AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

USING UNMANNED AERIAL SYSTEMS WITHIN THE HOMELAND: SECURITY GAME-CHANGER?

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT, INVESTIGATIONS, AND MANAGEMENT

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

JULY 19, 2012

Serial No. 112–107

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

80–848 PDF WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

LAMAR SMITH, Texas
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
TIM WALBERG, Michigan
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
PATRICK MEEHAN, Pennsylvania
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
BLAKE FARENTHOLD, Texas
ROBERT L. TURNER, New York

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
DANNY K. DAVIS, Illinois
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
HANSEN CLARKE, Michigan
WILLIAM R. KEATING, Massachusetts
KATHLEEN C. HOCHUL, New York
JANICE HAHN, California
RON BARBER, Arizona

MICHAEL J. RUSSELL, *Staff Director/Chief Counsel*
KERRY ANN WATKINS, *Senior Policy Director*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON OVERSIGHT, INVESTIGATIONS, AND MANAGEMENT

MICHAEL T. MCCAUL, Texas, *Chairman*

GUS M. BILIRAKIS, Florida
BILLY LONG, Missouri, *Vice Chair*
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
PETER T. KING, New York *(Ex Officio)*

WILLIAM R. KEATING, Massachusetts
YVETTE D. CLARKE, New York
DANNY K. DAVIS, Illinois
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

DR. R. NICK PALARINO, *Staff Director*
DIANA BERGWIN, *Subcommittee Clerk*
TAMLA SCOTT, *Minority Subcommittee Director*

CONTENTS

Page

STATEMENTS

The Honorable Michael T. McCaul, a Representative in Congress From the State of Texas, and Chairman, Subcommittee on Oversight, Investigations, and Management:
Oral Statement 1
Prepared Statement 3
The Honorable William R. Keating, a Representative in Congress From the State of Massachusetts, and Ranking Member, Subcommittee on Oversight, Investigations, and Management:
Prepared Statement 30
The Honorable Henry Cuellar, a Representative in Congress From the State of Texas 5
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:
Prepared Statement 10

WITNESSES

PANEL I

Mr. Todd E. Humphreys, Ph.D., Assistant Professor, Cockrell School of Engineering, The University of Texas at Austin:
Oral Statement 12
Prepared Statement 13

PANEL II

Mr. Gerald L. Dillingham, Ph.D., Director, Physical Infrastructure Issues, Government Accountability Office:
Oral Statement 36
Prepared Statement 38
Chief Deputy William R. McDaniel, Montgomery County Sheriff's Office, Conroe, Texas:
Oral Statement 46
Prepared Statement 47
Ms. Amie Stepanovich, Litigation Counsel, Electronic Privacy Information Center:
Oral Statement 49
Prepared Statement 50

FOR THE RECORD

The Honorable Michael T. McCaul, a Representative in Congress From the State of Texas, and Chairman, Subcommittee on Oversight, Investigations, and Management:
Statement of Michael Toscano, President and CEO, Association for Unmanned Vehicle Systems International (AUVSI) 6
Letter From the Air Line Pilots Association International 9
Association for Unmanned Vehicle Systems International:
Unmanned Aircraft System Operations Industry "Code of Conduct" 61

USING UNMANNED AERIAL SYSTEMS WITHIN THE HOMELAND: SECURITY GAME-CHANGER?

Thursday, July 19, 2012

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT, INVESTIGATIONS, AND MANAGEMENT,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The subcommittee met, pursuant to call, at 9:40 a.m., in Room 311, Cannon House Office Building, Hon. Michael T. McCaul [Chairman of the subcommittee] presiding.

Present: Representatives McCaul, Long, Duncan, Marino, Keating, Clarke, and Davis.

Also present: Representatives Cuellar and Brady.

Mr. MCCAUL. The committee will come to order. First and as a matter of business, Mr. Keating is running late, and I would ask unanimous consent that Mr. Cuellar sit as the Ranking Member of the subcommittee for this hearing. Seeing no objection? Mr. Duncan, you have no objection to that?

I now recognize myself for an opening statement.

Unmanned aerial systems, commonly known as drones, have been a game-changer for our men and women serving in Iraq and Afghanistan. The systems have provided our troops with much-needed eyes in the skies and have taken the fight to the enemy, eliminating some of the most dangerous al-Qaeda terrorists. Drones have also increased our capabilities to secure our borders and aid our first responders.

U.S. Customs and Border Protection began first looking at these drones back in 2004. Now CBP owns 10 UAS aircraft. These systems have been used to surveil drug smuggler tunnels, video dams, bridges, levees, riverbeds at risk of flooding, and assist with the deployment of National Guard resources responding to local flooding. CBP has also flown missions in support of the Border Patrol, Texas Rangers, U.S. Forest Service, FBI, and others. The systems have become a force multiplier for military operations and for border security.

However, we are on the edge of a new horizon: Using unmanned aerial systems within the homeland. Currently, there are 200 active Certificates of Authorization issued by the Federal Aviation Administration to over 100 different entities, such as law enforcement departments and academic institutions, to fly drones domestically. This map on the monitor shows the locations of COA, or COA recipients as of April 2012. The number of recipients since that time has in fact increased.

The FAA plans to select six test sites around the country for the use of non-Government drones this year and plans to allow the deployment of non-Government drones Nation-wide by the year 2015.

While the FAA is responsible for ensuring these systems fly safely in U.S. airspace, with only 2½ short years until drones begin to dominate the skies in the U.S. homeland, no Federal agency is taking the lead to deal with the full implications of using unmanned aerial systems and developing the relevant policies and guidelines for their use. This is despite the fact that 4 years ago the Government Accountability Office recommended to the Secretary of Homeland Security that she direct the TSA Administrator to examine the security implications of future, non-military UAS operations in the National airspace system and take any actions deemed appropriate.

GAO's recommendation was well-founded because in 2004, TSA issued an advisory that described possible terrorist interest in using UASs as weapons. The advisory noted the potential for UASs to carry explosives or disperse chemical or biological weapons. It discussed how the Revolutionary Armed Forces of Colombia, or FARC, and Hezbollah were interested in acquiring these UASs. While the advisory acknowledged there was no credible evidence to suggest that terrorist organizations planned to use these systems in the United States, it did state that the United States Government was concerned that these aerial vehicles could be modified and used to attack key assets and critical infrastructures within the United States.

These concerns were validated just last week, or last year when a Massachusetts man agreed to plead guilty to attempting to damage and destroy Federal buildings. The individual was arrested in September 2011 after an undercover FBI investigation revealed his plot to use multiple remote controlled aircraft laden with explosives to collapse the dome of the United States Capitol and attack the Pentagon using that UAV system.

As if this plot wasn't frightening enough, cutting-edge research out of the University of Texas at Austin has revealed yet more security vulnerabilities. Specifically, researchers from the Cockrell School of Engineering led by Dr. Todd Humphreys, who is our first witness today, proved that civilian unmanned aerial systems can be hacked into and hijacked with a relatively small investment of money and time. These findings are alarming and have revealed a gaping hole in the security of using unmanned aerial systems domestically. Now is the time to ensure these vulnerabilities are mitigated to protect our aviation system as the use of unmanned aerial systems continue to grow.

The Department of Homeland Security's mission is to protect the homeland. Unfortunately, DHS seems either disinterested or unprepared to step up to the plate to address the proliferation of unmanned aerial systems in U.S. airspace. The potential threats they pose to our National security and the concerns our citizens have of how drones fly over cities will be used, including protecting civil liberties of individuals under the Constitution.

For example, in discussions with my subcommittee staff prior to this hearing, Department officials repeatedly stated that the Department does not see this function, the domestic use of drones, as

part of their mission and has no role in the domestic unmanned aerial systems. I strongly disagree. I can't imagine how they would find that they have no role when there is a terror plot thwarted by the FBI attempting to hit the United States Capitol and the Pentagon. What more Homeland Security interest could there possible be?

DHS's lack of attention about this issue is truly incomprehensible.

It should not take a 9/11-style attack by a terrorist organization such as Hezbollah or a lone wolf-inspired event to cause DHS to develop guidance addressing the security implications of domestic drones. It should not take a hearing to force the DHS to develop policy when it comes to the security of our homeland, and what it should take is responsible leadership willing to recognize a potential threat and take the initiative. DHS lacks this initiative and I am concerned that DHS is reverting back to a pre-9/11 mindset, which the 9/11 Commission described as a lack of imagination in identifying threats and protecting the homeland.

We are disappointed that DHS declined to testify here today. This is simply another example of how DHS leadership is failing to get ahead of the curve on an issue which directly impacts the security of the United States. I hope our witnesses' testimony will be a call to action for the Department. During today's testimony we look forward to learning more about the security issues related to the domestic use of drones and what DHS needs to do to prepare for their widespread use.

[The statement of Mr. McCaul follows:]

STATEMENT OF CHAIRMAN MICHAEL T. MCCAUL

JULY 19, 2012

Unmanned aerial systems, commonly known as "drones", have been a game changer for our men and women serving in Iraq and Afghanistan. These systems have provided our troops with much-needed "eyes in the sky" and have taken the fight to the enemy, eliminating some of the most dangerous al-Qaeda terrorists. Drones have also increased our capabilities to secure our borders and aid first responders.

U.S. Customs and Border Protection began first looking at using drones back in 2004. Now, CBP owns ten UAS aircraft. These systems have been used to surveil drug smuggling tunnels; video dams, bridges, levees, and riverbeds at risk of flooding; and assist with the deployment of National Guard resources responding to local flooding. CBP has flown missions in support of the Border Patrol, Texas Rangers, U.S. Forest Service, FBI, and others. These systems have become a force multiplier for military operations and border security.

However, we are now on the edge of a new horizon: Using unmanned aerial systems within the homeland. Currently, there are about 200 active Certificates of Authorization issued by the Federal Aviation Administration to over 100 different entities, such as law enforcement departments and academic institutions, to fly drones domestically. This map shows the location of COA recipients as of April 2012. The number of recipients since that time has increased.

The FAA plans to select six test sites around the country for the use of non-Government drones this year and plans to allow the deployment of non-Government drones Nation-wide by 2015.

While the FAA is responsible for ensuring these systems fly safely in U.S. airspace, with only 2½ short years until drones begin to dominate the skies in the U.S. homeland, no Federal agency is taking the lead to deal with the full implications of using unmanned aerial systems and developing the relevant policies and guidelines for their use. This is despite the fact that 4 years ago the Government Accountability Office recommended the Secretary of Homeland Security direct the TSA

Administrator to examine the security implications of future, non-military UAS operations in the National airspace system and take any actions deemed appropriate.

GAO's recommendation was well-founded because in 2004 TSA issued an advisory that described possible terrorist interest in using UASs as weapons. The advisory noted the potential for UASs to carry explosives or disperse chemical or biological weapons. It discussed how the Revolutionary Armed Forces of Columbia, or FARC, and Hezbollah were interested in acquiring UASs. While the advisory acknowledged there was no credible evidence to suggest that terrorist organizations planned to use these systems in the United States, it did state that the U.S. Government was concerned that these aerial vehicles could be modified and used to attack key assets and critical infrastructure in the United States.

These concerns were validated just last week when a Massachusetts man agreed to plead guilty to attempting to damage and destroy Federal buildings. The individual was arrested in September 2011 after an undercover FBI investigation revealed his plot to use multiple remote-controlled aircraft laden with explosives to collapse the dome of the U.S. Capitol and attack the Pentagon.

As if this plot wasn't frightening enough, cutting-edge research out of the University of Texas at Austin has revealed yet more security vulnerabilities. Specifically, researchers from the Cockrell School of Engineering led by Dr. Todd Humphreys proved that civilian unmanned aerial systems can be hacked into and hijacked with a relatively small investment of money and time. These findings are alarming and have revealed a gaping hole in the security of using unmanned aerial systems domestically. Now is the time to ensure these vulnerabilities are mitigated to protect our aviation system as the use of unmanned aerial systems continues to grow.

The Department of Homeland Security mission is to protect the homeland. Unfortunately, DHS seems either disinterested or unprepared to step up to the plate to address the proliferation of Unmanned Aerial Systems in U.S. air space, the potential threats they pose to our National security, and the concerns of our citizens of how drones flying over our cities will be used including protecting civil liberties of individuals under the Constitution. For example, in discussions with my subcommittee staff prior to this hearing, Department officials repeatedly stated the Department does not see this function (domestic use of drones) as part of their mission and has no role in domestic unmanned aerial systems. I strongly disagree.

DHS's lack of attention about this issue is incomprehensible. It should not take a 9/11-style attack by a terrorist organization such as Hezbollah or a lone wolf-inspired event to cause DHS to develop guidance addressing the security implications of domestic drones. It should not take a hearing to force DHS to develop policy when it comes to the security of our homeland. What it should take is responsible leadership willing to recognize a potential threat and take the initiative. DHS lacks that initiative. I am concerned DHS is reverting back to a pre-9/11 mindset, which the 9/11 Commission described as a lack of imagination in identifying threats and protecting the homeland.

We are disappointed DHS declined to testify today. This is simply another example of how DHS leadership is failing to get ahead of the curve on an issue which directly impacts the security of the United States. I hope that our witnesses' testimony will be a call to action for the Department. During today's testimony, we look forward to learning more about the security issues related to the domestic use of drones and what DHS needs to do to prepare for their widespread use.

Source: Google Maps.

Location of FAA COA Recipients as of April 2012

Mr. MCCAUL. With that, the Chairman now recognizes the Ranking Member, I guess pro tem, Mr. Cuellar.

Mr. CUELLAR. Thank you very much, Mr. Chairman. Thank you for this opportunity to be here with you as the Ranking Member for the Border-Maritime where we deal with border security and dealing with some of the UAVs that I think you and I have worked on together. It certainly gives us an opportunity, and also as the co-chair of the Congressional Unmanned System Caucus with Congressman Buck McKeon. Just for informational purposes, Members, we do have tomorrow a caucus meeting, and we are going to

have Members, representatives from the FBI, DHS, CBP tomorrow at 10:00 at the Rayburn Room 2261. I will give a copy to the Members here. This will be an excellent opportunity for Members and their staff to learn about current and future domestic law enforcement use of unmanned aerial vehicles.

We have, Buck McKeon and myself, have spent a lot of time with other Members of the caucus looking at the issues that you have brought up, Mr. Chairman, privacy issues that have been brought up, and as you know a lot of the privacy issues have already been decided by the Supreme Court. All we are looking at is using a different type of platform. So whether it is a helicopter, an airplane, or in this case a UAV, a lot of those issues have been addressed by the Supreme Court issues, and there is 1, 2 pages that I have though. So if anybody wants to learn about the privacy issues on drones or UAVs, please contact my office or Buck's office.

But the other thing, Mr. Chairman, you do bring up a lot of good points that I think we need to cover. Good questions. I look forward to hearing from my UT graduate also, from UT. I do have two degrees from UT, and Doctor, it is a pleasure meeting you. I do have a few questions for you on that, but I think this type of a dialogue would be good to talk about the UAVs.

One last thing, Mr. Chairman, as you mentioned, the FAA, we did pass the reauthorization of the FAA that talks about the integration of more civilian UAVs and there are different steps we have brought in. If you haven't talked to the FAA, I would ask you to spend some time with the FAA because they have certain steps that they will be going into the future use on this. I know that the Ranking Member, Mr. Keating, for this particular subcommittee is on his way. He does have a statement. I am not going to read his statement. He will be up here and if you will give him the opportunity to also make that statement when he shows up.

But at this time, Mr. Chairman, thank you for allowing me to be here with you.

Mr. MCCAUL. I thank the Ranking Member, and before I continue I ask unanimous consent to include a statement from Mr. Michael Toscano, president and CEO of the Association for Unmanned Vehicle Systems International, and Captain Lee Moak, the president of the Airline Pilots Association, describing the domestic use of UAS, both of whom are very much in favor of this hearing. Hearing no objection, so ordered.

[The statements of Mr. Toscano and Mr. Moak follow:]

STATEMENT OF MICHAEL TOSCANO, PRESIDENT AND CEO, ASSOCIATION FOR UNMANNED VEHICLE SYSTEMS INTERNATIONAL (AUVSI)

On behalf of the Association for Unmanned Vehicle Systems International (AUVSI) and its members, I want to thank the committee for examining important issues relating to the expansion of unmanned aircraft systems (UAS) in the National Airspace System. Unmanned aircraft extend human potential and allow us to execute dangerous or difficult tasks safely and efficiently, saving time, saving money and, most importantly, saving lives.

Whether it is helping search-and-rescue teams find a lost child, giving researchers a new understanding of hurricanes, or helping to fight wildfires, the applications of unmanned aircraft in the United States are virtually limitless. The incredible benefits of UAS aren't just theoretical, however; the technology is already serving important homeland security and safety functions here at home. For example:

- U.S. Customs and Border Protection (CPB) currently uses UAS to monitor the border to help interdict illicit trafficking. According to the CPB's Office of Air

and Marine, unmanned aircraft in 2011 assisted with the seizure of thousands of pounds of narcotics and the apprehension of dozens of individuals taking part in illegal activities.

