effort. Counter-drone authority seems critical to ensuring security at these types of events.

23. Since the National Defense Authorization Act for Fiscal Years 2017 and 2018 provided the DoD with counter-drone authorities, explain why DOJ and DHS need these same authorities. Why isn't the authority provided to the DoD sufficient?

**Response:** DOD's existing CUAS authorities are specific to DOD's mission sets and facilities/assets; they cannot be conferred to other Departments and Agencies, nor is DOD permitted to use CUAS for protection of DHS or DOJ facilities, assets, or operations. Further, DOD's authorities do not address the mission sets that DOJ and DHS have outlined in this legislation, such as the protection of NSSE and SEAR events.

#### Intent of Drone Operator

FAA testimony mentioned the need to identify drones and their operators in order to differentiate between "the clueless, the careless, and the criminal."

24. Does DOJ believe that drone operator intent needs to be determined prior to conducting any counter-drone activity?

**Response:** Operator intent, when available, is one factor to consider in determining whether it is necessary to mitigate a threat posed by an unmanned aircraft system (UAS), as well as the options available for mitigation (e.g., apprehension of the criminal operator, rerouting--if possible--of the clueless). Although important, intent is not the only factor that must be considered. After all, even operators without any kind of malicious intent—the careless and the clueless—can injure people and property or pose security risks to sensitive facilities. Our responsive calculus will therefore encompass a range of factors, including the observable characteristics of the drone, its operational profile, and the nature of the risk presented based on the event or facility protected.

25. Does DOJ consider determination of a drone operator's intent as a key factor in its actions concerning management of drone safety risks?

**Response:** Please see the answer to question 24.

26. How do you plan to discern authorized drones from unauthorized drones in real time, in the absence of a comprehensive remote identification requirement?

**Response:** Currently, unlike manned aviation, there is no standardized identification (ID) requirement for unmanned aircraft systems (UAS), nor is there a UAS traffic management system in place. FAA is pursuing both remote ID and UAS traffic management solutions to help integrate UAS into the National Airspace System (NAS).

DOJ and DHS support both objectives to make it easier for law enforcement personnel to timely discern legitimate UAS traffic in the NAS. However, Section 336 of the FAA Reauthorization Act of 2012 limits FAA's ability to regulate hobbyist or recreational operators who comply with certain requirements. Unless repealed or substantially reformed, that limitation will impede the FAA's ability to require all participants in the NAS to participate in remote ID.

Under existing law, if a UAS is determined to be a threat, DOJ and DHS personnel lack effective options for mitigation consistent with federal law. The proposed legislation would authorize DOJ to utilize CUAS technologies to detect, track and, if necessary, mitigate a threat from a malicious or unauthorized UAS, notwithstanding certain impediments in the federal criminal law. While CUAS systems could be informed by remote identification capabilities, CUAS systems are not dependent on those capabilities. As a general matter, CUAS systems use other methods—such as acoustic, radio frequency, and thermal imaging—to detect and track UAS. Because bad actors will likely not follow or seek to defeat remote identification requirements, CUAS systems will remain necessary to counter UAS operated by those with ill-intent even after remote ID requirements come online.

27. To that end, do you support the repeal of Section 336 of the FAA Modernization and Reform Act so that you can require remote identification for all drones over a certain weight threshold?

**Response:** The FBI recognizes and appreciates that hobbyists and recreational UAS operators have an interest in operating their devices in a responsible manner without undue regulatory burdens. However, the categorical exemption for recreational operators created by Section 336 provides too much opportunity for abuse and too little ability for the FAA to issue regulations necessary to ensure safety and security in the skies.

As you know, many UAS operators believe they qualify as hobbyists in theory, but do not qualify in practice, because they do not satisfy the standards of Section 336. However, it is difficult for a law enforcement officer to know whether a particular operator complies with Section 336. That reality makes it extremely difficult for public safety and law enforcement officers to enforce rules regarding the use of UAS.

The FBI therefore supports the repeal or revision of Section 336. We believe that taking action to reconsider Section 336 in a manner that restores FAA's authority to regulate all UAS as necessary for safety and security, would achieve safer and more efficient skies, and provide a platform on which to facilitate continued hobbyist operations while enabling advanced uses of UAS necessary to bring about tremendous economic growth.

**Post-Hearing Questions for the Record  
Submitted to Angela Stubblefield  
From Senator Rand Paul**

**“S. 2836 – the Preventing Emerging Threats Act of 2018: Countering Malicious Drones”**

**June 6, 2018**

As addressed during my testimony on June 6, 2018, the FAA’s primary mission is to provide the safest, most efficient airspace system in the world. We ensure the safe movement of aircraft through the nation’s skies, 24 hours a day, 365 days a year, over almost 30 million square miles of airspace. Collaborating with our national defense, homeland security, and law enforcement partners is not new to the FAA. We have been working together successfully to address manned aircraft risks for decades. Close coordination with our partners to address Unmanned Aircraft Systems (UAS) security challenges is a natural extension of these time-tested and well-exercised relationships. We continue to work together to improve the Government’s ability to respond to threats posed by manned and unmanned aircraft operations, but more must be done if we are to realize the full benefits of safe and secure UAS integration.

Congress granted the Departments of Defense (DoD) and Energy (DOE) Counter-UAS authorities in December 2016. The Administration has authored a legislative proposal to give the Departments of Homeland Security (DHS) and Justice (DOJ) similar authorities to protect certain facilities, assets, and operations critical to national security against UAS threats. We support a phased approach, as well as the inclusion of provisions in this Committee’s proposal for robust coordination and risk-based assessment, which will ensure aviation safety is not compromised.

The FAA’s role in Counter-UAS is to support our partners’ testing and eventual use of these systems, while maintaining the safety and overall efficiency of the NAS. The FAA is responsible for balancing the requirements of our security partners’ protective missions with the need for 1) operator notification, 2) airspace access, and 3) airspace safety mitigations.

The FAA is currently working with DoD and DOE to strike this balance, as they deploy Counter-UAS technology at sensitive facilities in the United States. We are full partners in their efforts to implement these systems, and have received the same commitment from DHS and DOJ, should they be granted Counter-UAS authority.

In addition to working closely with our federal partners, FAA is progressing on a host of other actions that support both safe AND secure UAS integration, including:

- Publishing an Advance Notice of Proposed Rulemaking to solicit information on UAS security concerns impacting integration;
- Establishing remote identification requirements for UAS;
- Restricting UAS operations over certain federal facilities; and
- Appropriately warning operators in proximity to these restricted sites.

Being able to associate a drone in flight with its operator on the ground is crucial to enabling more complex operations and the ability of our law enforcement and national security partners to identify and respond to security risks. Anonymous operations in the NAS are inconsistent with safe and secure integration. However, even as the FAA is working to establish remote ID requirements, challenges remain. In particular, the current exception for model aircraft – Section 336 of the FAA’s 2012 Reauthorization – makes it nearly impossible for the FAA to develop new regulatory approaches that facilitate full UAS integration. This exception promotes the misperception by many recreational UAS operators that they are not required to follow basic safety rules.

To address this challenge, a basic set of requirements – including registration, remote identification, and observance of airspace restrictions – must apply to ALL UAS operators. This is essential to ensuring clueless and careless operators are distinguished from malicious threats. However, mitigating criminal threats will also require that our security partners be equipped with Counter-UAS authorities and tools.

**FAA Comment:** The original classification for classified documents pertaining to NDAA 2017 and 2018 DoD and DOE C-UAS system use have been classified by those agencies respectively. Because the FAA is not the original classifying agency for those documents, requests for access to those documents should be made to DoD and DOE, as appropriate.

1. S. 2836 authorizes the Secretary of Homeland Security and the Attorney General to empower select Department of Homeland Security (DHS) and Department of Justice (DOJ) personnel to “mitigate the threat” posed by unmanned aircraft systems or unmanned aircraft.

**Question:** Does the bill’s language in any way limit or prohibit the Secretary of DHS or the Attorney General from determining that all UAS or unmanned aircraft pose a potential threat?

**FAA Response:**

The bill prevents the Secretary of DHS or the Attorney General from determining that all Unmanned Aircraft Systems (UAS) or unmanned aircraft pose a potential ‘threat’ by defining the term in S.2836 as amended, SEC. 2 Paragraph (a) (3):  
“THREAT DEFINED.—In defining the term ‘threat’ for purposes of carrying out paragraph (1), the Secretary or the Attorney General, as the case may be, shall take into account factors, including, but not limited to, the potential for bodily harm or loss of human life, the potential loss or compromise of sensitive national security information, or the potential severe economic damage resulting from use of an unauthorized unmanned aerial system in the vicinity of a covered facility or asset.”

2. S. 2836 authorizes the Secretary of Homeland Security and the Attorney General to define “covered facility or asset” through a risk-based assessment process.

**Question:** Does the bill's language in any way limit or prohibit the Secretary of DHS or the Attorney General from identifying every DHS or DOJ facility (including every federal courthouse, corrections facility and/or port of entry) as a covered facility or asset?

**FAA Response:**

The bill prevents the Secretary of DHS or the Attorney General from identifying every DHS or DOJ facility as a 'covered facility or asset' by defining the term in S.2836 as amended:

SEC. 2 Paragraph (k)(3) "The term 'covered facility or asset' means any facility or asset that-

"(A) is identified by the Secretary or the Attorney General, in consultation with the Secretary of Transportation with respect to potentially impacted airspace, through a risk-based assessment for purposes of this section;

"(B) is located in the United States (including the territories and possessions, territorial seas or navigable waters of the United States); and

"(C) directly relates to-

"(i) a mission authorized to be performed by the Department, consistent with governing statutes, regulations, and orders issued by the Secretary, relating to-

"(I) security operations by the United States Coast Guard and U.S. Customs and Border Protection, including securing facilities, aircraft, and authorized vessels, whether moored or underway;

"(II) United States Secret Service protection operations pursuant to sections 3056 and 3056A of title 18, United States Code; or

"(III) protection of facilities pursuant to section 1315 of title 40, United States Code, considered to be high-risk or assessed to be a potential target for unlawful unmanned aircraft activity;

"(ii) a mission authorized to be performed by the Department of Justice, consistent with governing statutes, regulations, and orders issued by the Attorney General, relating to-

"(I) personnel protection operations by the Federal Bureau of Investigation and the United States Marshals Service, including the protection of Federal jurists, court officers, witnesses and other persons in the interests of justice, as specified in section 566(e) of title 28, United States Code;

"(II) penal, detention, and correctional operations conducted by the Federal Bureau of Prisons considered to be high-risk or assessed to be a potential target for unlawful unmanned aircraft activity; or