- UAS aided the response to the severe flooding of the Red River in the upper Midwest in April 2011. According to the U.S. Customs and Border Protections Office, which leant the UAS to the effort, the UAS mapped more than 800 nautical miles along the flooded tributaries and basins in Minnesota and North Dakota, and provided streaming video and analysis of the areas affected by the flood such as levee integrity and ice damming. The information provided by UAS gave forecasters more accurate predictions of when and where the flooding would be at its worst.
- In 2008, NASA assisted the State of California in fighting wildfires with the use of Ikhana, a UAS equipped with advanced technology. The information about the fires collected by Ikhana was transmitted to command centers within minutes, and then distributed into the field giving firefighters crucial situational awareness.
- UAS were used to help search-and-rescue teams in the aftermath of Hurricane Katrina. Scientists from the University of South Florida worked with Florida rescuers in Mississippi, in what was the first known use of small UAS for an actual disaster. Brought in to survey Pearlington, MS, within 2 hours, the responders had the data from the UAS showing that no survivors were trapped and that the flood waters from the cresting Pearl River were not posing an additional threat.

These are just a few examples of the real-world security and safety applications of UAS. And there are likely many more. As with any new revolutionary technology, all of the potential uses of UAS have probably not been thought of yet.

It's important to note, meanwhile, that, just as we recognize the beneficial security and safety functions of UAS, so too does the American public. According to a recent National poll conducted by Monmouth University in New Jersey, nearly two-thirds of Americans support the use of unmanned aircraft to protect the U.S. borders and control illegal immigration. Eighty percent of Americans support the use of unmanned aircraft to help in search-and-rescue missions.

As we further integrate UAS into the U.S. airspace and recognize the corresponding security and safety benefits, we are also mindful that UAS operations and the technology itself must be as safe as possible. Safety has always been a top priority for the industry, and we are already working with a variety of stakeholders to ensure unmanned aircraft are integrated safely into our Nation's airspace. The industry is in regular contact with the Federal Aviation Administration (FAA) and we have met with, and continue to maintain an open dialogue with, representatives from the pilot community, air traffic controllers, and others with an interest in aviation safety.

Safety is also one of three main pillars of the industry's new Code of Conduct published earlier this month. We understand and take very seriously the need to conduct UAS operations in safe manner that mitigates risk and instills confidence in our systems. Specifically with regard to safety, the guidelines recommend when and by whom UAS should be flown, address training and crew fitness requirements, call for a thorough risk assessment before each UAS flight and codify our commitment to respecting other users of the airspace, the privacy of individuals, and the concerns of the public.

UAS users are already demonstrating a commitment to safety. Case in point is the Arlington, Texas Police Department. Home to one of the most fully developed UAS programs of any local law enforcement agency in the country, the Arlington Police Department works cooperatively with the FAA to safely fly its UAS for operational missions city-wide. The department has developed pre-flight checklists, flight and squawk logs, training protocols and a standard operating procedure for all UAS flights. This is a model for the safe usage of UAS we hope to instill in manufacturers and operators through our Code of Conduct.

The UAS used by the Arlington Police Department also exemplify the types of unmanned aircraft we can expect to see more of in the coming years. The vast majority of UAS currently flying in the United States are small models that weigh under 25 pounds and can fit in the trunk of a car. The Arlington Police Department, for example, is using an 11-pound mini-helicopter, which has proven effective for surveying multi-car crashes on interstate highways. The UAS allow the crash scenes to clear more quickly, reduce pollution, and keep officers safe by reducing the amount of time they spend roadside. Even when the domestic airspace is further opened in 2015, most unmanned aircraft will be limited to no more than 55 pounds.

In addition to safe operations, the industry is committed to building safeguards into UAS technology, such as "sense and avoid" systems and other innovations,

which will enable a safe and orderly integration. For example, the U.S. Army recently completed a 2-week evaluation of a Ground Based Sense and Avoid (GBSAA) system at Dugway Proving Ground in Utah. The system uses 3-D radar and software algorithms to detect other aircraft flying in the vicinity of UAS, and safely steer UAS away from other aircraft. In both live and simulated tests, the system successfully recognized conflicts and navigated UAS away from other aircraft.

The GBSAA system provides a window into the type of "sense and avoid" technologies available for the U.S. domestic airspace. Meanwhile, the development of this particular system is ahead of schedule. The Army has said the GBSAA could be deployed as early as March 2014, 1 full year ahead of the Army's initial estimate of 2015.

In addition to "sense and avoid" systems, it is important to underscore that many UAS have multiple redundant systems that add extra layers of safety and security. This is an especially relevant point in light of the recent media attention surrounding so-called "spoofing" of a GPS signal by researchers at the University of Texas. "Spoofing" is not a new issue. Papers have been written on the subject since the 1990s and, in 2001, the U.S. Department of Transportation broadly examined vulnerabilities in the GPS system relating to aviation, maritime, and ground applications.

The industry is well-aware of "spoofing." Meanwhile, as the DOT vulnerability assessment demonstrates, "spoofing" is not a concern unique to UAS. "Spoofing" has implications for any technology that depends on GPS for guidance and timing, whether it is manned or unmanned aircraft, your cell phone, or your car. In fact, commercial airliners are relying more and more heavily on GPS signals to locate the runways at airports and, with the advent of the next generation air traffic control system, all aircraft—manned and unmanned—will rely on GPS for navigation.

At the same time, "spoofing" is not as simple or easy as news reports suggest. To successfully spoof a GPS signal, one must have the equipment and capability to broadcast a counterfeit signal at a high enough power level to overpower the GPS signals emanating from more than 20 satellites in orbit around the earth. One must know the location of the target vehicle and be able to track it. If the target vehicle is not in close proximity to the spoofing device, this requires a detection system such as radar. Meanwhile, custom software is needed to make adjustments to the target vehicle's course. It took the University of Texas team four years to develop the necessary software, and the professor overseeing the experiment has acknowledged that the skills involved in "spoofing" are "outside the capability of any average American citizen." In sum, in a controlled experiment where an aircraft is kept low to the ground, hovering in place and equipped with minimal safeguards, spoofing is feasible. Under real-world conditions, however, "spoofing" is much more difficult.

That said, the industry takes the potential for "spoofing" very seriously and is already advancing technologies, such as SAASM—Selective Availability Anti-Spoofing Module—to prevent it. SAASM, which involves the authentication of encrypted satellite signals, is already widely used by the military to thwart GPS spoofing. The Department of Defense (DOD) issued a directive that, as of October 2006, required all newly-acquired UAS systems—as well as systems going through major modifications or upgrades—to be SAASM-equipped. As has happened with other technologies, innovations developed for the military could transition in some form to the civilian market in the years to come. In fact, GPS itself was a military technology that transitioned to civilian use.

In addition to SAASM, many unmanned aircraft also have alternate navigation systems, such as radio links and backup inertial systems, which provide redundancy to GPS. Other backup technologies exist—or are being developed—that autonomously guide unmanned aircraft to a safe landing at a pre-determined location in the unlikely event of interference with navigation signals. Other "spoofing" countermeasures have been proposed since the 1990s, some of which are relatively simple software changes. Finally, it is also important to remember that while an aircraft itself may be unmanned, a trained professional is behind the controls, ready to respond, and bring a safe resolution to any problem that may arise.

Like any other technology, unmanned aircraft technology continues to become smarter and safer every day. In preparation for the expansion of UAS in the domestic airspace, AUVSI member companies have been hard at work developing new technologies that would add extra layers of safety and security to unmanned aircraft. More and more innovations will be available in the very near future.

While the industry continues to refine and enhance UAS technology, the FAA is preparing for its rule-making process, which will unfold over the next few years. In addition, later this year, the FAA is expected to announce the selection of six UAS test sites around the country. This window will provide ample time for all stake-

holders to develop a robust framework for the integration of unmanned aircraft, put the technology to the test, and resolve any outstanding issues.

Other concerns have been raised, for example, about privacy—concerns which the industry is actively working to address. AUVSI has met with nearly a dozen privacy advocates and civil liberties organizations, as well as other interested parties, to understand their concerns, encourage them to work together and let them know that, like them, AUVSI supports Americans' rights to privacy, especially the protections afforded under the Fourth Amendment to the U.S. Constitution. Meanwhile, the industry's recently released Code of Conduct clearly articulates our commitment to respecting individuals' privacy. As the integration progress, the industry will continue to engage in a constructive, thoughtful, and civil dialogue on the National, State, and local levels with all parties to address any privacy concerns.

The unmanned aircraft systems industry is committed to the safe and responsible integration of unmanned systems into the National airspace. We look forward to continuing to work with Congress, the FAA, DHS, and other stakeholders to ensure unmanned aircraft are integrated safely and responsibly, so we can unlock the tremendous potential of this technology to enhance public safety, advance scientific research, and otherwise benefit society.

LETTER FROM THE AIR LINE PILOTS ASSOCIATION INTERNATIONAL

JULY 18, 2012.

The Honorable MIKE MCCAUL,
Chairman, Oversight, Investigations, and Management Subcommittee, H2–176 Ford Building, Washington, DC 20515.

The Honorable BILL KEATING,
Ranking Member, Oversight, Investigations, and Management Subcommittee, H2–117 Ford Building, Washington, DC 20515.

DEAR CHAIRMAN MCCAUL AND REPRESENTATIVE KEATING: The Air Line Pilots Association, International (ALPA) represents the safety and security interests of more than 53,000 professional airline pilots flying for 37 airlines in the United States and Canada. On their behalf, I respectfully request ALPA's views be included in the hearing record for the upcoming hearing on "Using Unmanned Aerial Systems (UAS) Within the Homeland: Security Game-Changer?" ALPA is the world's largest professional pilot association and the world's largest non-Governmental aviation safety organization. As such, we are pleased the subcommittee is holding this hearing and appreciate your oversight and continued interest in the subject of unmanned aircraft systems.

The much-publicized success of Unmanned Aircraft Systems (UAS) in combat operations has created a large potential market for the use of these aircraft by commercial enterprises. The FAA has managed the process of accommodating UAS into the National Airspace System (NAS) since it began. Currently, several UAS are in domestic use by Government agencies (e.g., law enforcement, Customs Border Protection (CBP), agriculture, etc.) operating with FAA Certificates of Authorization (COA) in segregated airspace. As the number of these aircraft increases, and the potential for business applications also increases, so does pressure to allow their unrestricted operation in the NAS. FAA has recognized the need for regulations, standards development, and oversight unique to future domestic UAS operations in the NAS and has, for several years, proactively worked with industry stakeholders to develop those standards and regulations. This process is extremely complex and draws on the expertise of both industry stakeholders and FAA specialists in air traffic control, airspace management, equipment certification and other disciplines with a direct bearing on the safety and security of flight operations of UAS in the NAS.

ALPA recognizes the benefits that UAS may provide valuable National defense and law enforcement functions domestically. However, the introduction of such aircraft into an integrated National airspace system represents an entirely new concept that has the potential to profoundly degrade the safety of both commercial and general aviation flight operations if this integration is not accomplished in a responsible, comprehensive manner. To achieve the complex goals of safe and secure UAS integration in the NAS, the most capable agency to provide effective oversight would be the one that is currently the specialist agency in all aspects of aviation. FAA has decades of experience with safely integrating new technologies and concepts into the NAS and has the experience, knowledge, and expertise to provide harmonized regulatory standards and oversight to the many stakeholders to maintain aviation safety and security of NAS. While DHS can, and should continue to, provide expertise in the threats that must be mitigated, it is FAA with the expertise to develop and im-

plement those mitigations. This relationship is true for all aircraft operating in the NAS, regardless of where the pilot sits.

There are significant industry and Government regulatory and standards development activities already under way in North America and other parts of the world oriented toward addressing the challenges and concerns associated with attempts to integrate UAS into unsegregated airspace with the entire spectrum of civil traffic. FAA is central to these developments, and has partnered with numerous other agencies including the Department of Defense (DOD), the National Aeronautics and Space Administration (NASA), the Federal Aviation Administration (FAA), Transport Canada, and RTCA in the United States and its counterpart EUROCAE in Europe. The International Civil Aviation Organization (ICAO) has published a circular to guide the development of harmonized standards and practices for UAS. FAA is the lead U.S. Government agency in those international developments. In addition, in the United States, the FAA is in the process of selecting six UAS Test Site facilities to further develop technologies that enhance future aviation safety and security. RTCA is currently producing substantive recommendations for UAS standards for aviation safety and security for the FAA, as well. For further information regarding present and future issues of UAS relating to NAS safety and security integration, I refer you to the white paper attached, "Unmanned Aircraft Systems, Challenges for Safely Operating in the National Airspace System" and ask that this material be included in the hearing record as well.*

Unmanned Aircraft Systems approval for operations in the NAS requires comprehensive and exhaustive total system analysis to achieve integration. The needs of air traffic services, airspace, airports, airmen, and operators all will need to be evaluated to safely and securely integrate the UAS into the complex and dynamic operations of the NAS. There are also technological requirements inherently unique to the UAS and, therefore the regulator's expertise must not be limited to certification of just the aircraft, but also the complete system, including the data link infrastructure, g round control station, as well as the security of the ground control station that contain both the pilot(s) and communication components. The FAA processes are synonymous with safety of NAS and responsibility for those processes should reside with them. The current role played by TSA and DHS in identifying and mitigating threats to the security of operation NAS should similarly be maintained.

To maintain the exceptional level of safety in the NAS, it is the FAA that must evaluate the safety, operational, and security procedures that may need to be modified to provide for unique UAS requirements. As with all certified aircraft, furthering the understanding of the design and limitations of the aircraft will be required so that appropriate levels of safety and security assurances can be developed. ALPA has always been a vanguard of aviation safety, and we have worked as a stakeholder with the FAA for many years and are convinced that the thorough current certification processes of the FAA have the breadth and scope to continue to safely and securely maintain aviation safety during the entire current and future certification programs for UAS aircraft, pilots, and operators.

We appreciate the subcommittee's interest in this issue and look forward to continuing our work together to protect the security of the Nation's airspace.

Sincerely,

CAPTAIN LEE MOAK,
President, Air Line Pilots Association, International.

Mr. MCCAUL. Members are reminded that statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

JULY 19, 2012

I would first like to thank Chairman McCaul for holding this hearing on a very timely subject.

In February, President Obama signed the *Federal Aviation Administration Reauthorization Act* into law.

Included in the Act was a provision directing the Federal Aviation Administration (FAA), to rapidly expand the ability of public agencies—including State and local law enforcement—to use Unmanned Aerial Vehicles, or UAVs, to fulfill their missions.

*The document has been retained in committee files.

The use of UAVs within the homeland is not a new concept.

Following Hurricane Katrina, UAVs played a vital role in surveying storm-damaged communities and assisting in the search and rescue of trapped survivors in Mississippi and other areas affected by the storm.

Moreover, since 2004, the U.S. Customs and Border Protection (CBP), within the Department of Homeland Security has deployed UAVs along the Southwestern Border as a force-multiplier in its border security efforts.

CBP recently announced its intention to increase its fleet of 10 UAVs to 24 by the year 2016.

Clearly, UAVs have many beneficial uses in the National airspace and, when used within proper parameters, can serve as an important tool in securing the homeland.

However, the use of UAVs in our National airspace may be expanding at a faster rate than the legal protections governing its use.

In late 2010, there were 273 active Government-licensed UAVs, nearly 100 more than the previous year. Reports in 2012 demonstrate that the FAA has issued more than 300 UAV licenses.

Yet, according to the Government Accountability Office, "no Federal agency has specific statutory responsibility to regulate privacy matters related to UAVs."

Despite the Department of Homeland Security's role as the leading Federal agency operating UAVs, its Chief Privacy Officer has never performed a Privacy Impact Assessment on UAVs or developed safeguards and guidelines for ensuring that privacy protections are in place.

Furthermore, although FAA is responsible for incorporating UAVs into our National airspace, according to its website: "the FAA's sole mission and authority as it focuses on the integration of unmanned aircraft systems is safety."

So, who is watching the henhouse, with respect to privacy?

That is the question that causes me concern.

UAVs are capable of hovering in the same spot for up to 30 hours and recent reports indicate that in the near future, 45 hours is not out of the question.

They can find and follow a single target or up to 65; utilize facial recognition software to find a face in a crowd or an event; read license plates from the sky; and some can even shoot taser projectiles, tear gas, and rubber balls from 300 feet above ground.

Given these capabilities, there is the potential for invasive surveillance and warrantless searches with little to no privacy protections in place.

Like my colleagues, I strongly support providing homeland security officials and law enforcement agencies with the tools they need to carry out their vital work on behalf of our Nation.

However, we have a responsibility to ensure that as technology develops and our systems become more sophisticated, proper safeguards and protections are in place to ensure the right to privacy is maintained.

I look forward to hearing from our witnesses and thank them for appearing before us today.

I yield back.

Mr. MCCAUL. The Chairman now will go to the panel and introduce Dr. Todd Humphreys I had the pleasure to visit yesterday, and being from Austin I take particular pride that you are here also today, and growing up in a family of Long Horns, I take even more in that as well. So I have a little bit of orange blood in myself.

Dr. Todd Humphreys is an Assistant Professor at the Cockrell School of Engineering at the University of Texas at Austin. He specializes in the application of optimal estimation techniques to problems in satellite navigation, orbital and attitude dynamics, and signal processing. For anybody here who understands that, other than Dr. Humphreys, congratulations to you.