"(III) protection of the buildings and grounds leased, owned, or operated by or for the Department of Justice identified as essential to the function of the Department of Justice, and the provision of security for Federal courts, as specified in section 566(a) of title 28, United States Code, considered to be high-risk or assessed to be a potential target for unlawful unmanned aircraft activity; and

"(iii) a mission authorized to be performed by the Department of Homeland Security or the Department of Justice, acting together or separately, consistent with governing statutes, regulations, and orders issued by the Secretary or the Attorney General, respectively, relating to-

"(I) National Special Security Events and Special Event Assessment Rating events;

"(II) upon the request of a State's governor or attorney general, providing support to State, local, or tribal law enforcement authorities to ensure protection of people and property at mass gatherings, where appropriate and within available resources;

"(III) active Federal law enforcement investigations, emergency responses, or security operations; or

"(IV) in the event that either the Department of Homeland Security or the Department of Justice has identified a national security threat against the United States and the threat could involve unlawful use of an unmanned aircraft, responding to such national security threat."

There are also robust oversight requirements in the bill, including semiannual joint briefings for appropriate committees of jurisdiction and a 5-year sunset clause on the grant of authority.

3. S. 2836 authorizes the Secretary of Homeland Security and the Attorney General to identify "active Federal law enforcement investigations, emergency responses, or security operations" as a "covered facility or asset." The U.S. Border Patrol and the U.S. Coast Guard conduct security operations around-the-clock.

**Question:** Does the bill's language in any way limit or prohibit the Secretary of DHS from identifying the entire 100-mile "border zone" as a covered facility or asset?

**FAA Response:**

The bill's language restricts actions described in subsection (b) (1) to areas and timeframes described in the requirements in S.2836 as amended, SEC. 2 Paragraphs:

(a)(2)(B) "limit the geographic reach and duration of the actions to only those areas and timeframes that are reasonably necessary to address a reasonable threat; and"

Furthermore, a "covered facility" must meet specific criteria through a risk-based assessment as defined in S.2836 as amended, SEC. 2 Paragraphs (k)(3)(A) and (d)(3):

(k)(3) "The term 'covered facility or asset' means any facility or asset that-  
 "(A) is identified by the Secretary or the Attorney General, in consultation with the Secretary of Transportation with respect to potentially impacted airspace, through a risk-based assessment for purposes of this section;"

(d)(3) "RISK-BASED ASSESSMENT.—The guidance issued by the Secretary and the Attorney General, respectively, shall include criteria of the risk-based assessment required under subsection (k) (3) (A) that includes an evaluation of the potential impacts on the use of the authorities granted in this section on the safety and efficiency of the national airspace system, including the ability to provide advance notice to aircraft operators as appropriate, and the needs of law enforcement agencies and national security."

4. S. 2836 authorizes the Secretary of Homeland Security and the Attorney General to "[u]se reasonable force to disable, damage, or destroy the unmanned aircraft system or unmanned aircraft."

**Question:** Does the bill's language in any way require DHS or DOJ personnel, before downing or destroying a UAS or unmanned aircraft, to assess the potential harm such actions may cause to life and property in the vicinity of the target or on the ground below?

**FAA Response:**

The bill's language requires DHS or DOJ personnel to assess the potential harm such actions may cause to life and property in the vicinity of the target or on the ground below before downing or destroying a UAS or unmanned aircraft through coordination and risk-based assessment as defined in S.2836 as amended, SEC. 2 Paragraphs:

(a)(2)"REQUIREMENTS.—In taking the actions described in subsection (b) (1), the Secretary or the Attorney General, as the case may be, shall—

"(A) avoid infringement of the privacy and civil liberties of the people of the United States and the freedom of the press consistent with Federal law and the Constitution of the United States, including with regard to the testing of any equipment and the interception or acquisition of unmanned aircraft or systems;

"(B) limit the geographic reach and duration of the actions to only those areas and timeframes that are reasonably necessary to address a reasonable threat; and

"(C) use reasonable care not to interfere with authorized or non-threatening manned or unmanned aircraft, communications, equipment, facilities or services.

(d)(2)(B)"EFFECT ON AVIATION SAFETY.—The Secretary and the Attorney General shall respectively coordinate with the Secretary of Transportation and the Administrator of the Federal Aviation Administration before issuing any guidance, or otherwise implementing this section, if such guidance or implementation might affect aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, or the use of airspace.

(d)(3)“RISK-BASED ASSESSMENT.—The guidance issued by the Secretary and the Attorney General, respectively, shall include criteria of the risk-based assessment required under subsection (k) (3) (A) that includes an evaluation of the potential impacts on the use of the authorities granted in this section on the safety and efficiency of the national airspace system, including the ability to provide advance notice to aircraft operators as appropriate, and the needs of law enforcement agencies and national security.”

5. S. 2836 authorizes the Secretary of Homeland Security and the Attorney General to “[u]se reasonable force to disable, damage, or destroy the unmanned aircraft system or unmanned aircraft.”

**Question:** Does the bill’s language contemplate any process by which the actions of DHS or DOJ personnel may be subject to judicial review?

**FAA Response:**

The FAA suggests that questions concerning the broader legal implications of the bill are more appropriately answered by the Department of Justice.

**Question:** Does the bill’s language contemplate any process by which a UAS or unmanned aircraft operator might challenge the lawfulness or appropriateness of the actions taken by DHS or DOJ personnel?

**FAA Response:**

The FAA suggests that questions concerning the broader legal implications of the bill are more appropriately answered by the Department of Justice.

6. S. 2836 authorizes the Secretary of Homeland Security and the Attorney General to “seize or otherwise confiscate the unmanned aircraft system or unmanned aircraft” as well as to “[u]se reasonable force to disable, damage, or destroy the unmanned aircraft system or unmanned aircraft.”

**Question:** Would the seizure or destruction of private property under this Act by DHS or DOJ violate the Fifth Amendment to the U.S. Constitution? Why or why not?

**FAA Response:**

The FAA suggests that questions concerning the broader legal implications of the bill are more appropriately answered by the Department of Justice.

7. S. 2836 authorizes the Secretary of Homeland Security and the Attorney General to seize and control “unmanned aircraft systems” without a warrant. These systems include “communication links and the components that control the unmanned aircraft.”

**Question:** Would smartphones and personal computers that control unmanned aircraft be considered “unmanned aircraft systems”?

**FAA Response:**

Yes, smartphones and personal computers that control unmanned aircraft are considered part of “unmanned aircraft systems” as defined in SEC. 2 Paragraph:

(k)(7)“The terms ‘unmanned aircraft’ and ‘unmanned aircraft system’ have the meanings given those terms in section 331 of the FAA Modernization and Reform Act of 2012 (49 U.S.C. 40101 note).”

The FAA Modernization and Reform Act of 2012 provides the definition in Subtitle B Section 331, which includes components that control the unmanned aircraft:

(9) “UNMANNED AIRCRAFT SYSTEM.—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 pilot in command to operate safely and efficiently in the national airspace system.”

**Question:** Would the DHS or DOJ be able to seize and control such devices without a warrant under this Act?

**FAA Response:**

The FAA suggests that questions concerning the broader legal implications of the bill are more appropriately answered by the Department of Justice.

**Question:** Could records of communication to or from such a device or other data collected with authority under this Act be used to support warrants, arrests, or indictments unrelated to threats presented by unmanned aircraft?

**FAA Response:**

The FAA suggests that questions concerning the broader legal implications of the bill are more appropriately answered by the Department of Justice.

8. S. 2836 gives the Secretary of Homeland Security and the Attorney General broad authority to seize and control expensive personal property. The American people have an interest in understanding how government will invoke this authority.

**Question:** What recourse will the public have if DHS or DOJ mistakenly seizes, controls, or destroys a system not related to unmanned aircraft, perhaps due misattribution of a controlling device or misidentification of wire, oral, electronic, or radio communications protocols?

**FAA Response:**

The FAA suggests that questions concerning the broader legal implications of the bill are more appropriately answered by the Department of Justice.

9. S. 2836 authorizes the Secretary of Homeland Security and the Attorney General to “[u]se reasonable force to disable, damage, or destroy the unmanned aircraft system or

unmanned aircraft.” The Department of Defense and the Department of Energy enjoy similar authorities.

**Question:** What course or courses of action are available to private U.S. citizens to mitigate the threat posed by an unknown UAS or unmanned aircraft on their property, if that UAS or unmanned aircraft presents a threat to the individual’s life, property, or privacy?

**FAA Response:**

Just as they would with a ground-based nuisance or safety/security risk, if someone feels his or her safety or privacy is being violated or threatened, the FAA encourages the individual to call local law enforcement. We have been working with police departments all over the country on how to respond appropriately, including providing guidance and pocket cards as resources for law enforcement agencies on the FAA’s public UAS website. Current law prohibits the destruction, sabotage, or disruption of any aircraft, which include UAS, and the Department of Justice is responsible for applying that law to the destruction of drones. Shooting at or taking another disruptive or destructive action against any aircraft, including unmanned aircraft, could result in a safety hazard as the UAS could crash and injure someone or damage property on the ground, or it could hit other objects in the air.

This example highlights the urgent need to require remote identification of all UAS in the National Airspace System (NAS). Many recreational UAS users have misinterpreted the 2012 FAA Modernization and Reform Act Section 336 to mean they do not need to be knowledgeable of or comply with basic safety requirements. The vast majority of these operators do not meet the criteria for designation under 336; however, the nuance of that distinction is lost in practice and creates both safety and security concerns. Anonymous operations are inconsistent with both safety and security in the NAS. Remote Identification enables us to connect a drone to its operator if it is flying or found on the ground. Like a license plate on a car or a tail number on a manned aircraft, it allows law enforcement through registration of that car or aircraft to know who owns it and better assess what the operator’s intent may be. The FAA envisions remote identification will also enable law enforcement to determine the location of the operator in real time if it is flying. Universal remote identification will enable security partners to better discriminate between UAS that pose security threats and those that may be errant. Without remote identification on all UAS operating in the NAS, determining which UAS present a potential threat will remain extremely challenging.

With this requirement in place, local police could identify the UAS and locate the operator in real time. Additionally, the FAA is responsible for the safety of people in the air, “the flying public,” and those affected by aviation on the ground. Shooting at or taking another disruptive or destructive action against an unmanned aircraft could also result in a civil penalty from the FAA and/or criminal charges filed by federal, state or local law enforcement. There also may be state or local ordinances that address property owners’ rights and firing guns near people or property.