He directs the radio navigation laboratory at UT Austin, where his current research focuses on defending against intentional GPS spoofing and jamming. Most recently Dr. Humphreys uncovered that GPS signals that navigate unmanned aerial systems can be hijacked and controlled. He conducted experiments at White Sands Missile Range with the Department of Homeland Security, and Dr. Humphreys—and also I believe at the Memorial Stadium in Aus-

tin. I believe we will see a video that describes that. He obtained his doctorate from Cornell University.

The Chairman now recognizes Dr. Humphreys for his opening statement.

STATEMENT OF TODD E. HUMPHREYS, PH.D., ASSISTANT PROFESSOR, COCKRELL SCHOOL OF ENGINEERING, THE UNIVERSITY OF TEXAS AT AUSTIN

Mr. HUMPHREYS. Chairman McCaul, Members of the subcommittee, you may have heard these reports mentioned by Chairman McCaul that at about this time last month my students and I from the University of Texas hijacked a civilian unmanned aerial vehicle, a small helicopter, and brought it down from a remote location. That much is true, and I have come today prepared to talk about what we did, what the implications are for the National airspace, and what can be done to address the problem that our experiment brought to the fore.

So how did we hijack this UAV, this small helicopter? We exploited a weakness in the Global Positioning System. You see, GPS signals come in two flavors. There are the military signals which are encrypted to prevent counterfeiting and unauthorized use. Then there are the second class of signals, civilian signals, and these signals are not encrypted. They are freely accessible and that has explained—that explains their enormous popularity, their usefulness, but it also opens up a vulnerability. It makes them easy to counterfeit or, in other words, to spoof.

Just like monopoly money, they have a detailed structure but they don't have any built-in protection against counterfeiting or spoofing.

So what does this have to do with UAVs? Well, the connection is fairly obvious. Almost all civilian UAVs depend heavily on civil GPS for their navigation, and that means that if you can convincingly fake a GPS signal you can fool a UAV into tracking your signal instead of the authentic one, and at that point you can control the UAV. You make it move left or right, front or back, up or down. In other words, you have hijacked the UAV, and you can do this from miles away.

My friends at the University of Texas have prepared a video that I would like to show you which illustrates what we did and helps me to explain the technique involved.

You see against the background here, a UAV, an animated one, like the one we used, flying above the desert floor. This white person entering your picture is the good guy. He is the UAV's remote operator and he is now uploading to the UAV a way point. That white diamond is a destination the UAV is supposed to move to. The GPS satellites above help the UAV locate itself and as you can see here, it recognizes where it is, where the destination is, and makes its tracks toward the destination lining up nicely with its goal.

But the bad guy moving in here from the left is a spoofer operator, and he is going to transmit fake GPS signals to the UAV. At this point, we will pause so that I can talk a little bit about what you see on the screen. The peak you see on the screen exists in every GPS receiver. It corresponds to the authentic signals. You

can go ahead and roll it now. But if you can create fake GPS signals, you have caused another peak to appear, and that peak, when it lines up with the authentic one, ends up hijacking the tracking loops inside the GPS receiver, and what you will notice is that as it draws off the tracking loops, a ghost UAV slides out the back. That ghost UAV is where now the UAV thinks it is. It is not its actual location, it is its perceived location. As it moves toward its way point it is the ghost UAV that lines up the way point instead of the actual UAV.

We did the same here at Texas Memorial Stadium by making our UAV think that it was rising upward at a fast clip, and you will see here that in response it falls downward. We can go ahead and roll it. The bar at the bottom will tell you who is in control. At first it is the authentic signals and the ground controller who is in control of this UAV, but at this point when they go red, it is now the spoofer, the hijacker, who controls the UAV and you will see that it drops precipitously toward the ground. That is all under control of this remote hijacker.

Then at White Sands we were invited by the Department of Homeland Security or authorized by the Department Security, and in fact they facilitated some of this test, so that we could conduct a test over the air where we capture the UAV in mid-air. We did it from about a half-mile away. On a hilltop, we broadcast our signals. You can go ahead and roll it now, and you will see that in this case, as in the former case, the UAV started in a nice hovering position but then came straight down as if it were an elevator moving down a shaft entirely under control of the remote hacker.

So what are the implications for our National airspace? Well, back in February, Congress handed a mandate, the Federal Aviation Administration, to develop a comprehensive plan for safely accelerating the integration of civil UAVs into the National airspace system, and I believe that the results of our demonstration should factor heavily into that plan. But the truth is that the FAA is, its culture and its expertise is geared more toward safety than security and our test implicated the security of the airspace. So I think it is fair to say that the DHS may have also a role to play in drawing up these new rules and regulations, and I am happy to entertain questions from the committee.

[The statement of Mr. Humphreys follows:]

PREPARED STATEMENT OF TODD E. HUMPHREYS

JULY 18, 2012

1. SUMMARY

Military Global Positioning System (GPS) signals have long been encrypted to prevent counterfeiting and unauthorized use. Civil GPS signals, on the other hand, were designed as an open standard, freely accessible to all. These virtues have made civil GPS enormously popular, but the transparency and predictability of its signals give rise to a dangerous weakness: They can be easily counterfeited, or spoofed. Like Monopoly money, civil GPS signals have a detailed structure but no built-in protection against counterfeiting. Civil GPS is the most popular unauthenticated protocol in the world.

The vulnerability of civil GPS to spoofing has serious implications for civil unmanned aerial vehicles (UAVs), as was recently illustrated by a dramatic remote hijacking of a UAV at White Sands Missile Range. The demonstration was conducted by the University of Texas Radionavigation Laboratory at the behest of the Department of Homeland Security (DHS). From a stand-off range of a half mile, the Uni-

versity spoofer commandeered the UAV and induced it to plummet toward the desert floor. The results of this demonstration will no doubt factor into the Federal Aviation Administration's (FAA's) plans for integrating UAVs into the National airspace.

Hacking a UAV by GPS spoofing is but one expression of a larger problem: Insecure civil GPS technology has over the last 2 decades been absorbed deeply into critical systems within our National infrastructure. Besides UAVs, civil GPS spoofing also presents a danger to manned aircraft, maritime craft, communications systems, banking and finance institutions, and the National power grid.

Constructing from scratch a sophisticated GPS spoofer like the one developed by the University of Texas is not easy. It is not within the capability of the average person on the street, or even the average Anonymous hacker. But the emerging tools of software-defined radio and the availability of GPS signal simulators are putting spoofers within reach of ordinary malefactors.

There is no quick, easy, and cheap fix for the civil GPS spoofing problem. What is more, not even the most effective GPS spoofing defenses are fool-proof. But reasonable, cost-effective spoofing defenses exist which, if implemented, will make successful spoofing much harder.

I recommend that for non-recreational operation in the National airspace civil UAVs exceeding 18 lbs be required to employ navigation systems that are spoof-resistant.

More broadly, I recommend that GPS-based timing or navigation systems having a non-trivial role in systems designated by DHS as National critical infrastructure be required to be spoof-resistant.

Finally, I recommend that the DHS commit to funding development and implementation of a cryptographic authentication signature in one of the existing or forthcoming civil GPS signals.

2. BACKGROUND

The design of the Global Positioning System came together over Labor Day weekend in 1973. A group of hard-working engineers, mostly Air Force officers, decided over that weekend that the GPS satellites would broadcast two different types of signals, a precise military signal and a so-called clear access or C/A signal. The military signal would later be encrypted to prevent unauthorized use and imitation.

But the clear access signal, true to its name, would be freely accessible to all. Detailed and accurate specifications for the clear access signal were later distributed to encourage its use.

The early designers of the GPS system, for whose tireless efforts we are all indebted, knew the GPS was going to be valuable for civilians across the globe, but they never could have imagined just how valuable. An intentional degradation of the C/A signals called selective availability was discontinued by Presidential Order in 2000. Instantaneously, every GPS receiver across the globe went from errors the size of a football field to errors the size of a small room. It is hard to overstate the impact of this improvement in accuracy. Before selective availability was turned off, there were no in-car navigation systems giving turn-by-turn directions, because back then civilian GPS couldn't tell you what block you were on, let alone what street. For geolocation, accuracy matters.

Things have only improved over the last decade. With more ground stations, better algorithms, more open-access signals, and better receivers, civil GPS—the family of open-access signals to which all civilians have access—can now tell you not only what street you are on, but what part of the street.

The accuracy, transparency, and low cost of civil GPS have enabled a firestorm of innovation. After 2000, any engineer designing a system for which accurate timing or location was important found GPS to be an almost irresistible option. As a result, civil GPS receivers are built deeply into our National infrastructure: From our smartphones to our cars to the internet to the power grid to our banking and finance institutions. Some call GPS the invisible utility: It works silently, and for the most part perfectly reliably, in devices all around us—devices of which we are scarcely aware.

Nearly 40 years after the GPS design was put together we can look back and marvel at its designers' foresight. The GPS that we all depend on today is nearly identical to their original design. But with 40 years of hindsight, many of us in the GPS community, if we could be transported back to those seminal meetings over Labor Day weekend in 1973, would suggest that one crucial change be made to the clear access signal.

The problem is that the same transparency and predictability that have made civil GPS signals so wildly popular all across the globe give rise to a dangerous vul-

nerability. Transparency and predictability make the civil GPS signals easy to imitate—to counterfeit. The fact is that civil GPS signals are like Monopoly money: They have a detailed structure but no built-in protection against forgery.

That civil GPS is so easy to counterfeit, or "spoof," would not be a problem if GPS were not so popular, its use so widespread. But such is not the case.

For the past few years my students and I at the University of Texas Radionavigation Laboratory, and several others in the GPS community, have had two goals with regard to GPS security. First, we aim to alert GPS device manufacturers, the public, and public officials that civil GPS—notwithstanding its spectacular utility and historical reliability—is inherently insecure and shouldn't be trusted blindly. Second, we endeavor to develop practical and effective techniques to fix the problem, to make GPS secure and trustworthy for civilian users. The remainder of this statement is a brief summary of our major findings and recommendations to date.

3. EXAMPLE CASE: HIJACKING A UAV BY CIVIL GPS SPOOFING

What implications follow from the lack of authentication on civil GPS signals? Consider unmanned aerial vehicles (UAVs). In February 2012 the U.S. Congress passed the FAA Modernization and Reform Act, which gives the FAA until 2015 to develop a "comprehensive plan for safely accelerating the integration of civil UAVs into the National airspace system." The Modernization Act has spurred a great deal of discussion. Hobbyists, public safety officials, academics, UAV manufacturers, and many in the general public envision myriad beneficial applications of civil UAVs. Others, less sanguine, point out that UAVs threaten to invade our privacy. Still others question whether UAVs can be integrated safely into the National airspace.

The connection between civil UAVs and civil GPS is straightforward: The vast majority of civil UAVs depend on civil GPS for navigation. It is true that the navigation sensor suite of a typical civil UAV also includes inertial sensors (accelerometers and rate sensors), magnetometers, altimeters, and in some cases a camera; even so, GPS is fundamental to the sensor suite because, unlike the other navigation sensors, it works in all weather conditions and does not drift.

Does the dependence of UAVs on civil GPS make them susceptible to hijacking via GPS spoofing? In February 2012 the University of Texas Radionavigation Laboratory posed this question to the DHS. DHS considered the question seriously. At the time, DHS was moving forward with plans to offer universities and other interested civilian groups a chance to test their proposed techniques for addressing civil GPS vulnerabilities in a series of realistic over-the-air tests at White Sands Missile Range. My students and I proposed to DHS an experiment whereby we would attempt to commandeer a civilian UAV by GPS spoofing. DHS agreed to the test on the condition that the University of Texas furnish all the necessary manpower and equipment—including the target UAV.

Our group selected a Hornet Mini from Adaptive Flight as the target UAV. This sophisticated $80k rotorcraft, used by law enforcement, has a navigation system built around an extended Kalman filter that draws measurements from an altimeter, a magnetometer, an inertial measurement unit, and a civil L1 C/A GPS receiver. The Hornet Mini's sensor suite and flight control system are representative of those in much larger commercial UAVs.

It is important to note that the Hornet Mini's GPS receiver was equipped with a standard technology called Receiver Autonomous Integrity Monitoring (RAIM), which is designed to identify and discard GPS signals that appear to be outliers. Standard RAIM is ineffective against GPS spoofing because a spoofer generates a fully self-consistent ensemble of spoofing signals; there are no outliers.

After a dry run on the University of Texas campus, our research group traveled to White Sands for the test of record. The test was conducted as follows: A sophisticated civil GPS spoofer developed in our laboratory was placed on a hilltop about a half mile from the designated test site where the UAV would be flying. The UAV was commanded by its ground control operator to hover 50 feet above the ground at the test site. On command, our spoofer began transmitting weak counterfeit GPS signals toward the hovering UAV, achieving meter-level alignment with the counterpart authentic signals at the location of the UAV's GPS antenna. The spoofer then rapidly increased its counterfeit signal power, bringing the UAV under its control. By inducing a false upward drift in the UAV's perceived location, the spoofer fooled the UAV's flight controller into commanding a dive. At about 10 feet above ground level a human safety pilot assumed manual control of the UAV to prevent it from crashing.

Between this and other tests, the spoofer demonstrated short-term three-dimensional control of the UAV. Thus, we conclude that it is indeed possible to hijack a civil UAV—in this case, a fairly sophisticated one—by civil GPS spoofing.

4. THE LARGER PROBLEM

The vulnerability of civil UAVs to GPS spoofing is but one expression of a more fundamental problem: the insecurity of civil GPS signals. If a UAV can be hijacked by GPS spoofing, what else could go wrong within our GPS-dependent National infrastructure? In what follows, the potential vulnerabilities of our National transportation, communications, banking and finance, and energy distribution infrastructure are discussed briefly.

4.1 Transportation

In 2001, the U.S. Department of Transportation issued a report assessing the vulnerability of the U.S. transportation infrastructure to disruption of civil GPS.[1] Known as the Volpe report, it highlighted the threats posed by civil GPS spoofing attacks. At the time, the open literature contained little research on such attacks and possible countermeasures. Accordingly, the report recommended further study of GPS spoofing and development of civil GPS anti-spoofing techniques. Unfortunately, despite a flurry of GPS security research over the past decade, brought about in part by the Volpe report, no dedicated spoofing defenses have been built into any commercially-available GPS receivers so far as I am aware. This means that the GPS receivers used in commercial and general aviation aircraft, in maritime vessels, and in surface vehicle transport are vulnerable to GPS spoofing just as was the GPS receiver on the UAV tested at White Sands.

4.1.1 Manned Aviation

Manned civil aircraft increasingly depend on civil GPS for navigation. Nonetheless, they are currently somewhat less vulnerable than civil UAVs to GPS spoofing for two reasons:

(1) All commercial aircraft and many general aviation aircraft continue to operate legacy VOR/DME navigation equipment along with newer GPS equipment. Because of their higher power, VOR/DME signals are less vulnerable to spoofing than GPS signals. Legacy VOR/DME equipment can provide pilots a valuable cross-check against which to compare GPS-produced position and velocity data.

(2) Manned aircraft are typically equipped with higher-quality (lower drift) inertial measurement units (IMUs) than those used in small UAVs, which means that the GPS navigation solution can be more effectively cross-checked against the IMU. Whereas a spoofer might be able to induce a fictitious acceleration of 0.5 m/s^2 in a small UAV without being detected in a cross-check against the (relatively poor) IMU, an attack against a larger craft with a higher-quality IMU might be limited to an induced acceleration of 0.1 m/s^2. However, it should be noted that the benefit of a higher-quality IMU is only realized if the navigation systems is designed to be on the lookout for suspicious accelerations in the GPS solution.

Despite these advantages, GPS spoofing remains a significant risk to civil manned aircraft. When the aircraft's autopilot is engaged, the course it commands depends primarily on the aircraft's IMU. However, GPS plays a role in estimating the bias drift in each of the IMU's axes. Thus, neither the autopilot nor the human pilot(s) may notice a spoofer-induced navigation error that builds up gradually over time. Pilots are trained to continually monitor the autopilot for errant behavior, and disengage it if necessary, but they rely on anomaly alerts provided by the aircraft's navigation system itself. I have reason to believe that the resilience of commercial aircraft navigation systems to civil GPS spoofing has not been sufficiently tested. Roll-out of the FAA's NextGen air traffic control system, which will further increase the reliance of commercial and general aviation on civil GPS, would seem to demand even greater scrutiny as regards vulnerability to GPS spoofing.

4.1.2 Maritime

Many of the adverse effects of GPS spoofing in maritime applications follow the pattern of those in aviation applications. As with aircraft, marine craft rely on civil GPS to estimate the bias drift in their inertial sensors. This reliance opens up an indirect vulnerability to GPS spoofing. Marine vessels may in fact be more vulnerable than aircraft to spoofing because the discontinuation of LORAN in the United States 2 years ago left them with fewer radionavigation backups to GPS. It should be noted that differential GPS, often used for improved navigation accuracy on marine craft, is not a defense against GPS spoofing.

---

[1] Anon., "Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System," tech. rep., John A. Volpe National Transportation Systems Center, 2001.

Many marine craft autopilot systems could likely be induced by GPS spoofing to veer gradually off course, which could be especially dangerous in constricted waterways. And whereas formal trials have been conducted to evaluate the effect of GPS jamming on commercial marine craft (with alarming results—see the tests conducted in the North Sea by the U.K. Lighthouse Authority), to my knowledge no such tests have been performed to evaluate the effects of GPS spoofing.