**Post-Hearing Questions for the Record  
Submitted to Angela Stubblefield  
From Senator Claire McCaskill**

**“S. 2836 – the Preventing Emerging Threats Act of 2018: Countering Malicious Drones”**

**June 6, 2018**

As addressed during my testimony on June 6, 2018, the FAA’s primary mission is to provide the safest, most efficient airspace system in the world. We ensure the safe movement of aircraft through the nation’s skies, 24 hours a day, 365 days a year, over almost 30 million square miles of airspace. Collaborating with our national defense, homeland security, and law enforcement partners is not new to the FAA. We have been working together successfully to address manned aircraft risks for decades. Close coordination with our partners to address Unmanned Aircraft Systems (UAS) security challenges is a natural extension of these time-tested and well-exercised relationships. We continue to work together to improve the Government’s ability to respond to threats posed by manned and unmanned aircraft operations, but more must be done if we are to realize the full benefits of safe and secure UAS integration.

Congress granted the Departments of Defense (DoD) and Energy (DOE) Counter-UAS authorities in December 2016. The Administration has authored a legislative proposal to give the Departments of Homeland Security (DHS) and Justice (DOJ) similar authorities to protect certain facilities, assets, and operations critical to national security against UAS threats. We support a phased approach, as well as the inclusion of provisions in this Committee’s proposal for robust coordination and risk-based assessment, which will ensure aviation safety is not compromised.

The FAA’s role in Counter-UAS is to support our partners’ testing and eventual use of these systems, while maintaining the safety and overall efficiency of the NAS. The FAA is responsible for balancing the requirements of our security partners’ protective missions with the need for 1) operator notification, 2) airspace access, and 3) airspace safety mitigations.

The FAA is currently working with DoD and DOE to strike this balance, as they deploy Counter-UAS technology at sensitive facilities in the United States. We are full partners in their efforts to implement these systems, and have received the same commitment from DHS and DOJ, should they be granted Counter-UAS authority.

In addition to working closely with our federal partners, FAA is progressing on a host of other actions that support both safe AND secure UAS integration, including:

- Publishing an Advance Notice of Proposed Rulemaking to solicit information on UAS security concerns impacting integration;
- Establishing remote identification requirements for UAS;
- Restricting UAS operations over certain federal facilities; and
- Appropriately warning operators in proximity to these restricted sites.

Being able to associate a drone in flight with its operator on the ground is crucial to enabling more complex operations and the ability of our law enforcement and national security partners to identify and respond to security risks. Anonymous operations in the NAS are inconsistent with safe and secure integration. However, even as the FAA is working to establish remote ID requirements, challenges remain. In particular, the current exception for model aircraft – Section 336 of the FAA’s 2012 Reauthorization – makes it nearly impossible for the FAA to develop new regulatory approaches that facilitate full UAS integration. This exception promotes the misperception by many recreational UAS operators that they are not required to follow basic safety rules.

To address this challenge, a basic set of requirements – including registration, remote identification, and observance of airspace restrictions – must apply to ALL UAS operators. This is essential to ensuring clueless and careless operators are distinguished from malicious threats. However, mitigating criminal threats will also require that our security partners be equipped with Counter-UAS authorities and tools.

*Please provide responses in a separate classified submission where necessary.*

**FAA Comment:** The original classification for classified documents pertaining to NDAA 2017 and 2018 DoD and DOE C-UAS system use have been classified by those agencies respectively. Because the FAA is not the original classifying agency for those documents, requests for access to those documents should be made to DoD and DOE, as appropriate.

Coordination with the Department of Defense (DoD)

You testified about your engagement with the DoD to coordinate deployment of counter-drone authorities.

1. What does coordination mean in this context?

**FAA Response:**

For purposes of Section 130i of Title 10, U.S. Code, DoD and the Department of Transportation (DOT) explicitly defined the term "coordination" in subsection (b)(2). It requires the Secretary of Defense to seek the views, information, and advice of the Secretary of Transportation concerning any potential effects on the National Airspace System (NAS) as the Secretary of Defense develops the types of actions to be taken and the circumstances of execution under Section 130i. This also means the Secretary of Transportation will provide such views, information, and advice in a reasonably prompt manner. If the Secretary of Transportation notifies the Secretary of Defense that taking the proposed actions would affect aviation safety or NAS operations, the Secretary of Defense and the Secretary of Transportation will work collaboratively to consider proposed actions to mitigate or otherwise address effects on aviation safety, air navigation services, and NAS efficiency, consistent with national security requirements, prior to the Secretary of Defense finalizing the types of actions authorized to be taken under Section 130i.

Practically speaking, coordination includes defining the threat and development of the concepts of operation and tactical use and notification procedures for C-UAS systems for each fixed location and for any ad hoc or mobile operations. To ensure safety is not compromised, the FAA conducts specific, data intensive analyses for each potential location of or situation for use of C-UAS technologies to ensure the concept of operations informs the need for operator notification, airspace access, and appropriate airspace safety mitigations.

A key element of the FAA's work with DoD and DOE has been related to notification and reporting requirements and procedures. Ideally and whenever possible, DoD alerts the FAA in advance of when they plan to utilize a C-UAS system, for example, when conducting testing or training. However, advance notice to the FAA is not realistic during tactical use to counter a threatening UAS. The protocols we developed with DoD and DOE dictate notification to FAA as soon as operationally feasible, which is generally within a few minutes of system use. The extensive pre-operational coordination and establishment of documented procedures ensures we have a common understanding of expectations and requirements. We envision establishing these same expectations and protocols with DHS and DOJ for their employment of C-UAS systems in the NAS, should they be granted authority.

In addition to the operational notifications at the commencement and conclusion of each specific instance of C-UAS use, DoD also provides subsequent reports (known as 'storyboards') to FAA, which chronicle events from detection through mitigation. These reports are classified and distributed within DoD leadership and to the FAA.

We review the incident reports and seek additional information and/or clarifying data (as needed) if we have any questions regarding the threat, system use, or outcomes. If remote identification becomes a requirement for all UAS, we and our security partners will have improved capabilities for locating the operator of a suspect UAS and will further investigate to ascertain their intent and to determine any violations for possible civil and/or criminal enforcement.

2. Have you said experienced conflict with DoD in the implementation of their authorities?

**FAA Response:**

While the FAA has had a longstanding and successful relationship with DoD and national security partners to address manned aircraft risks for decades, deployment of C-UAS authorities has presented new challenges and opportunities. For example, although most federal departments and agencies that use spectrum-impacting systems understand the interagency spectrum approval process, the operational coordination and approval required from FAA is a new component in the deployment of UAS detection and mitigation systems in the Homeland. Lessons learned were used in jointly designing, refining and coordinating procedures on the front end as well as in the execution phase. We learned that it is vital that C-UAS system operators understand the potential impact(s) that system use can have on an aircraft and aviation infrastructure beyond the UAS they are targeting; and, why the immediate FAA notification is necessary. Storyboard reporting is necessary to understand the response taken to detect and mitigate the UAS, as not all UAS react in the same way.

As with any new endeavor, there are challenges and disagreements on how to proceed on some issues; however, given our explicit definition of coordination and the joint understanding of the importance in maintaining aviation safety, FAA and DoD have been able to successfully work through each challenge to determine an acceptable solution. We have used these lessons learned to develop a roadmap, identifying the steps needed to safely deploy Counter UAS systems in coordination with FAA. This roadmap will assist DHS and DOJ in avoiding many of the challenges we have already addressed with DoD.

3. Has the Federal Aviation Administration (FAA) refused any DoD requests in the process of implementing their authorities? Please explain by providing one example.

**FAA Response:**

FAA has had one instance in which a condition of concurrence was not agreed upon prior to DoD's deployment for an urgent mission. DoD is best suited to elaborate on their decision(s), due to the classified nature of the event. Importantly, however, we used this opportunity to clarify expectations and determine what is needed to address such situations in the future.

Intent of Drone Operator

In your testimony, you mentioned the need to identify drones and their operators in order to differentiate between "the clueless, the careless, and the criminal."

4. Does the FAA believe that drone operator intent needs to be determined prior to conducting any counter-drone activity?
5. Does FAA consider determination of a drone operator's intent as a key factor in its actions concerning management of drone safety risks?
6. How do you plan to discern authorized drones from unauthorized drones in real time, in the absence of a comprehensive remote identification requirement?
7. To that end, do you support the repeal of Section 336 of FAA Modernization and Reform Act so that you can require remote identification for all drones over a certain weight threshold? Yes

**FAA Response:**

The bill prevents the Secretary of DHS or the Attorney General from determining that all UAS or unmanned aircraft pose a potential threat by defining the term in S.2836 as amended: SEC. 2 Paragraph (a) (3): "THREAT DEFINED.—In defining the term 'threat' for purposes of carrying out paragraph (1), the Secretary or the Attorney General, as the case may be, shall take into account factors, including, but not limited to, the potential for bodily harm or loss of human life, the potential loss or compromise of sensitive national security information, or the potential severe economic damage resulting from use of an unauthorized unmanned aerial system in the vicinity of a covered facility or asset."

Anonymous operations are inconsistent with both safety and security in the national airspace system. Remote identification enables us to connect a drone to its operator if it is flying or found on the ground. Like a license plate on a car or a tail number on a manned aircraft, it allows law enforcement, through registration of that car or aircraft, to know who owns it and better assess what the operator's intent may be. We envision remote identification will also enable law enforcement to determine the location of the operator in real time if it is flying. Universal remote identification will enable security partners to better discriminate between UAS that pose security threats and those that may be errant. Without remote identification on all UAS operating in the NAS, determining which UAS present a potential threat will remain extremely challenging.

The FAA has the authority to promulgate a rule requiring remote identification, and we are working on that as expeditiously as possible. However, even as the FAA is working to establish remote ID requirements, challenges remain. We have been working with our committees of jurisdiction and other stakeholders, including the Academy of Model Aeronautics (AMA), regarding our safety concerns—and the concerns of our security partners—related to the challenges with the practical implications of the exception for model aircraft in Section 336 and possible ways to mitigate those concerns. The exception makes it nearly impossible for the FAA to develop new regulatory approaches that facilitate full UAS integration and promote the misperception by many recreational UAS operators that they are not required to follow basic safety rules. The Administration believes that the most straightforward way to overcome these challenges is the repeal of Section 336. Additionally, there have been several provisions to the House authorization bill that attempt to address some issues stemming from Section 336.

Being able to associate a drone in flight with its operator on the ground is crucial to enabling more complex operations and the ability of our law enforcement and national security partners to identify and respond to potential security risks. Anonymous operations in the NAS are inconsistent with safe and secure integration.

To address this challenge, a basic set of requirements – including registration, remote identification, and observance of airspace requirements – must apply to ALL UAS operators. This is essential to ensuring clueless and careless operators are distinguished from malicious actors. However, mitigating criminal threats will also require that our security partners be equipped with Counter-UAS authorities and tools.

#### Drone Integration into Air Space

You testified that the Department of Transportation (DOT) and the FAA have been working closely with security partners to advance UAS integration while addressing and mitigating security risks.