4.1.3 Surface Transportation

The reliance of surface transportation on civil GPS is collectively greater than that of aviation or maritime transportation, but the nature of the reliance is different, being attached to far less worrisome consequences. A spoofing attack against an automobile could induce the in-car navigation system to display a false position, which may confuse the driver, but would be unlikely to result in an accident. In the case of autonomous vehicles such as the Google autonomous car, a substantial suspicion of GPS is built into the navigation system. GPS measurements are used to estimate the biases in inertial sensors, but LIDAR, RADAR, and optical sensors are also used for this purpose and their measurements are constantly cross-checked against GPS. The robustness of the Google autonomous car to loss of GPS or GPS spoofing is a good model for all autonomous systems in their use of GPS.

Rail transport employing so-called Positive Train Control (PTC) systems, which automatically locate a train on a digital map in the on-board and control center computers, may be susceptible to civil GPS spoofing. A GPS spoofing attack mounted against a PTC-enabled train at a railway switch may be able to deceive the train operator and the control center monitors into thinking that the train is moving along a different track.

4.2 Communications

Many communications networks, including cellular networks and the internet, rely on civil GPS for precise timing. The discussion here will focus on cellular networks because these have stringent synchronization requirements.

Code division multiple access (CDMA) cell-phone towers rely on GPS timing for tower-to-tower synchronization. Synchronization prevents towers from interfering with one another and enables call hand-off between towers. If a particular tower's time estimate deviates more than 10 μs from GPS time, hand-off to and from that tower is disrupted. In laboratory tests conducted at the University of Texas we have demonstrated that a spoofer can induce a 10-μs time deviation in less than 30 minutes when acting against a typical CDMA tower setup. A spoofer, or spoofer network, could also cause multiple neighboring towers to interfere with one another. This is possible because CDMA cell-phone towers all employ the same spreading code, distinguishing themselves only by the phasing (that is, the relative time offset) of their spreading codes. Furthermore, it appears that a spoofer could impair CDMA-based E911 user-location.

4.3 Banking and Finance

All global financial exchanges, including the New York Stock Exchange (NYSE) and the Nasdaq, have gone digital. Large data centers hold the exchanges' matching engines, the modern-day equivalent of the historic trading floor, in racks of interconnected servers. The DHS considers these data centers critical National infrastructure. Private security personnel, tall fences, and the best network security money can buy protect the integrity of the thousands of high-stakes trades executed every second within these data centers.

But there is one input port that the network firewalls leave entirely unprotected. An unassuming set of antennas on the roof of these data centers carry unsecured civil GPS signals directly into the core of the matching engine network. Slaved to a once-per-second synchronization pulse from a GPS-disciplined clock, the individual servers in the network apply time stamps to the trades they execute. A decade ago, a tenth of a second was an acceptable time stamp resolution. High-frequency traders now demand nanoseconds.

I believe that all major financial exchanges across the globe are aware of the GPS spoofing threat. I have been in indirect contact with network service managers at the NYSE, BATS, and London exchanges; they have each taken precautions against GPS spoofing. For example, system time at the NYSE is ultimately traced to civil GPS, but a spoofing attack that shifted the apparent GPS time by more than 0.05 nanoseconds per second would fail a timing consistency check against redundant local atomic clocks. This would limit a spoofer to shifting the exchange's system time by less than 5 microseconds per day, making the NYSE system time an attractive target only for the most patient of spoofers.

High-frequency traders whose servers are co-located with the matching engines at major exchanges may be more vulnerable to GPS spoofing. In the NYSE and some

other exchanges, these co-located customers are offered either a timing feed from the exchange's system time or a direct feed from GPS antennas on the roof. Many co-located customers, distrustful of the exchange's system time, opt for the direct GPS feed. In laboratory tests conducted at the University of Texas we have shown that a popular model of GPS-disciplined oscillator used by these co-located customers is incapable of detecting GPS spoofing attacks that shift timing by less than 100 nanoseconds per second—or 2,000 times faster than the maximum undetectable rate when targeting NYSE system time.

Why could this be a problem? Automated transactions initiated by co-located servers account for 50 to 70 percent of the trading volume on major exchanges. The high-frequency traders who own the servers do not like inexplicable market behavior, and unlike old-fashioned traders who are obligated to stay in the market no matter its behavior, high-frequency traders can pull the plug at any moment. In the aftermath of the May 6, 2010 flash crash, it was revealed that automatic data integrity checks in trading algorithms were configured to trigger on unusual latency in the exchanges data feeds. In other words, if transaction time stamps do not look right, algorithmic traders flee the marketplace. A spoofing attack that aggressively manipulated the timing in a large number of co-located servers could therefore cause a partial market vacuum—what traders call a loss of liquidity—with the result being increased price volatility and damage to market confidence.

4.4 Energy Distribution

In a recent study, our laboratory examined the vulnerability of a particular type of smart grid equipment, the phasor measurement unit (PMU), to a timing attack.[2] If a spoofer manipulates a PMU's time stamps, it could cause spurious variations in measured phase angles. These variations could distort power flow or stability estimates in such a way that grid operators or automatic response systems would take incorrect or unnecessary control actions, including powering up or shutting down generators, potentially causing blackouts or damage to power-grid equipment. Under normal circumstances, a changing separation in the phase angle between two PMUs indicates changes in power flow between the regions measured by each PMU. Thus, a spoofing attack could create the false indications of power flow across the grid.

Under controlled experimental conditions at a Department of Energy National laboratory, we demonstrated last December that a GPS-spoofer-induced timing offset does indeed create a proportional offset in the voltage phase angle measured by a PMU. In a brief examination of the consequences of such an offset, we found that future smart grids will likely employ advanced PMUs in automated closed-loop grid control[3] and that such closed-loop control has already been implemented in at least one network.[4] We have reason to believe that timing manipulation would cause generators to trip in this network and in future automated closed-loop grid control networks.[2]

5. ASSESSING THE RISK

A thorough assessment of the spoofing risk would investigate two factors: (1) The probability, and (2) the consequences of an attack. The foregoing section presented various consequences, though certainly not a thorough listing, related to critical National infrastructure. The probability of a spoofing attack is a function of the incentives that would prompt an attack and the difficulty of mounting one. As an investigation of incentives is necessarily subjective and, in any case, outside my expertise, I will leave this to others, focusing here on assessing the difficulty of mounting a spoofing attack.

5.1 What Does it Take to Build a Spoofer?

Constructing from scratch a sophisticated GPS spoofer like the one developed by the University of Texas is not easy. It is not within the capability of the average person on the street, or even the average Anonymous hacker. It is orders of magnitude harder than developing a GPS jammer. Nonetheless, the trend toward software-defined GNSS receivers for research and development, where receiver

[2] D. Shepard, T. Humphreys, and A. Fansler, "Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing," in *Sixth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection,* (Washington, DC), 2012.

[3] J. Giri, D. Sun, and R. Avila-Rosales, "Wanted: A more intelligent grid," *IEEE Power & Energy,* pp. 34–40, April 2009.

[4] E.O. Schweitzer, A. Guzman, H.J. Altuve, and D.A. Tziouvaras, "Real-time synchrophasor appliactions for wide-area protection, control, and monitoring," tech. rep., Schweitzer Eng. Laboratories, 2009.

functionality is defined entirely in software downstream of the A/D converter, has, in recent years, significantly lowered the bar to developing a spoofer.

5.1.1 Cost of Hardware

The University of Texas spoofer was constructed almost entirely from commercial off-the-shelf components. The total hardware cost was between $1k and $2k. Universal software radio platforms that rival the capability of our hardware system can be purchased for less than $2k.

5.1.2 Required Skill and Effort

As a point of reference, I estimate that there are more than 100 researchers in universities across the globe who are well-enough-versed in software-defined GPS that they could develop a sophisticated spoofer from scratch with a year of dedicated effort. Spoofer development is likely outside the capability of organized crime or terrorist organizations without access to advanced training, but is well within the capability of near-peer nation states.

5.2 Can One Buy a Spoofer?

Unlike GPS jammers, marketed by overseas firms as "personal privacy devices" and sold by the thousands on the internet, sophisticated GPS spoofers such as the one developed by the University of Texas Radionavigation Laboratory cannot currently be obtained in any market of which I am aware. However, a GPS signal simulator, a piece of test equipment that is readily obtainable from various vendors, can serve as an unsophisticated yet effective GPS spoofer. A sophisticated spoofer is only different from a GPS signal simulator in the following respects:

(1) It is capable of predicting, with nearly 100% accuracy, the navigation data sequence that modulates the GPS signals—not just the implied orbital and clock data, but the exact sequence. This same effect can be realized on a standard GPS signal simulator only by developing a secondary system that generates blocks of predicted navigation data and uploads these to the signal simulator.

(2) A sophisticated spoofer is capable of precisely aligning (within a few meters equivalent) the codes in its counterfeit signals with the corresponding codes of the authentic signals at the location of the target receiver's antenna. The University of Texas spoofer is capable of achieving this alignment from a standoff distance of several kilometers. An off-the-shelf GPS signal simulator would have to be substantially modified to achieve such alignment.

These differences are only important if one wishes to carry out a stealthy spoofing attack, that is, one that effects a near-seamless transition from authentic to counterfeit signals and is therefore difficult to detect by simple timing and signal checks within the target system. But this is hardly necessary for a successful attack against most targets at present, given that few GPS-based systems perform even these rudimentary checks. Indeed, a vulnerability assessment team from Los Alamos National Lab convincingly demonstrated over a decade ago that an off-the-shelf GPS signal simulator is sufficient to mount a spoofing attack,[5] and spoofing defenses in commercial receivers have hardly progressed since that time.

High-end commercial GPS signal simulators cost several hundred thousand dollars, but these can be leased for a few hundred dollars on a weekly basis. Moreover, within the past few years much less expensive (less than $40k) single-frequency GPS signal simulators have emerged on the market. GPS signal record-and-playback devices, which can be purchased for a few thousand dollars, can also be used effectively as unsophisticated spoofers.

5.3 Range and Required Knowledge of Target

Assuming one could build or otherwise obtain a spoofing device, a successful spoofing attack further requires proximity to and knowledge of the target system.

5.3.1 At What Standoff Range Can a Spoofer Be Effective?

The University of Texas Radionavigation Laboratory demonstrated a successful spoofing attack from a 0.62-km standoff range in our over-the-air test at White Sands. Our spoofer's maximum standoff range is fundamentally limited only by the spoofer's need to track all or nearly all of the authentic GPS signals seen by the target receiver, which implies an operational range of several tens of kilometers. A spoofer's broadcast power requirement, even at a stand-off range of several kilometers, is quite modest because the authentic GPS signals are themselves extremely weak.

[5] J.S. Warner and R.G. Johnston, "A simple demonstration that the GPS is vulnerable to spoofing," *The Journal of Security Administration,* vol. 25, pp. 19–28, 2002.

5.3.2 What Must the Spoofer Know About the Target to Be Effective?

For a near-seamless transition from authentic to counterfeit signals, and, in the case of UAV spoofing, for fine-grained control of the UAV after capture, a spoofer must be furnished with real-time estimates of the target system's location and velocity accurate to within a few meters and meters per second, respectively. This represents a substantial challenge for a would-be spoofer. In the case of UAV spoofing it implies that the UAV is being accurately tracked by a RADAR or LIDAR system. However, if a spoofer operator's goal is simply to confuse the target's navigation or timing system, and the operator is unconcerned about possible detection, then knowledge of the target's position and velocity is unnecessary.

6. FIXING THE PROBLEM: WHAT CAN BE DONE TO DEFEND AGAINST GPS SPOOFING?

There is no quick, easy, and cheap fix for the civil GPS spoofing problem. Moreover, not even the most effective GPS spoofing defenses are foolproof. In contrast to message authentication, such as is used to sign data transmitted across the internet, the security of GPS signal authentication is much weaker and demands a probabilistic model. Nonetheless, there are many possible remedies to the spoofing problem that, while not foolproof, would vastly improve civil GPS security. For discussion, it is convenient to categorize spoofing defenses along two axes: (1) Cryptographic or non-cryptographic, and (2) networked or stand-alone. A cryptographic spoofing defense relies on secret keys that encrypt or digitally sign components of the broadcast signals, whereas a non-cryptographic defense does not depend on encryption or digital signatures. A networked defense requires a (possibly intermittent) link to a communications network whereas a stand-alone defense operates in isolation of a network.

Our laboratory has been engaged in developing civil GPS spoofing defenses over the past several years. In addition, a number of other researchers have proposed civil GPS spoofing defenses in the open literature or have otherwise disclosed their ideas to me. In what follows, I examine each of the proposed techniques of which I am aware. More promising techniques approach the ideal spoofing defense, which: (1) Would reliably detect a sophisticated spoofing attack such as the one conducted at White Sands with a low probability of false alarm, (2) could be implemented in the short term, (3) would not significantly increase the cost of a GPS-based navigation system, and (4) would be applicable to a broad range of GPS-dependent systems.

It should be noted at the outset that a military-style spoofing defense, in which the transmitted signals are fully encrypted, is not appropriate for the civilian sector as it denies free and open access. All techniques discussed below permit signal authentication without denying access. Likewise, I do not believe that widespread civilian use of military-grade SAASM receivers is practical or likely. The constraints on manufacture of SAASM receivers makes them significantly more bulky and expensive than standard civil GPS receivers. Furthermore, even though SAASM receivers can be operated in an unclassified setting and can be re-keyed with unclassified "black" keys, use of SAASM receivers is currently restricted to military personnel and to other select and authorized end-users, and initial keying logistics would likely present a headache for civil users. Therefore, civilian use of SAASM-type receivers is not considered here as a viable option.

6.1 Jamming-to-Noise Sensing Defense

Perhaps the simplest and most readily-implementable defense against GPS spoofing is to monitor the total received power near the GPS band(s) of interest (e.g., GPS L1). This can be done with a jamming-to-noise (J/N) sensor within the radio frequency (RF) front-end of a GPS receiver. The presence of in-band spoofing signals tends to increase the total in-band received power. In the case of the White Sands demonstration, to ensure a clean capture of the UAV GPS receiver, the spoofing signal ensemble was configured to be at least 10 times as powerful as the authentic signal ensemble. The presence of these spoofing signals would have been readily detectable with a J/N sensor.

This is a stand-alone non-cryptographic defense.

6.1.1 Benefits

(1) Simple and inexpensive. At least one mass-market GPS receiver, the uBlox GPS.G6–SW–10018, already provides a crude J/N output indicator.

(2) Immediately implementable.

(3) Forces spoofer to maintain received signal power below threshold.

6.1.2 Drawbacks

(1) For threshold corresponding to a reasonable false alarm rate, a J/N sensor will not typically detect a spoofing attack in which the spoofed signals are only slightly more powerful than their authentic counterparts.

6.2 Defense Based on SSSC or NMA on WAAS Signals

The SSSC- or NMA-based defenses described below could be implemented on the geostationary wide-area augmentation system (WAAS) satellites even if they are never implemented on the GPS satellites themselves.

6.2.1 Benefits

(1) WAAS is a civil program and thus could be seen as a proper avenue for implementation of civil signal authentication.

(2) WAAS signals are generated on the ground, not on the satellite, so an SSSC or NMA overlay is readily implementable.

(3) A single WAAS-authenticated WAAS signal would be sufficient to secure pre-surveyed timing receivers.

6.2.2 Drawbacks

(1) Implementation of SSSC or NMA on WAAS satellites alone would only provide users with one, or possibly two, authenticated GPS signals. While this would constrain a spoofer significantly, it would not be sufficient to authenticate a full three-dimensional navigation solution.

6.3 Multi-System Multi-Frequency Defense

The GPS receiver on the UAV that was spoofed in the White Sands demonstration was a simple single-frequency GPS L1 C/A receiver. The UAV's navigation system could immediately be made much more secure by incorporating a multi-system or multi-frequency receiver that performs proper cross-checks among separate signal ensembles. The improvement in security is one of degree, not of kind because the new signals accessible with such a receiver would not necessarily have any better inherent security than the GPS L1 C/A signals. Nonetheless, the improvement in security can be significant because, from a spoofer's perspective, it is much more challenging to simultaneously spoof signals at multiple frequencies and from multiple systems than to spoof the popular single-frequency single-system GPS L1 C/A signals.

Satellite navigation systems other than GPS include the Russian GLONASS system (fully operational), the European Galileo system (undergoing in-orbit validation of early spacecraft; may be operational by 2019), and the Chinese Compass system (global system in preliminary test phase). Small, low-power, inexpensive GPS + GLONASS receivers are now available off-the-shelf. These appear to be an excellent option for immediately improving navigation security in existing systems.

As a result of GPS modernization, new civil GPS signals are now being broadcast at the L2 and L5 frequencies in addition to the legacy civil signal on L1. These signals are not yet modulated with proper navigation data, but they can nonetheless already be used for consistency checks against the GPS L1 C/A signals. Similarly, the Galileo system will offer open-access signals at three separate frequencies. Off-the-shelf multi-frequency receivers are currently available, but these are currently several times more expensive than single-frequency GPS receivers or GPS + GLONASS receivers.

The multi-system multi-frequency defense is non-cryptographic and stand-alone.

6.3.1 Benefits

(1) Small, low-power, inexpensive GPS + GALILEO receivers are available today.

(2) Increases the difficulty of mounting a spoofing attack by forcing a would-be spoofer to generate other signal ensembles besides GPS L1 C/A.

6.3.2 Drawbacks

(1) Difficulty of mounting a spoofing attack only increases linearly with the number of new signal ensembles.

(2) Multi-system, multi-frequency capability must be combined with supervisory software that performs proper consistency checks among observables from all signals. Currently available multi-system, multi-frequency receivers do not perform this supervisory function.

(3) Multi-frequency receivers will likely remain significantly more expensive than legacy single-frequency GPS L1 C/A receivers.

6.4 Single-Antenna Defense

A stand-alone non-cryptographic single-antenna spoofing defense developed by Cornell University was tested against the University of Texas spoofer during the June White Sands trials. The technique is still under development but initial results indicate that it offers reliable spoofing detection with a low probability of false alarm. Without false alarms, it successfully detected each spoofing trial in which it was invoked at White Sands. The Cornell single-antenna defense is an extension of the signal spatial correlation technique developed by the University of Calgary PLAN group.[6]

6.4.1 Benefits

(1) Rapid (sub-second), reliable spoofing detection with a low probability of false alarm.

(2) Stand-alone, compact.

6.4.2 Drawbacks

(1) Specialized receiver will likely be several times more expensive than current GPS L1 C/A receivers.

(2) Uncertain availability.

6.5 Defense Based on Spread-Spectrum Security Codes on L1C

In 2003, Logan Scott proposed a cryptographic anti-spoofing technique based on spread spectrum security codes (SSSCs).[7] The most recent proposed version of this technique targets the L1C signal, which will be broadcast on GPS Block III satellites. Logan has briefed his proposal to the GPS Independent Review Team and the GPS Directorate is aware of it.

6.5.1 Benefits

(1) SSSC are an example of a high-rate security code. As shown in [footnote 8],[8] such codes offer an excellent defense against spoofing.

(2) Because the signal modification is targeted to L1C, whose center frequency coincides with that of the legacy GPS L1 C/A signal, even single-frequency receivers would have access to an authenticated signal.

(3) The SSSC defense would offer global civil GPS authentication for all users of GPS.

6.5.2 Drawbacks

(1) It appears that the first 8 Block III satellites are under design lockdown. There may still be time to modify the remaining satellites to incorporate hardware to support SSSC, but time is quickly running out.

(2) Even if funds materialized to implement Scott's SSSC proposal, the formal design and validation process would take several years.

(3) In stand-alone operation, the keys required to verify each SSSC would be released up to 5 minutes after the SSSC was transmitted. For 10 satellites in view, this equates to more than 30 seconds between authentication events on any signal. This would be far too long for use in aviation, where integrity alerts within 2 seconds of an event are required. The time-to-authentication could be reduced to less than 2 seconds in a networked architecture. For example, the keys could be sent over a UAVs command-and-control link. But if the command-and-control link were somehow compromised, then short-horizon authentication would again become impossible.

6.6 Defense Based on Navigation Message Authentication on L1C, L2C, or L5

A spoofing defense based on navigation message authentication (NMA) embeds public-key digital signatures into the flexible GPS civil navigation (CNAV) message,

---

[6] J. Nielsen, A. Broumandan, and G. LaChapelle, "Method and system for detecting GNSS spoofing signals," May 31 2011. US Patent 7,952,519.

[7] L. Scott, "Anti-spoofing and authenticated signal architectures for civil navigation systems," in *Proceedings of the ION GNSS Meeting,* (Portland, Oregon), pp. 1542–1552, Institute of Navigation, 2003.

[8] T.E. Humphreys, "Detection strategy for cryptographic GNSS anti-spoofing," *IEEE Transactions on Aerospace and Electronic Systems,* 2011 to be published; available at *http://radionavlab.ae.utexas.edu/detstrat.*

which offers a convenient conveyance for such signatures. A detailed proposal for NMA-based authentication is given in [footnote 9].[9]

6.6.1 Benefits

(1) NMA-based authentication is easier to implement than SSSC because the CNAV format is extensible by design so that new messages can be defined within the framework of the GPS Interference Specification (IS). The current GPS IS defines only 15 of 64 CNAV messages, reserving the undefined 49 CNAV messages for future use.

(2) Could be implemented post-launch on Block IIR–M, Block II–F, and Block III satellites.

(3) Like SSSC, the NMA-based defense would offer global civil GPS authentication for all users of GPS.

6.6.2 Drawbacks

(1) Inherently less secure than SSSC because its security codes are low rate.

(2) As with SSSC, in stand-alone operation there is an up-to-5-minute delay between authentication events for any particular signal. The discussion in Drawback 3 of the SSSC technique applies here in full.

6.7 Correlation Profile Anomaly Defense

This stand-alone non-cryptographic defense relies on the difficulty of: (1) Suppressing the true GPS signals during a spoofing attack, and (2) exactly duplicating the correlation profile of the authentic GPS signals. A preliminary description of this defense is given in [footnote 10].[10]

6.7.1 Benefits

(1) Immediately implementable, low-cost defense.

(2) No additional hardware required.

(3) Effective for stationary GPS receivers such as are used for timing applications.

6.7.2 Drawbacks

(1) Can get confused by multipath when implemented on moving receivers.

6.8 Multi-Antenna Defense

This stand-alone non-cryptographic defense is based on the premise that a spoofer will have great difficulty in mimicking the relative carrier phase of the authentic signals as seen by two or more spatially-separated antennas. The technique is detailed in [footnote 11].[11]

6.8.1 Benefits

(1) Extremely effective spoofing defense when combined with physical security of the antenna array.

(2) Immediately implementable.

6.8.2 Drawbacks

(1) Additional antenna(s) and RF front-ends required add cost and weight to the defended receiver.

6.9 Defense Based on Cross-Correlation with Military Signals

This networked cryptographic defense correlates the unknown encrypted military P(Y) code between two civil GPS receivers, exploiting known carrier-phase and code-phase relationships. It is similar to the dual-frequency codeless and semicodeless techniques that civil GPS receivers apply to track the P(Y) code on L2. Originally

---

[9] K. Wesson, M. Rothlisberger, and T.E. Humphreys, "Practical cryptographic civil GPS signal authentication," *NAVIGATION, Journal of the Institute of Navigation,* 2012 to be published; available at *http://radionavlab.ae.utexas.edu/nma.*

[10] K. Wesson, D. Shepard, J. Bhatti, and T.E. Humphreys, "An evaluation of the vestigial signal defense for civil GPS anti-spoofing," in *Proceedings of the ION GNSS Meeting,* (Portland, Oregon), Institute of Navigation, 2011.

[11] P.Y. Montgomery, T.E. Humphreys, and B.M. Ledvina, "A multi-antenna defense: Receiver-autonomous GPS spoofing detection," *Inside GNSS,* vol. 4, pp. 40–46, April 2009.

developed by researchers at Stanford University, the technique has been refined and tested by researchers at Cornell University and the University of Texas.[12]

6.9.1 Benefits

(1) Strong defense.

(2) Immediately implementable.

(3) Less than 2-second time to detection.

6.9.2 Drawbacks

(1) Requires a persistent network connection.

(2) Computationally expensive.

7. RECOMMENDATIONS

(1) I recommend that for non-recreational operation in the National airspace, civil unmanned aerial vehicles exceeding 18 lbs be required to employ navigation systems that are spoof-resistant. Spoof resistance will be defined through a series of four canned attack scenarios that can be recreated in a laboratory setting. A navigation system is declared spoof resistant if, for each attack scenario, the system is:

- (a) unaffected by the spoofing attack, or
- (b) able to detect the spoofing attack.

(2) More broadly, I recommend that GPS-based timing or navigation systems having a non-trivial role in systems designated by DHS as National critical infrastructure be required to be spoof-resistant.

(3) I recommend that the Department of Homeland Security commit to funding, development, and implementation of a cryptographic authentication signature in one of the existing or forthcoming civil GPS signals. The signature should at minimum take the form of a digital signature interleaved into the navigation message stream of the WAAS signals. Better would be to interleave the signature into the CNAV or CNAV2 GPS navigation message stream. Best would be to implement the signature as a spread spectrum security code interleaved into the spreading code of the L1C data channel.

Mr. MCCAUL. Thank you, Dr. Humphreys, and let me just state for the record I think they canceled the UT football practice to do that demonstration; is that correct?

Mr. HUMPHREYS. Losing football practice was the biggest miracle of all in my students' eyes.

Mr. MCCAUL. Which is a big deal in Texas.

Let me just follow-up on your last comment because I think that is probably the most—well, first of all this is astounding that you could hijack a UAV and bring it down, and I think it is an eye opener. Let me also state that military UAVs are encrypted. This could not be done to a military UAV such as the ones used on the border, but any ones used domestically I think have this vulnerability that we are very concerned about. I will ask you about that later.

But you mentioned that you talked to the FAA and their main concern is security of the airways.

Mr. HUMPHREYS. Safety of the airways.

Mr. MCCAUL. I am sorry. Safety of the airways. In terms of—we will designate a flight pattern and they want to make sure that there are no other either airplanes or UAVs that would interfere with that flight pattern, but their focus is not security.

Mr. HUMPHREYS. That is right.

[12] M. Psiaki, B. O'Hanlon, J. Bhatti, D. Shepard, and T. Humphreys, "GPS spoofing detection via dual-receiver correlation of military signals," *IEEE Transactions on Aerospace and Electronic Systems,* 2012 submitted for review; available at *http://web.mae.cornell.edu/psiaki/*.

Mr. MCCAUL. So there is no Federal agency that is providing oversight in terms of that security aspect today; is that correct?

Mr. HUMPHREYS. As far as I know. As far as I know. I believe that the DHS has a role to play in that and that the FAA could possibly play a role there, too. But as I say, its culture and its expertise are not designed for that.

Mr. MCCAUL. Well, I think the Government Accountability Office agreed for you. In their report they said that this is the role, when they directed the Secretary of Homeland Security, to the TSA, to basically provide for that security, assess the security risk within the country domestically and develop a National policy. So I think you have some company there in terms of agreement. I find this to be you know a bit of a "no one's minding the store"-type scenario. No Federal agency is wanting to step up to the plate, and when you got the GAO saying that DHS needs to do it, I tend to agree with them that DHS should be stepping up to the plate, and yet they failed to even bring witnesses to testify here today on this very, very important issue when you had a terror plot just thwarted right at the United States Capitol less than a year ago using one of these UAVs.

Getting back to—well, let me ask you this. You have identified a real vulnerability with these domestic UAVs. Tell me what would be sort of your kind of nightmare scenario in demonstrating what you are able to do with the UAVs if a terrorist or some other malicious person wanted to exploit the system.

Mr. HUMPHREYS. Okay. Well, first I should point out that currently I am not terribly worried about this. The UAV that we brought down was only about 13 pounds. Not very large. It could do some damage to you if it fell on you and the helicopter blades swing swiftly. But I am not terribly worried at present.

What my nightmare scenario would be is looking forward 3 or 4 years where we have now adopted the UAVs into the National airspace without addressing this problem, and now the problem is scaling up so that we have got more heavy UAVs, more capable UAVs and yet this particular vulnerability isn't addressed. So that would be my nightmare scenario. We don't fix it and it becomes even more an indigenous problem in the UAV navigation systems.

Mr. MCCAUL. In fact I think in the next 2 years predictably we will have thousands of these things flying around domestically. Does that give you concern given the fact that there is no Federal agency really addressing the security aspects?

Mr. HUMPHREYS. The FAA did make a prediction that by 2020 there could be 30,000 of these flying our airspace. It does concern me. I would like someone to take, to take ownership of the security component of UAVs coming into the National airspace.

Mr. MCCAUL. Getting back to the—I mean, you have done I think the country a great service by identifying a vulnerability. You know, we talk a lot about cybersecurity, if you are connected to the internet you are vulnerable. What you have identified is if you are connected to a GPS device you are vulnerable.

Can you explain to us basically how that works in the limited amount of time I have left and how we can fix that?

Mr. HUMPHREYS. Yeah, sure. Well, you are right. This is a bigger problem than UAVs. This is just one expression of the larger prob-

lem of unauthenticated civilian GPS signals The civilian GPS signals have been so popular, so useful that over the last 2 decades we have absorbed the technology deeply into our critical National infrastructure. So it is that even manned aircraft have some vulnerability to spoofing. Financial exchanges and the energy distribution system are increasingly reliant on GPS for timing. So in fact this is, this is a larger problem than the UAV and it all gets traced back to the unauthenticated civilian GPS signals.

Mr. MCCAUL. I see my time is about ready to expire but let me just say "thank you" for coming up to Washington and testifying here today. Thank you for what I believe is a great service to the country. Thanks for identifying a vulnerability, not only technology-wise but also from a bureaucratic standpoint. I intend for this committee to fix this problem.

With that, the Chairman now recognizes the Ranking Member, Mr. Cuellar.

Mr. CUELLAR. Thank you very much, Mr. Chairman. Doctor, thank you again very much and I appreciate the work that you have done. Let me just to repeat again, the specific spoofing efforts were beyond successful against the encrypted military-grade GPS systems, is that correct?

Mr. HUMPHREYS. It is important to remember that. Yes.

Mr. CUELLAR. Right. So we are talking civilian UAVs.

Mr. HUMPHREYS. We are talking about civilian GPS and civilian UAVs.

Mr. CUELLAR. I would note that also my understanding is that for the civilian, there is different purposes, law enforcement, ag purposes, university.

Mr. HUMPHREYS. Research purposes.

Mr. CUELLAR. Research purposes. All of that.

So for civilian purposes or commercial purposes most of those UAVs are going to be small, maybe 11 pounds, mini-helicopters, and I just saw one in Laredo for law enforcement purposes, small ones, and they are used for specific instances and it is usually line of sight, is that correct, most of them?

Mr. HUMPHREYS. Those are the norms under which they currently operate.

Mr. CUELLAR. So if it is law enforcement, it would be line of sight, most of the time it would be there, and they are usually 11 pounds; or whatever the case might be?

Mr. HUMPHREYS. Yeah. That helps to put that into perspective, and I appreciate that, too.

Mr. CUELLAR. Right. The other thing is since spoofing focuses on GPS signals, it goes beyond unmanned aircraft which means that anything from cell phones to aircraft will depend, you can have an impact on anything dealing with GPS that depends on GPS for navigation. So it is not only the unmanned. It could be other technologies; is that correct?

Mr. HUMPHREYS. Entirely true. As long as they are depending on civilian GPS signals.

Mr. CUELLAR. Right. Exactly.

Now, I think in a recent interview you stated that the closest thing we had for a foolproof way to prevent spoofing would be for

the GPS, the—I think it is part of the Air Force or actually also civilian?

Mr. HUMPHREYS. Yes. The Directorate.

Mr. CUELLAR. Yeah, the Directorate, that is correct, from coming down. Can you explain how this would be done without an impact to existing devices that rely on GPS and explain that Air Force Directorate?

Mr. HUMPHREYS. Sure. Well, I said that is the closest thing to foolproof, but the truth is that it would take a long time for that to be planned, rolled out, and implemented. So I am not holding my breath for a change in the signals being broadcast by the GPS satellites. I would like to have it happen because it would be a solution that would solve the problem for everyone worldwide that uses the civil GPS signals. At least it would solve the problem to some degree. How this would not affect people who currently use GPS, well, we can make it backward-compatible. So that if you pay attention, it is like a watermark you see in a $20 bill. If you hold up the $20 dollar bill, you can see the watermark. But if you don't pay attention you are not bothered by its presence. The same thing happens with adding authentication signatures to civilian GPS.

Mr. CUELLAR. Right. Bottom line is spoofing will affect GPS signals which means anything that depends on GPS signals for navigation, right?

Mr. HUMPHREYS. Yeah, you can think of this UAV problem as but one expression of the larger problem.

Mr. CUELLAR. Right, exactly. Most of the civilian commercial purposes of the UAVs are going to be small, and I have seen different types of UAVs and most of them are, I mean a lot of them are going to be mini-helicopters. They are going to be within a specific site for that specific purpose, law enforcement, ag, scientific, news, whatever the case might be?

Mr. HUMPHREYS. That is right. Initially I anticipate that it will always be very specific when these get authorization. I don't know how it is going to look 10 or 20 years from now, whether we are going to have UAV highways in the sky like you might see in the movies. But initially it is going to be very specific. As far as your comments about small UAVs, I want to point out that one of my recommendations in the written testimony is that UAVs exceeding 18 pounds in weight be required to have a spoof-resistant navigation system, but I recognize that we wouldn't want to encumber the smaller UAVs which are less of a danger and more sensitive to price with that same sort of requirement.

So I recognize there is a balance to be struck here and we can debate about the 18 pounds versus the 16 pounds, but as they get above 18 pounds they do become quite, quite deadly if they, if something goes awry.

Mr. CUELLAR. Right, right. The bottom line is I really appreciate it because like any time we go into a new technology and we are talking about UAVs and it is basically the technology is a different platform. You got cameras or sensors, whatever it might be, but it is a different platform, whether it is a helicopter, an airplane, this time a UAV. I really appreciate what you are doing, and I certainly will be looking at your recommendations. I think it is a lot of good work that—you and your students' data. I think it is a great job

and certainly we are going to take that into consideration, and I thank you for your good work.

Mr. HUMPHREYS. Thank you, Mr. Cuellar.

Mr. MCCAUL. I thank the Ranking Member and just I would like for you—I haven't had a chance to ask you about your recommendations for safety and security but if I ask that you submit that for the record, that would be excellent.