8. Does the FAA believe that the growth in drone operations is proportional to safety and security risks concerning drone operations? If not, please explain FAA's views on the relationships to these risks, and how any data obtained by the agency supports its view.

#### **FAA Response:**

The current exception for model aircraft – Section 336 of the FAA’s 2012 Reauthorization – makes it nearly impossible for the FAA to develop new regulatory approaches that facilitate full UAS integration. Virtually all stakeholders (particularly those with safety and security missions) would acknowledge that the landscape has dramatically changed since 2012, and the overall effort to safely integrate UAS would benefit from a reexamination of the model aircraft exception. This exception promotes the misperception by many recreational UAS operators that they are not required to follow basic safety rules. To address this challenge, a basic set of requirements – including registration, remote identification, and the observance of airspace requirements – must apply to ALL UAS operators. This is essential to ensuring clueless and careless operators fly safely. However, mitigating criminal threats will also require that our security partners be equipped with Counter-UAS authorities and tools.

We respect and value the freedom and rights of all Americans to operate UAS for personal use, including recreational purposes. The FAA recognizes and values the strong tradition of model aircraft operations in the United States. However, the vast majority of operators under Section 336 do not meet the criteria for designation under Section 336. Unfortunately, the nuance of that distinction is lost in practice and creates both safety and security concerns. The FAA and DOT believe Section 336 impedes the FAA’s efforts to create new regulatory approaches that will help expand and facilitate the greater use of UAS in the navigable airspace, while also addressing the concerns of our national security partners.

9. Has FAA performed a program-wide safety/security risk or hazard analysis concerning drone operations? Does it intend to?

**FAA Response:**

On June 21, 2016, the FAA finalized the rule for small unmanned aircraft systems, which offered safety regulations for unmanned aircraft drones weighing less than 55 pounds that are conducting non-hobbyist operations. Prior to the promulgation of the rule, the FAA performed a program-wide safety/security risk and hazard analysis concerning drone operations under 49 CFR part 107. The rule took effect on August 29, 2016. Further, prior to granting operational waivers, exemptions, certifications and public aircraft operations, extensive safety analyses are conducted.

As the FAA has no authority to promulgate rules for recreational operations conducted—or mistakenly presumed to be conducted—under community-based organizations, such as the Academy of Model Aeronautics (AMA), we have safety concerns, along with our security partners, related to the challenges with the practical implications of Section 336 and possible ways to mitigate those concerns.

Flight Restrictions

10. Would you please detail how the FAA is determining which facilities require airspace restrictions due to drone security risks? Would you outline the factors considered?

**FAA Response:**

FAA is using existing airspace mechanisms found in 14 CFR 99.7, Special Security Instructions, to implement temporary UAS-specific flight restrictions at certain Federal locations. Flight restrictions are established based on a request from and an agreement with a Federal security or intelligence agency, and must be justified as serving the interest of national security.

These 14 CFR 99.7 restrictions include the development and approval of Memorandums of Understanding and Joint Standard Operating Procedures, which establish roles and responsibilities and set expectations. Requesting airspace restrictions and managing the temporary restrictions is an ongoing interagency relationship. Each partner agency has the responsibility to provide a contact for 24/7 airspace access requests.

As of June 2018, the FAA completed and posted restrictions for 254 DoD facilities with 1,341 specific DoD airspace restrictions; 10 combined Department of Interior facilities/airspaces; 7 DOE combined facilities/airspaces; 10 USCG facilities with 13 airspace restrictions; and 20 Federal Bureau of Prisons combined facilities/airspaces.

Further, the FAA has vital safety concerns in equating flight restrictions with the authority to use counter UAS systems. Flight restrictions serve two purposes – they provide warning to operators to stay away from an area where UAS could pose a hazard and they help to mitigate aviation safety hazards. The size, shape, and volume of a given flight restriction is directly related to whether we are serving one or both of those purposes. UAS-specific flight restrictions in place at various national security-sensitive federal facilities are different, both in process and construct, than airspace restrictions in places at facilities where DoD is currently deploying CUAS. The latter restrictions are constructed to account for the concepts of operation and impacts of the use of CUAS systems. The former are not. To consider them interchangeable is not appropriate.

#### Enforcement Actions

11. Has the FAA taken any enforcement actions against state or local law enforcement officials or private entities for unlawful counter-drone actions? If so, please describe.

#### **FAA Response:**

To date, the FAA has not taken any enforcement actions against state or local law enforcement officials or private entities for unlawful counter-drone actions. The FAA's Law Enforcement Assistance Program (LEAP) has created a reporting process for incidents and follows up with law enforcement on every UAS sighting or incident reported to the FAA and a law enforcement agency to determine if the operator was identified. LEAP agents conduct extensive outreach and educational seminars across the federal, state, and local law enforcement community. We have also been conducting monthly public safety webinars for law enforcement and other first responders (called "411 for 911") to educate them about how to fly UAS to support their missions, and how to respond to unsafe or illegal UAS operations. The FAA has a comprehensive law enforcement guide and pocket card to support law enforcement training and response. Both are available on the FAA's UAS website.

#### State and Local Incident Reporting

12. How many incident reports has FAA received from law enforcement community concerning unsafe or unauthorized drone operations? What actions were taken as a result of these reports, and in what timeframes?

**FAA Response:**

The FAA collaborates with law enforcement (LE) regularly and dedicates resources to support LE use of, response to, and investigation of UAS. This includes developing reference materials to provide guidance to LE, providing regular briefings and webinars, giving one on one guidance, and supporting LE specific outreach. The FAA's Law Enforcement Assistance Program (LEAP) has created a reporting process for incidents and follows up with law enforcement on every UAS sighting or incident reported to the FAA and a law enforcement agency to determine if the operator was identified, share relevant information, and support both potential civil and criminal enforcement actions.

Since the FAA began tracking UAS sightings in January 2015, law enforcement agencies have contacted FAA over 400 times to report potentially unauthorized and/or unsafe UAS operations. Those reports are submitted to our local FAA offices for investigation and action. While we don't specifically distinguish our responses to LE reports from other UAS investigations (i.e., those initiated from reports from other sources), all of our responses generally fall under the FAA's Compliance Oversight Program. The FAA considers the reckless or intentional nature of the non-compliant activity in determining whether a compliance action, such as education, or an enforcement action is appropriate.

In total, we have initiated over 75 enforcement actions, and taken over 400 compliance actions, against unsafe or unauthorized UAS operators. However, we also note, in the vast majority of reported incidents of potentially unsafe or unauthorized UAS operations, we cannot pursue any investigation because neither we nor law enforcement can identify the operator, because we lack remote identification requirements that apply to all UAS operating in the NAS. The FAA is working expeditiously on rulemaking to establish those remote identification rules; however, under current law, those requirements will not apply to those operating under—or believed to be operating under—the Section 336 modeler exception, thus underscoring the need to address the constraints this exception places on the FAA's authority to address safety and security risks.

Integration Pilot Program

FAA recently selected 10 projects under its UAS Integration Pilot Program (IPP), which was open to counter-drone projects.

13. Of the 149 proposals submitted, how many involved counter drone technology?

**FAA Response:**

Of the 149 proposals submitted, 80 identified their intent to conduct research in counter-drone technology or some security related issues in some capacity. The 80 were identified by reviewing Lead Applicant proposals. Section 10.2.1.7 of the FAA Screening Information Request (SIR) for the UAS IPP required Lead Applicants to select from a checkbox list on the

Airspace Identification Form the type of technology(s) it intends to research in each airspace from the following list:

*Identification (ID) & Tracking, Counter-UAS and Other Security-Related Issues, Cybersecurity, Unmanned Traffic Management, Detect and Avoid, other, and none [emphasis added].*

However, given the current legal constraints of Title 18, among others, there are substantial limitations on CUAS research for all state, local, and private sector entities and almost all federal agencies.

14. How many solely involved counter-drone operations?

**FAA Response:**

Three Lead Applicant proposals prominently featured the use and deployment of counter-UAS technology or security related activities, which are subject to current legal constraints, which would not be waived in any way under the IPP.

15. Of the 10 selected, how many included counter-drone?

**FAA Response:**

Six of the ten selected Lead Participants identified Counter-UAS and Other Security-Related Issues in their proposals. Lead Participants are developing operations directly or indirectly related to the following security topics:

- Border security
- Airport security
- Critical infrastructure security
- Public safety
- Remote identification

16. What is FAA doing to encourage proposals for counter-drone testing?

**FAA Response:**

The FAA UAS Integration Pilot Program (UAS IPP) is not taking specific actions to encourage proposals for counter-drone testing. In accordance with the Presidential Memorandum for the Secretary of Transportation, Section 4(e) states:

In implementing the Program, the Secretary shall coordinate with the Secretaries of Defense and Homeland Security and the Attorney General to test counter-UAS capabilities, as well as platform and system-wide cybersecurity, to the extent appropriate and consistent with law.

The UAS IPP, in collaboration with the FAA Office of Security and Hazardous Materials, has and will continue coordinating UAS IPP activities in accordance with the Presidential Memorandum.

The Screening Information Request for the UAS IPP program required Lead Applicants to identify and describe the technologies they intended to research within each proposed airspace, including but not limited to Identification (ID) & Tracking and Counter-UAS and other Security-Related Issues [emphasis added].

It is important to note that Title 18, among other statutes, heavily constrains most federal and all state, local, and private sector entities engagement in much counter drone testing and research.

17. Concerning the review process for this program, how many of the reviewers were counter-drone experts?
18. Were all proposals involving counter-drone reviewed by these FAA counter-drone experts?
19. Were DHS, DOJ or DoD personnel directly involved in the review of counter-UAS proposals? If so, how?

**FAA Response:**

The FAA UAS Integration Office worked closely with the FAA Office of Security and Hazardous Materials Safety throughout all phases of the UAS IPP source selection. In accordance with the Presidential Memorandum, proposals were evaluated relative to the potential to safely integrate UAS operations into the National Airspace System. There were no evaluation criteria or requirements specific to counter-UAS technologies and testing.

Each proposal was evaluated by a team of several dozen FAA subject matter experts. Additionally, in accordance with the Presidential Memorandum's requirement directing the Secretary to coordinate with the Secretaries of Defense, Homeland Security and the Attorney General (the Security Partners), the FAA provided UAS security experts from these agencies with the information described in the response to the previous question for the most highly rated Lead Applicant Proposals. The FAA asked our National Security Partners to review and flag any security concerns. The Security Partner UAS experts completed the requested review and did not identify any significant concerns.

We continue to engage our Security Partners as we work with the Lead Participants to develop their concepts of operation to identify both potential security concerns as well as opportunities for collecting data or work of interest to our security partners' counter-UAS efforts.