Mr. MCCAUL. I now recognize the gentleman from South Carolina, Mr. Duncan.

Mr. DUNCAN. Thank you, Mr. Chairman, and I want to thank Dr. Humphreys for being here. This is very educational to me.

In thinking through as we watched the video, thinking through what happened in 2011 in Iran with the Iranians claiming to have hijacked a military UAV, I guess the question I have for you, I know that was an encrypted signal but do you think that the Iranians were able to use a similar technology of spoofing to help bring down that UAV?

Mr. HUMPHREYS. I think it is important to take whatever the Iranians say with a couple of doses of salt. But in this case, I am somewhat concerned that their claims could have some merit. They may have initiated an electronic barrage against the CIA UAV that was flying their airspace, and it could have initiated a sequence of events that led to its capture. The plain fact is it showed up on Iranian television intact. Intact. That means we have got a lot of explaining to do.

Mr. DUNCAN. Right. I mean, that means that didn't crash.

So that type of an electronic barrage that you mentioned that may have been used, is that possible, a possibility within civilian airspace? If someone wanted to capture say a law enforcement UAV, could they put up an electronic barrage to bring down a law enforcement UAV?

Mr. HUMPHREYS. Similar techniques could be used. UAVs typically have two important wireless signals, the command-and-control signal, the signal that goes back to the remote pilot, and then of course the GPS signal that helps it to navigate. Mostly the UAVs do well if you cut one of those two umbilical cords, but they don't do well if you cut both of them. In our case, with the spoofing, we didn't cut the cord, we supplanted it with a fictitious one. So I am broadly concerned about jamming electronic barrage attacks and about spoofing, these more sinister under-the-wire attacks.

Mr. DUNCAN. So you not only changed the GPS signal to fool the UAV in regard to elevation or direction but you were able to tap into the command-and-control aspect as well?

Mr. HUMPHREYS. No, we did not attempt that. What I am saying is that that could be done as a jamming attack. You could cut that cord and prevent the remote operator from controlling the UAV as he or she wishes.

Mr. DUNCAN. So you were able to change the GPS signal and to fool the plane into thinking the elevation was differently to bring it down?

Mr. HUMPHREYS. Yes, and the remote operator was in contact with the UAV the entire time. It was just that nothing appeared wrong to his sensors in the current configuration that we attacked.

Mr. DUNCAN. But you couldn't have flown that UAV through any command-and-control ability to another runway and captured it.

Mr. HUMPHREYS. Ultimately, yes. It is not terribly easy to control it once you have got it. It is like a black stallion you find in the forest. You can jump on its back; can you ride it? The question that we have been asking ourselves is what could be done actually after you have captured it other than just moving it down like we did or doing broad strokes.

Mr. DUNCAN. Right. Well, if the drone is used for surveillance purposes and has a real-time video feed, could that feed be hacked into or a replacement feed sent to fool the operator? I am thinking Mission Impossible here where they change the video feed and the operator is seeing something completely different; is that a possibility?

Mr. HUMPHREYS. Or sneak up there and put a Polaroid picture right in front of the video feed?

Mr. DUNCAN. Exactly.

Mr. HUMPHREYS. Well, it turns out that these are areas of research in our laboratory and elsewhere, but the truth is that those kinds of data feeds can take advantage of the existing encryption utilities that are very difficult to crack. So if precautions have been put in place so those feeds are encrypted then it is not so easy.

The attack that we were successful in was going after the unencrypted, unauthenticated civil GPS signal. Nobody had bothered to protect that signal and so that was the weakest link.

Mr. DUNCAN. Do you think most law enforcement or most agencies, even Governmental agencies over the United States are using encrypted signals capability or using just civilian GPS?

Mr. HUMPHREYS. Only a very few civil government agencies in the United States are using the encrypted military signal. Almost all of us depend on these civilian signals. I will tell you that I had two of the lieutenants in the Austin Police Department in my office on Tuesday, and they were asking me for guidance on what I would do with their newly-purchased UAV. Would I use it, would I recommend that they use it during game day as they want to monitor for suspicious activities on, around the UT football stadium? Would I recommend they for SWAT activities as they have perhaps hostage situations and so forth? So I gave them my recommendations, which were if you have got some risk on the ground already I would get those eyes in the sky but if there isn't an on-going risky activity on the ground, I would probably keep it down.

Mr. DUNCAN. Do you think criminal elements could utilize this activity to thwart law enforcement surveillance?

Mr. HUMPHREYS. I think they could use the technology, the spoofing technology that I was talking about?

Mr. DUNCAN. The GPS technology that the students have come up with.

Mr. HUMPHREYS. I want to make a point that this is not easy. It wasn't easy to build the device that we have got. It has taken us years to perfect its use. The trouble is that civilian malefactors or others can get a hold of what are called GPS signal simulators, and they can do almost everything that we did. These are readily available, even purchasable. So I am worried that it could be a

weapon in the arsenal of organized crime or state actors or organized terrorists.

Mr. DUNCAN. Thank you. My time is up. I yield back, Mr. Chairman.

Mr. MCCAUL. Right. The Chairman now recognizes the actual Ranking Member of the subcommittee, Mr. Keating.

Mr. KEATING. Thank you, Mr. Chairman. The thought of having two Texas representatives here prompted me to get here with great alacrity, but I want to thank Mr. Cuellar for his fine performance. I appreciate that. Thank you, Mr. Chairman. I just ask unanimous consent that my statement go on the record so that we can move expeditiously to questions.

[The statement of Mr. Keating follows:]

STATEMENT OF RANKING MEMBER WILLIAM KEATING

I want to thank Chairman McCaul for holding today's hearing to examine the use of Unmanned Aerial Vehicles, or UAVs, within the homeland.

For years, the United States has successfully deployed UAVs in military operations throughout Iraq and Afghanistan.

More recently, changes in the law have paved the way for public agencies—including State and local law enforcement—to pursue UAVs technology for law enforcement use.

At present, the impact of UAVs flying in the National airspace and participating in day-to-day activities like watering fields and spraying pesticides is unknown; however, there are both risks and benefits to expanding this technology within the homeland.

As a Member representing a maritime district, I am impressed with the ability of UAVs to map hurricanes, respond to severe flooding, and assist the U.S. Coast Guard in search-and-rescue missions.

The unique manner in which UAVs conduct surveillance and reconnaissance has also resulted in successful military missions; however, it is these same capabilities that make UAVs so disconcerting at home.

To that end, I am concerned about the lack of oversight on these vehicles, the fact that there is a continuing need to define what they can and cannot be used for and finally, the absence of privacy safeguards that currently do not exist.

I understand the general public's concern. UAVs can be equipped with thermal-imaging sensors; WiFi sniffers; license plate readers, and facial recognition cameras.

Moreover, they can hover over the same location for extended periods of time, collecting information and searching targets and properties within view without first obtaining a warrant.

Some law enforcement agencies have already procured UAVs capable of firing non-lethal weapons and there aren't any rules, laws, or regulations in place to prevent these agencies from fully weaponizing this equipment.

I do not mean to use this hearing as an opporuntity to fear monger because as a former District Attorney, I do not believe that it's law enforcement's intent to employ these technologies in a harmful manner, but I am seriously concerned that there is not one single Federal agency responsible for overseeing the operations of UAVs in our National airspace.

Moreover, safety issues, such as: Sense-and-avoid technologies that enable UAVs to avoid other aircraft; the absence of a dedicated radio frequency for UAVs; and the assurance of constant command-and-control on the ground—continue to exist.

As Chairman McCaul knows, I take a particular interest in airport perimeter security and the deployment of these technologies makes me wonder how far we are stretching this perimeter when airplanes are made to share the skies with UAVs. What does this mean for passenger safety?

Furthermore, as we will learn this morning, the risk faced by hackers and spoofers seeking to intercept and use for their own purposes information captured by UAVs has not been fully addressed.

As a result, I am looking forward to hearing from today's witnesses about the best path forward as we seek to safely and lawfully integrate UAVs in our National airspace.

As we grapple with UAVs and the privacy and safety issues they present, I would be remiss if I did not also mention a much safer and non-invasive unmanned tech-

nology—underwater unmanned vehicles, or UUVs—developed throughout the United States and often tested in waters right off the Cape.

There are today an estimated 450 underwater unmanned vehicles in the U.S. military inventory.

At present, the primary missions of UUVs are mine detection and maritime security and as we've already seen with the Deepwater horizon disaster—where UUVs developed at Wood's Hole Oceanographic Institute were deployed to record the contamination of the water—there are many homeland security-related applications that can be pursued for underwater technologies, as well.

Again, I look forward to hearing from today's witnesses.

I yield back the balance of my time.

Mr. KEATING. I had just a question for Dr. Humphreys. When you are comparing the civilian, if you want to use that term, versus what law enforcement uses in the different codes of encryption, what is the cost differential? You know, if law enforcement wants encrypted more, is the cost-prohibitive or would that be a better track to take to differentiate it so that there is more encryption and more safety as a result from spoofing?

Mr. HUMPHREYS. Right. So perhaps you are voicing some of the recommendations that the AUVSI group has recommended. They would like to use the so-called SASM receivers, GPS receivers that have been formerly dedicated just for military uses, into the civilian UAVs so that they can be protected from these kinds of hacking attacks. The trouble I see with that is two-fold. No. 1, yes, the price goes quite a bit up because there are only a couple of companies that can build these SASM receivers and so the price would much more than double, and that is going to hurt this Nation's industry that is sensitive to price, especially for the smaller devices. Second, I don't see the logistics working out. These SASM receives are hot items. You would not want them proliferating among civilians. You wouldn't want them to end up in the wrong hands, and you wouldn't necessarily want to distribute the keys on a short-term basis because that is cumbersome for the owners and you don't want to distribute them on a long-term basis because then they can be used in unauthorized senses.

So I don't see that as a solution. I don't see military signals being used by civilians as a widespread solution.

Mr. KEATING. Just another question. You know, we have dealt quite a bit with airport security on this committee as well. As any person is told to turn off your cell phone, turn off everything during the critical periods of communication on landing and takeoff, how could this be used to disrupt the orderly and safe takeoffs and landings of airplanes, commercial airplanes?

The FAA is rolling out what is called its NextGen system. It is an air traffic control system that depends much more heavily on GPS than their current system. Of course, they are also using in commercial aircraft and general aviation the civilian GPS signals. Now, these planes are large and they have good inertial sensors and they have two pilots at the helm. So there is some redundancies in place. But the autopilots depend quite heavily on the GPS. Whereas they deal fairly well with an outage of GPS, a jamming attack for example, or some other reason that it goes away, I don't think the testing has been adequate for understanding how they would deal with a spoofing attack.

Mr. KEATING. Thank you. Mr. Chairman, I yield back my time.

Mr. MCCAUL. Thank the Ranking Member. The Chairman now recognizes the gentlelady from New York, Ms. Clarke.

Ms. CLARKE. Thank you very much, Mr. Chairman. I thank our Ranking Member, Mr. Cuellar, for filling in.

Dr. Humphreys, I find this whole topic quite fascinating. I serve as Ranking Member on the Subcommittee for Cybersecurity and Infrastructure Protection. So this is quite fascinating. One of the questions I have, and I have had this quite frequently as we advance our technological know-how, is whether in fact it pays in the outset to bake into our technology ways in which we can counteract disruption or if need be disarm and disable the devices that are developed. It would seem to me knowing what we know, that the next generation of UAVs would be sensitive enough that if any spoofing activity were to take place, something could be baked into the device that would protect us.

What say you about that?

Mr. HUMPHREYS. I agree with that, and I would recommend wholeheartedly efforts to bake in, as you say, anti-spoofing techniques into the UAV technology. The problem would be finding ourselves 5 or 10 years from now without taking this issue as seriously enough that now we have got a great number of these UAVs plying our airspace which are, which continue to be just as vulnerable as the one that we took down. There are techniques, there are simple techniques that, while not foolproof, they can increase the resistance to a spoofing attack significantly. I recommend in my written testimony a long list of these techniques. Some of them simple, some of them not so simple. The bare fact is that anti-spoofing is hard. There is no quick and easy and cheap solution, but there are reasonable cost-effective measures we can take in the short term to bake this in, as you say.

Ms. CLARKE. You also stated that in your view the problem should be solved at the source, at the GPS satellites themselves. Do you believe that this is likely to occur?

Mr. HUMPHREYS. So I did say that on an interview. I guess I despair at the kinds of institutional changes that would be required looking for funding, looking for a political will to bring that about. In the very best scenario it might take 5 years before we see any protection. So I am becoming more pessimistic that we can solve this problem at the GPS satellites themselves. I suppose that a more grassroots approach from the UAVs within their navigation systems is more reasonable, more practical.

Ms. CLARKE. Dr. Humphreys, you recommended that DHS commit to funding development and implementation of a cryptographic authentication signature in existing or forthcoming civil GPS signals.

How did DHS respond to this recommendation, and do you think the agency will make the suggested changes?

Mr. HUMPHREYS. So this is a long-term recommendation. As I said, I am not terribly sanguine about it happening tomorrow or even within 5 years, but long-term I would like DHS to commit to funding this. The Department of Defense has indicated some willingness to implement a change to the civil GPS signals so that the can be authenticated like putting a watermark on a $20 bill, but they don't have funds to do it. They have got tight budgets and

they are looking for somebody who would step up to fund it. I believe it would fall to the DHS to fund something like this. I can't say that I am terribly optimistic.

Ms. CLARKE. So just listening what you have had to say, when you look at the rate at which these UAVs are being produced, and if your estimate is that it might take us about 5 years to get there, we could be talking about you know tens of thousands of UAVs at that point in time having been deployed at some level, whether it is military, whether it is local law enforcement.

So, you know, I want to thank you first of all for the work that you have done, the research, and the capabilities that you have uncovered, but my concern is, you know, what you suggest we do right now.

Mr. HUMPHREYS. The suggestions I have right now are these grassroots approaches for fixing the UAV without having to ask permission of the DHS or the GPS Directorate of the Air Force. There are reasonable techniques that you can bake into the GPS receivers and into the entire navigation systems of these UAVs. But while they don't prevent sophisticated, very sophisticated attacks, they would sure make them much harder.

Ms. CLARKE. Thank you very much. I yield back, Mr. Chairman.

Mr. MCCAUL. I thank the gentlelady and you raise a great point, and if anything, I hope we can fix these vulnerabilities that we have, and I again ask that you put those recommendations into the record.

The Chairman now recognizes the gentleman from Illinois, Mr. Davis.

Mr. DAVIS. Thank you very much, Mr. Chairman. I must confess that I am fascinated by this. I was sitting here thinking that we may have all of these things in the environment zinging all around every place when you watch what used to be science fiction. I am not sure it is as much fiction now as it used to be. But I was trying to figure out the utilization and utility. What is the usefulness of the continuous development of this technology?

Mr. HUMPHREYS. That is a great question. There are in fact a lot of great uses to which these drones could be put. I particularly want to use them in our research so that we can do better detection of interference sources in the GPS radio bands, and I will confess also that I am looking forward to a day when I could get a burrito delivered to my doorstep from a drone that does takeout delivery.

Other types of uses could be in monitoring power lines. Of course monitoring the border, helping to surveil to difficult situations like a SWAT attack against somebody who has got a hostage situation on-going. So I see these as being very useful, and I would not want to put the brakes on the plan the FAA has to roll them out in the future. I would simply want to hold the FAA to the language of the act passed back in February so that we safely accelerate the adoption of these UAVs into the National airspace.

Mr. DAVIS. I guess since we have got a great deal of concern about terrorism, terrorists, terrorist plots, that it would give us the opportunity to stay a step ahead of individuals or countries even that might have other kinds of motivation for further development.

Mr. HUMPHREYS. That is true. If you put the brakes on this massive industry now, you end up putting us at a disadvantage com-

pared to other countries. The UAV revolution is coming and we might as well be on the cutting edge of it.

Mr. DAVIS. How do we balance, and I am thinking of all of the concerns that we have right now about money and expenditures and, you know, when we cut $25 billion out of this or we deny people food stamps. You know I think of people who are having so much difficulty simply having shelter or a place to live. How do we balance the utilization of our resources in terms of what it would take to further develop the technology that we are talking about versus how do you feed the hungry?

Mr. HUMPHREYS. Well, it is a good question, but I guess I would point out that in many cases these UAVs would save money. The Austin Police Department, the lieutenants that were talking to me last Tuesday, were telling me that it cost them $5 million to buy a helicopter for manned use for surveillance and so forth and maybe only $50,000 for UAV. They are on a tight budget, so I can understand why they would be looking to the UAVs to save money. That frees up budgets for other worthy uses of those funds.

It is also going to be I think a dynamo for innovation and jobs, a healthy domestic UAV industry. My main contention is that, let's let it go ahead, but let's be vigilant about the uses to which these UAVs are put and ensure that people's privacy and their security is a top priority.

Mr. DAVIS. Well, let me thank you very much. I certainly support technological exploration and technological advancement. I just want to be as balanced about it as we can, and I commend you for your work. Thank you very much.

Mr. MCCAUL. I thank the gentleman. The Chairman now indulges the gentleman from Texas, Mr. Cuellar, for one question.

Mr. CUELLAR. One question. Again, I appreciate all of the good work you have done. There are, first of all, there is the military type of drones or UAVs, and then there is the hobby UAVs and then the commercial UAVs. Would you say that?

Mr. HUMPHREYS. I think those are good broad classifications, yes.

Mr. CUELLAR. What you used was——

Mr. HUMPHREYS. It wasn't a personal UAV. It was an $80,000 device.

Mr. CUELLAR. But was it a hobby?

Mr. HUMPHREYS. No. I mean a hobbyist could use it, of course, but it was quite expensive for your average weekend hobbyist.

Mr. CUELLAR. Right. My understanding is that most of the hobby UAVs do not have protection over radio signals and they can be easily taken over, whether it is $80,000 or $5,000. My understanding is most commercial UAVs have encryption communication, the frequency hop or the transmission methods where hacking or spoofing would be a lot more difficult; is that correct?

Mr. HUMPHREYS. The communication to the UAV from the remote pilot might well be secure, but the spoofing of the GPS signals is not secure and that is what we demonstrated. We were using a high-end sophisticated UAV. We were not using a do-it-yourself drone.

Mr. CUELLAR. Right. My understanding is most of the commercial UAVs do have the encryption on it and having the encryption is very important because just like Robert Hanssen, remember the

FBI person, they were selling the encryption keys and there were certain things involved on that, but I just wanted to—like I say I appreciate the work but I want to make sure we——

Mr. HUMPHREYS. Yes. They may well have encryption on the command-and-control link. They do not have encryption on the GPS navigation link.

Mr. CUELLAR. Those are the recommendations that you mentioned to the Chairman——

Mr. HUMPHREYS. I recommend that we ensure that UAVs exceeding 18 pounds have certified themselves as spoof-resistant, and I give a brief definition for that in my statement. Also I am willing to entertain that definition in further research.

Mr. CUELLAR. Okay. Thank you. Thank you, Mr. Chairman.

Mr. MCCAUL. I thank the gentleman. Let me just also reiterate what Mr. Cuellar said earlier, and that is we have worked together very closely on getting these UAVs, military, DHS, down on the border, Southwest Border where they are very needed and very valuable in securing the border. What we are talking about here today is the domestic use of UAVs, which are not encrypted, which are vulnerable, and there is really no policy set forth at a National level in terms of: How do we deal with these UAVs that we know in the next couple of years are going to multiply by the thousands? I think it is incumbent upon the Department of Homeland Security, particularly in light of this terrorist plot, to engage on this issue and come forward with some leadership and provide that security and policy.

So with that, I would really want to thank our witness, Dr. Humphreys. It has been a real pleasure, not only to hear your insightful and very intelligent testimony but on a personal level to meet you as well. Thank you for being here.

Mr. HUMPHREYS. Thank you, Chairman McCaul and all of you Members of the subcommittee.

Mr. MCCAUL. With that, the first panel is adjourned and we will move into the second panel.

The Chairman now recognizes the second panel, and before I do that, I want to ask unanimous consent that this committee welcome a colleague and fellow Texan, Congressman Kevin Brady, to introduce his local hometown sheriff.

Mr. BRADY. Great. Well, thank you very much, Chairman McCaul and Ranking Member Keating. I want to thank you and the other Members of the committee for allowing me this special privilege today. I am very pleased to be able to introduce to the committee today not only a constituent but a friend and an incredible law enforcement officer who has hands-on experience in this very subject, Chief Deputy William Randy McDaniel of the Montgomery County Sheriff's Office. The Montgomery County, Texas Sheriff's Office has jurisdiction over Houston's largest suburb, and it is one of the fastest-growing counties in America. It is the only agency in Texas that is currently using unmanned aerial vehicles for law enforcement purposes. In my view it has tremendous potential for public safety, for emergency response, for search and rescue, and at times during natural disasters such as the wildfires we experienced locally last year.

Chief McDaniel is a decorated law enforcement officer with an impressive career spanning many decades. He has received the Texas Department of Public Safety, Traffic Law Enforcement Division Chief's Award for Excellence, two awards in that arena. While serving the United States Air Force, he received the Air Force Commendation Medal, the Humanitarian Service Medal, and the 15th Air Force Combat Crew Excellence Award. He is also a graduate of the FBI National Academy in Quantico, Virginia.

I know that Chief McDaniel's testimony will be insightful and helpful in an emerging issue. So thank you for allowing me to introduce this good friend of the community today, Chief McDaniel. Thank you for being here.

Mr. MCCAUL. Thank you, Mr. Brady, for that very good and kind introduction. With that I am going to introduce the rest of the panel.

Dr. Gerald Dillingham is currently the director of the civil aviation issues for the U.S. Government Accountability Office, or GAO. He is a member of the Senior Executive Service and is responsible for direction, program evaluations, and policy analysis studies related to civilian aviation issues, including safety, environment, air traffic control, airport development, and international aviation.

Prior to coming to GAO in 1981, Dr. Dillingham served on the faculties of the University of California and the University of Illinois. I note that for Mr. Davis, my colleague, a fellow Illinoian. In addition, he served on the National Commission on Terrorist Attacks upon the United States, or the 9/11 Commission, on the aviation in transportation security team from 2003 to 2004.

Let me see here. My notes. I apologize. Our last witness, last but not least, Ms. Amie Stepanovich is the legal counsel at the Electronic Privacy Information Center. Her work includes issues of National security, Government surveillance, digital security, and open Government. Ms. Stepanovich is the moderator of a weekly Twitter-based privacy discussion. She regularly assists with EPIC's internet and social media web presence. Prior to joining EPIC, not to be confused with the El Paso Intelligence Center, I don't think anybody would ever confuse you with being associated with them, but Ms. Stepanovich graduated from New York Law School where she pursued studies on media law, technology, and the First Amendment. We appreciate you being here today as well to bring up these very important privacy issues that we see with the domestic use of these UAVs.

So with that, now the Chairman recognizes Mr. Dillingham for his opening statement.

STATEMENT OF GERALD L. DILLINGHAM, PH.D., DIRECTOR, PHYSICAL INFRASTRUCTURE ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. DILLINGHAM. Thank you, Mr. Chairman, Ranking Member, and Members of the subcommittee. My statement today discusses three areas: First, an overview of the findings and recommendations from our 2008 study that focused on some of the key challenges to safe integration of unmanned aerial systems in the National airspace; second, DHS's role in the domestic use of these systems; and, third, our preliminary observations on emerging issues.

In 2008, the four key challenges we identified to integration were the ability of UASs to sense and avoid other aircraft, ensuring uninterrupted command and control, the development of standards to ensure that UASs meet established safety, reliability, and performance requirements and, finally, to ensure that the regulations being developed for unmanned aircraft be equal to existing regulations for manned aircraft.

To address these challenges, GAO developed a matter for Congressional consideration and three recommendations, two for FAA and one for DHS. We recommended that FAA issue a comprehensive UAS program plan and that it establish processes to obtain available operational data. We have closed those recommendations as being implemented. We suggested that Congress create an organization within FAA to coordinate Government and private-sector efforts to address the safety challenges and we also recommended that TSA examine the potential security implications related to UASs and take appropriate action.

We have closed our matter for Congressional consideration and our recommendation to TSA, but as not being implemented.

Regarding DHS's role with UASs international airspace, DHS is one of several partner agencies of FAA's Joint Planning and Development Office that is working to integrate UASs.

FAA has granted Customs and Border Protection authority to operate its 10 UASs to support its National security missions along the U.S. Northern and Southern Borders. DHS has also provided UAS support to other Federal and State agencies in carrying out their missions.

As the Chairman described in his opening statement, TSA, acting in this role as lead agency for transportation security, in 2004 issued an advisory which indicated that the Federal Government was concerned that UASs could be modified and used to attack key assets and infrastructure in the United States.

However, neither DHS nor TSA has taken any significant actions to implement our 2008 recommendations to examine the potential security implications of UAS.

According to TSA officials, in 2008 and again as recently as this month, they believe that the agency's current practices are sufficient and that no additional actions are needed.

With regard to emerging issues, our on-going work has identified three key issues that warrant further consideration. First is privacy as it relates to the collection and use of surveillance data. Members of Congress, civil liberties organizations, and civilians have expressed concerns at the potential increased use of UASs in the National airspace by law enforcement or for commercial purposes as potential privacy implications. Currently, no Federal agency has specific statutory responsibility to regulate privacy matters relating to UAS. Stakeholders have told us by developing guidelines for the appropriate use of UASs ahead of widespread proliferation could in fact preclude abuses of the technology and negative public perception of the potential uses that are planned for these aircraft.

A second emerging issue is that owners of model aircraft do not require permission or license from FAA to operate their aircraft. As the Chairman described in his opening statement, a man in Massa-

chusetts pleaded guilty for plotting to use a large, remote-controlled model aircraft filled with C4 plastic explosive to attack the Pentagon and the U.S. Capitol. This kind of incident highlights the potential for model aircraft to be used to cause harm.

A third emerging issue is the potential for jamming of GPS signals that control UASs. In a GPS jamming scenario, the aircraft could potentially lose its ability to determine where it is located and in what direction it is traveling. Low-cost devices that jam GPS signals are readily available on the internet.

Mr. Chairman, Ranking Member Keating, and Members of the subcommittee, we plan to issue a full report to this subcommittee and other committees in the Congress on our UAS work later in the fall.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Dillingham follows:]

PREPARED STATEMENT OF GERALD L. DILLINGHAM

JULY 19, 2012

GAO HIGHLIGHTS

Highlights of GAO–12–889T, a testimony before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives.

Why GAO Did This Study

UAS aircraft do not carry a human operator on board, but instead operate on preprogrammed routes or by following commands from pilot-operated ground stations. An aircraft is considered to be a small UAS if it is 55 pounds or less, while a large UAS is anything greater. Current domestic uses of UAS are limited and include law enforcement, monitoring or fighting forest fires, border security, weather research, and scientific data collection by the Federal Government. FAA authorizes military and non-military UAS operations on a limited basis after conducting a case-by-case safety review. Several other Federal agencies also have a role or interest in UAS, including DHS. In 2008, GAO reported that safe and routine access to the National airspace system poses several obstacles.

This testimony discusses: (1) Obstacles identified in GAO's previous report on the safe and routine integration of UAS into the National airspace, (2) DHS's role in the domestic use of these systems, and (3) preliminary observations on emerging issues from GAO's on-going work.

This testimony is based on a 2008 GAO report and on-going work, and is focused on issues related to non-military UAS. In on-going work, GAO analyzed FAA's efforts to integrate UAS into the National airspace, the role of other Federal agencies in achieving safe and routine integration, and other emerging issues; reviewed FAA and other Federal agency efforts and documents; and conducted selected interviews with officials from FAA and other Federal, industry, and academic stakeholders.

UNMANNED AIRCRAFT SYSTEMS.—USE IN THE NATIONAL AIRSPACE SYSTEM AND THE ROLE OF THE DEPARTMENT OF HOMELAND SECURITY

What GAO Found

GAO earlier reported that unmanned aircraft systems (UAS) could not meet the aviation safety requirements developed for manned aircraft and posed several obstacles to operating safely and routinely in the National airspace system. These include: (1) The inability for UAS to detect, sense, and avoid other aircraft and airborne objects in a manner similar to "see and avoid" by a pilot in a manned aircraft; (2) vulnerabilities in the command and control of UAS operations; (3) the lack of technological and operational standards needed to guide the safe and consistent performance of UAS; and (4) the lack of final regulations to accelerate the safe integration of UAS into the National airspace. GAO stated in 2008 that Congress should consider creating an overarching body within the Federal Aviation Administration (FAA) to address obstacles for routine access. FAA's Joint Planning and Development Office (JPDO) has taken on a similar role. FAA has implemented GAO's two

recommendations related to its planning and data analysis efforts to facilitate integration.

The Department of Homeland Security (DHS) is one of several partner agencies of JPDO working to safely integrate UAS into the National airspace. Since 2005, FAA has granted DHS authority to operate UAS to support its National security mission in areas such as the U.S. northern and southern land borders. DHS's Transportation Security Administration (TSA) has the authority to regulate security of all modes of transportation, including non-military UAS, and according to TSA officials, its aviation security efforts include monitoring reports on potential security threats regarding the use of UAS. Security considerations could be exacerbated with routine UAS access. TSA has not taken any actions to implement GAO's 2008 recommendation that it examine the security implications of future, non-military UAS.

GAO's on-going work has identified several UAS issues that, although not new, are emerging as areas of further consideration in light of greater access to the National airspace. These include concerns about privacy relating to the collection and use of surveillance data. Currently, no Federal agency has specific statutory responsibility to regulate privacy matters relating to UAS. Another emerging issue is the use of model aircraft (aircraft flown for hobby or recreation) in the National airspace. FAA is generally prohibited from developing any rule or regulation for model aircraft. The Federal Bureau of Investigation report of a plot to use a model aircraft filled with plastic explosives to attack the Pentagon and U.S. Capitol in September 2011 has highlighted the potential for model aircraft to be used for unintended purposes. An additional emerging issue is interruption of the command and control of UAS operations through the jamming and spoofing of the Global Positioning System between the UAS and ground control station. GAO plans to report more fully this fall on these issues, including the status of efforts to address obstacles to the safe and routine integration of UAS into the National airspace.

Figure 1: Example of a Small UAS (SkySeer) and a Large UAS (Predator)

Sources: Octatron, Inc. and DHS.

Chairman McCaul, Ranking Member Keating, and Members of the subcommittee: I appreciate the opportunity to testify before you today on obstacles to unmanned aircraft systems (UAS) safe and routine operations in the National airspace, the role that the Department of Homeland Security (DHS) has in UAS operations, and emerging UAS issues. Many stakeholders have exhibited increased interest in UAS for border security and disaster assistance, among other uses. Additionally, as combat operations in Afghanistan decrease, all of the United States military services expect to conduct more UAS training flights across the contiguous United States.[1]

UAS aircraft do not carry a human operator on board, but instead operate on preprogrammed routes or by following commands from pilot-operated ground stations. These aircraft are also referred to as "unmanned aerial vehicles," "remotely piloted aircraft," "unmanned aircraft," or "drones." The term "unmanned aircraft system" is used to recognize that a UAS includes not only the airframe, but also associated elements such as a ground station and the communications links. UAS are typically described in terms of weight, endurance, purpose of use, and altitude of operation. Most UAS are considered small, weighing less than 55 pounds; some of which fly less than 400 feet above the ground. According to an industry association, small UAS are expected to comprise the majority of UAS that will operate in the National airspace.

The Federal Aviation Administration (FAA) authorizes military and non-military (academic institutions; Federal, State, and local governments including law enforcement entities; and private sector entities) UAS operations on a limited basis after conducting a case-by-case safety review. Only Federal, State, and local government agencies can apply for a Certificate of Waiver or Authorization (COA); private-sector

[1] House Permanent Select Committee on Intelligence, *Performance Audit of the Department of Defense Intelligence, Surveillance, and Reconnaissance* (Washington, DC: Apr. 2012).

entities must apply for special airworthiness certificates in the experimental category.[2]

Between January 1, 2012 and July 17, 2012, FAA had issued 201 COAs to 106 Federal, State, and local government entities across the United States, including law enforcement entities as well as academic institutions. Additionally, FAA had issued 8 special airworthiness certifications for experimental use to four UAS manufacturers. Presently, under COA or special airworthiness certification, UAS operations are permitted for specific times, locations, and operations. Thus it is not uncommon for an entity to receive multiple COAs for various missions. Over the years, concerns have been expressed by the Congress and other stakeholders that sufficient progress has not been made to integrate UAS into the National airspace system. In 2008, GAO reported that safe and routine access to the National airspace system poses several obstacles. We also stated that Congress should consider creating an overarching body within FAA to coordinate Federal, academic, and private-sector efforts in meeting the safety challenges of allowing routine access to the National airspace system. Additionally, we made two recommendations to FAA related to its planning and data analysis efforts to facilitate the process of allowing UAS routine access to the National airspace. We also recommended that DHS assess the security implications of routine access. FAA is working toward implementing the requirements set forth by its February 2012 reauthorization to accelerate UAS integration.[3]

Several other Federal agencies also have a role or interest in UAS, including the Department of Homeland Security (DHS), the Department of Defense (DOD), and the National Aeronautics and Space Administration (NASA).[4] DHS's Transportation Security Administration (TSA) has authority to regulate the security of all transportation modes, including non-military UAS, to ensure that appropriate safeguards are in place. According to TSA, its aviation security efforts include addressing risks, threats, and vulnerabilities related to non-military UAS. In addition, according to DHS officials, Customs and Border Protection (CBP) owns ten UAS that it operates for its own missions as well as for missions in conjunction with other agencies. DOD has successfully used UAS for intelligence, surveillance, reconnaissance, and combat missions.[5] While many of DOD's UAS operations currently take place outside of the United States, the military services require access to the National airspace to conduct UAS training. DOD has also assisted DHS in border security missions, including two missions since 2006 where the National Guard provided support in four Southwestern Border States. NASA uses UAS primarily for research purposes, such as the Predator B for wildfire mapping and investigations as well as an expected arctic mission next year on surface sea ice.

My statement today discusses: (1) Obstacles we identified in our previous report to the safe and routine integration of UAS into the National air space, (2) DHS's role in the domestic use of these systems, and (3) preliminary observations on emerging issues from our on-going work examining UAS. This statement is based on our 2008 UAS report[6] and on-going work for this subcommittee, the House Committee on Transportation and Infrastructure and its subcommittee on Aviation, and the Senate Committee on Science, Commerce, and Transportation. Our on-going work is focused on issues related to non-military UAS and is based on our analysis of FAA's efforts to integrate UAS into the National airspace, the role of other Federal agencies in achieving safe and routine integration, and other emerging issues. Our preliminary observations are based on our review of various FAA and other Federal agency efforts and documents; and selected interviews with officials from FAA and other Federal, industry, and academic stakeholders. Our 2008 report contains detailed explanations of the methods used to conduct that work. We have discussed the information in this testimony with officials from FAA and DHS, and incorporated their comments as appropriate. The work on which this statement is

---

[2] COAs and special airworthiness certifications in the experimental category represent exceptions to the usual certification process. FAA examines the facts and circumstances of a proposed UAS to ensure that the prospective operator has acceptably mitigated safety risks.

[3] FAA Modernization and Reform Act of 2012, Pub. L. No. 112–95, §§ 332–334, 126 Stat. 11 (2012).

[4] Senior executives from these four Federal agencies represent the UAS ExCom, whose mission is to enable increased and ultimately routine access of Federal UAS engaged in non-military aircraft operations into the National airspace to support these agencies' operational, training, development, and research requirements.

[5] GAO, *Unmanned Aircraft Systems: Comprehensive Planning and a Results-Oriented Training Strategy Are Needed to Support Growing Inventories,* GAO–10–331 (Washington, DC: Mar. 26, 2010).

[6] GAO, *Unmanned Aircraft Systems: Federal Actions Needed to Ensure Safety and Expand Their Potential Uses Within the National Airspace System,* GAO–08–511 (Washington, DC: May 15, 2008).

based was performed in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

BACKGROUND

Current domestic uses of UAS are limited and include law enforcement, monitoring or fighting forest fires, border security, weather research, and scientific data collection. UAS have a wide-range of potential uses, including commercial uses such as pipeline, utility, and farm fence inspections; vehicular traffic monitoring; real estate and construction site photography; relaying telecommunication signals; and crop dusting. FAA's long-range goal is to permit, to the greatest extent possible, routine UAS operations in the National airspace system while ensuring safety. Using UAS for commercial purposes is not currently allowed in the National airspace. As the list of potential uses for UAS grows, so do the concerns about how they will affect existing military and non-military aviation as well as concerns about how they might be used.

Domestically, State and local law enforcement entities represent the greatest potential use of small UAS in the near term because small UAS can offer a simple and cost-effective solution for airborne law enforcement activities for agencies that cannot afford a helicopter or other larger aircraft.[7] For example, Federal officials and one airborne law enforcement official said that a small UAS costing between $30,000 and $50,000 is more likely to be purchased by State and local law enforcement entities because the cost is nearly equivalent to that of a patrol car. According to recent FAA data, 12 State and local law enforcement entities have a Certificate of Waiver or Authorization (COA) while an official at the Department of Justice said that approximately 100 law enforcement entities have expressed interest in using a UAS for some of their missions. According to law enforcement officials with whom we spoke, small UAS are ideal for certain types of law enforcement activities. Officials anticipate that small UAS could provide support for tactical teams, post-event crime scene analysis and critical infrastructure photography. Officials said that they do not anticipate using small UAS for routine patrols or missions that would require flights over extended distances or time periods.

FAA has been working with the Department of Justice's National Institute of Justice to develop a COA process through a memorandum of understanding to better meet the operational requirements of law enforcement entities. While the memorandum of understanding establishing this COA process has not been finalized, there are two law enforcement entities that are using small UAS on a consistent basis for their missions and operations. The proposed process would allow law enforcement entities to receive a COA for training and performance evaluation. When the entity has shown proficiency in operating its UAS, it would then receive an operational COA allowing it to operate small UAS for a range of missions. In May 2012, FAA stated that it met its first requirement to expedite the COA process for public safety entities. FAA's reauthorization also required the agency to enter into agreements with appropriate Government agencies to simplify the COA process and allow a Government public safety agency to operate unmanned aircraft weighing 4.4 pounds or less if flown within the line of sight of the operator, less than 400 feet above the ground, and during daylight conditions, among other stipulations.

OBSTACLES TO SAFE AND ROUTINE INTEGRATION OF UAS

In 2008, we reported that UAS could not meet the aviation safety requirements developed for manned aircraft and posed several obstacles to operating safely and routinely in the National airspace system.

- *Sense-and-avoid technologies*.—To date, no suitable technology has been identified that would provide UAS with the capability to meet the detect, sense, and avoid requirements of the National airspace system. Our on-going work indicates that research has been carried out to mitigate this, but the inability for UAS to sense and avoid other aircraft or objects remains an obstacle. With no

[7] FAA generally considers UAS in the two broad categories of "small" and "large," and has used these categories to split its efforts to develop rules that would allow Government and commercial UAS access to the National airspace. FAA has been developing rules for small UAS for several years. Although there is no widely-accepted common classification system for UAS, an aircraft is considered to be a small UAS if it is 55 pounds or less, while a large UAS is anything greater.

pilot to scan the sky, UAS do not have an on-board capability to directly "see" other aircraft. Consequently, the UAS must possess the capability to sense and avoid an object using on-board equipment, or with the assistance of a human on the ground or in a chase aircraft,[8] or by other means, such as radar. Many UAS, particularly smaller models, will likely operate at altitudes below 18,000 feet, sharing airspace with other vehicles or objects. Sensing and avoiding other vehicles or objects represents a particular challenge for UAS, because other vehicles or objects at this altitude often do not transmit an electronic signal to identify themselves and, even if they did, many small UAS, do not have equipment to detect such signals if they are used and may be too small to carry such equipment.

- *Command-and-control communications*.—Similar to what we previously reported, ensuring uninterrupted command and control for UAS remains a key obstacle for safe and routine integration into the National airspace. Without such control, the UAS could collide with another aircraft or crash, causing injury or property damage. The lack of dedicated radiofrequency spectrum for UAS operations heightens the possibility that an operator could lose command and control of the UAS. Unlike manned aircraft that use dedicated radio frequencies, non-military UAS currently use undedicated frequencies and remain vulnerable to unintentional or intentional interference. To address the potential interruption of command and control, UAS generally have pre-programmed maneuvers to follow if the command-and-control link becomes interrupted (called a "lost-link scenario"). However, these procedures are not standardized across all types of UAS and, therefore, remain unpredictable to air traffic controllers who have responsibility for ensuring safe separation of aircraft in their airspace.
- *Standards*.—A rigorous certification process with established performance thresholds is needed to ensure that UAS and pilots meet safety, reliability, and performance standards. Minimum aviation system standards are needed in three areas: Performance; command-and-control communications; and sense-and-avoid. In 2004, RTCA, a standards-making body sponsored by FAA, established a Federal advisory committee called the Special Committee 203 (or SC 203), to establish minimum performance standards for FAA to use in developing UAS regulations.[9] Individuals from academia and the private sector serve on the committee, along with FAA, NASA, and DOD officials. ASTM International Committee F38 on UAS, an international voluntary consensus standards-making body, is working with FAA to develop standards to support the integration of small UAS into the National airspace.[10]
- *Regulations*.—FAA regulations govern the routine operation of most aircraft in the National airspace system.[11] However, these regulations do not contain provisions to address issues relating to unmanned aircraft. As we highlighted in our previous report, existing regulations may need to be modified to address the unique characteristics of UAS. Today, UAS continue to operate as exceptions to the regulatory framework rather than being governed by it. This has limited the number of UAS operations in the National airspace, and that limitation has, in turn, contributed to the lack of operational data on UAS in domestic operations previously discussed. One industry forecast noted that growth in the non-military UAS market is unlikely until regulations allow for the routine operation of UAS. Without specific and permanent regulations for safe operation of UAS, Federal stakeholders, including DOD, continue to face challenges. The lack of final regulations could hinder the acceleration of safe and routine integration of UAS into the National airspace.

Given the remaining obstacles to UAS integration, we stated in 2008 that Congress should consider creating an overarching body within FAA to coordinate Federal, academic, and private-sector efforts in meeting the safety challenges of allow-

---

[8] Chase pilots are in constant radio contact with research pilots and serve as an "extra set of eyes" to help maintain total flight safety during specific tests and maneuvers. Chase pilots monitor certain events for the research pilot and are an important safety feature on all research missions.

[9] RTCA, formerly the Radio Technical Commission for Aeronautics, is a private, not-for-profit corporation that develops consensus-based performance standards regarding communications, navigation, surveillance, and air traffic management system issues. RTCA serves as a Federal advisory committee, and its recommendations are the basis for a number of FAA's policy, program, and regulatory decisions.

[10] ASTM International, formerly known as the American Society for Testing and Materials (ASTM), is a globally recognized leader in the development and delivery of international voluntary consensus standards. ASTM members deliver the test methods, specifications, guides, and practices that support industries and governments worldwide.

[11] Title 14, Code of Federal Regulations (14 CFR).

ing routine access to the National airspace system. While it has not created this overarching body, FAA's Joint Planning and Development Office has taken on a similar role. In addition, Congress set forth requirements for FAA in its February 2012 reauthorization to facilitate UAS integration. Additionally, we made two recommendations to FAA related to its planning and data analysis efforts to facilitate the process of allowing UAS routine access to the National airspace, which FAA has implemented.

ROLE OF THE DEPARTMENT OF HOMELAND SECURITY IN DOMESTIC UAS USE

DHS is one of several partner agencies of FAA's Joint Planning and Development Office (JPDO) working to safely integrate UAS into the National airspace. TSA has the authority to regulate the security of all transportation modes, including nonmilitary UAS, and according to TSA officials, its aviation security efforts include monitoring reports on potential security threats regarding the use of UAS. While UAS operations in the National airspace are limited and take place under closely controlled conditions, this could change if UAS have routine access to the National airspace system. Further, DHS owns and uses UAS.

Security is a significant issue that could be exacerbated with an increase in the number of UAS, and could impede UAS use even after all other obstacles have been addressed. In 2004, TSA issued an advisory in which it stated that there was no credible evidence to suggest that terrorist organizations plan to use remote-controlled aircraft or UAS in the United States. However, the TSA advisory also provided that the Federal Government remains concerned that UAS could be modified and used to attack key assets and infrastructure in the United States. TSA advised individuals to report any suspicious activities to local law enforcement and the TSA General Aviation Hotline.[12] Security requirements have yet to be developed for UAS ground control stations—the UAS equivalent of the cockpit.[13] Legislation introduced in the 112th Congress would prohibit the use of UAS as weapons while operating in the National airspace.[14]

In our 2008 report, we recommended that the Secretary of Homeland Security direct the administrator of TSA to examine the security implications of future, nonmilitary UAS operations in the National airspace and take any actions deemed appropriate. TSA agreed that consideration and examination of new aviation technologies and operations is critical to ensuring the continued security of the National airspace. According to TSA officials, TSA continues to work with the FAA and other Federal agencies concerning airspace security by implementing security procedures in an attempt to protect the National Airspace System. Examples of this collaboration include the coordinated efforts to allow access to temporary flight-restricted airspace such as those put in place for Presidential travel and DHS Security Events. However, to date, neither DHS nor TSA has taken any actions to implement our 2008 recommendation. According to TSA officials, TSA believes its current practices are sufficient and no additional actions have been needed since we issued our recommendation.

DHS is also an owner and user of UAS. Since 2005, CBP has flown UAS for border security missions. FAA granted DHS authority to operate UAS to support its National security mission along the United States northern and southern land borders, among other areas. Recently, DHS officials told us that DHS has also flown UAS over the Caribbean to search for narcotics-carrying submarines and speedboats. According to DHS officials, CBP owns ten UAS that it operates in conjunction with other agencies for various missions. As of May 2012, CBP has flown missions to support six Federal and State agencies along with several DHS agencies. These missions have included providing the National Oceanic and Atmospheric Administration with videos of damaged dams and bridges where flooding occurred or was threatened, and providing surveillance for DHS's Immigration and Customs Enforcement over a suspected smuggler's tunnel. DHS, DOD, and NASA, are working with FAA to identify and evaluate options to increase UAS access in the National airspace. DHS officials reported that if funding was available, they plan to expand their fleet to 24 total UAS that would be operational by fiscal year 2016, including 11 on the Southwest Border.

The DHS Inspector General reviewed CBP's actions to establish its UAS program, the purpose of which is to provide reconnaissance, surveillance, targeting, and acquisition capabilities across all CBP areas of responsibility. The Inspector General

[12] Department of Homeland Security, *TSA Advisory: Security Information Regarding Remote Controlled Aircraft and Unmanned Aerial Vehicles* (Washington, DC: Nov. 22, 2004).

[13] Additionally, in response to the events of September 11, 2001, entry doors to passenger airplane cockpits were hardened to prevent unauthorized entry.

[14] No Armed Drones Act of 2012, H. R. 5950, 112th Cong. (2012).

assessed whether CBP has established an adequate operation plan to define, prioritize, and execute its unmanned aircraft mission. The Inspector General's May 2012 report found that CBP had not achieved its scheduled or desired level of flight hours for its UAS. It estimated that CBP used its UAS less than 40 percent of the time it would have expected.[15]

PRELIMINARY OBSERVATIONS ON EMERGING UAS ISSUES

Our on-going work has identified several UAS issues that, although not new, are emerging as areas of further consideration in light of the efforts towards safe and routine access to the National airspace. These include concerns about: (1) Privacy as it relates to the collection and use of surveillance data, (2) the use of model aircraft, which are aircraft flown for hobby or recreation, and (3) the jamming and spoofing of the Global Positioning System (GPS).

- *Privacy concerns over collection and use of surveillance data*.—Following the enactment of the UAS provisions of the 2012 FAA reauthorization act, Members of Congress, a civil liberties organization, and others have expressed concern that the increased use of UAS for surveillance and other purposes in the National airspace has potential privacy implications. Concerns include the potential for increased amounts of Government surveillance using technologies placed on UAS as well as the collection and use of such data. Surveillance by Federal agencies using UAS must take into account associated Constitutional Fourth Amendment protections against unreasonable searches and seizures. In addition, at the individual agency level, there are multiple Federal laws designed to provide protections for personal information used by Federal agencies. While the 2012 FAA reauthorization act contains provisions designed to accelerate the safe integration of UAS into the National airspace, proposed legislation in the 112th session of Congress, seeks to limit or serve as a check on uses of UAS by, for example, limiting the ability of the Federal Government to use UAS to gather information pertaining to criminal conduct without a warrant.[16]

  Currently, no Federal agency has specific statutory responsibility to regulate privacy matters relating to UAS. UAS stakeholders disagreed as to whether the regulation of UAS privacy-related issues should be centralized within one Federal agency, or if centralized, which agency would be best positioned to handle such a responsibility. Some stakeholders have suggested that FAA or another Federal agency should develop regulations for the types of allowable uses of UAS to specifically protect the privacy of individuals as well as rules for the conditions and types of data that small UAS can collect. Furthermore, stakeholders with whom we spoke said that developing guidelines for technology use on UAS ahead of widespread adoption by law enforcement entities may preclude abuses of the technology and a negative public perception of UAS. Representatives from one civil liberties organization told us that since FAA has responsibility to regulate the National airspace, it could be positioned to handle responsibility for incorporating rules that govern UAS use and data collection. Some stakeholders have suggested that the FAA has the opportunity and responsibility to incorporate such privacy issues into the small UAS rule that is currently underway and in future rulemaking procedures. However, FAA officials have said that regulating these sensors is outside the FAA's mission, which is primarily focused on aviation safety, and has proposed language in its small UAS Notice of Proposed Rulemaking to clarify this.
- *Model aircraft*.—According to an FAA official with whom we spoke and other stakeholders, another concern related to UAS is the oversight of the operation of model aircraft—aircraft flown for hobby or recreation—capable of sustained flight in the atmosphere and a number of other characteristics.[17] Owners of model aircraft do not require a COA to operate their aircraft.[18] Furthermore, as part of its 2012 reauthorization act, FAA is prohibited from developing any

[15] The report made four recommendations intended to improve CBP's planning of its UAS program to address its level of operation, program funding, and resource requirements, along with stakeholder needs.

[16] Preserving Freedom from Unwarranted Surveillance Act of 2012, S. 3287, 112th Cong. (2012) and Farmer's Privacy Act of 2012, H.R. 5961, 112th Cong. (2012).

[17] The 2012 reauthorization act defines the term "model aircraft" to mean an unmanned aircraft that is: (1) Capable of sustained flight in the atmosphere, (2) flown within visual line of sight of the person operating the aircraft, and (3) flown for hobby or recreational purposes.

[18] FAA's Advisory Circular 91–57 sets out model aircraft operating standards that encourage voluntary compliance with specified safety standards for model aircraft operators.

rule or regulation for model aircraft under a specified set of conditions.[19] However, the 2012 reauthorization act also specifies that nothing in the act's model aircraft provisions shall be construed to limit FAA's authority to take enforcement action against the operator of a model aircraft who endangers the safety of the National airspace system.[20] The Federal Bureau of Investigation report of the arrest and criminal prosecution of a man plotting to use a large remote-controlled model aircraft filled with plastic explosives to attack the Pentagon and U.S. Capitol in September 2011 has highlighted the potential for model aircraft to be used for non-approved or unintended purposes.

The Academy of Model Aeronautics, which promotes the development of model aviation as a recognized sport and represents a membership of over 150,000, published several documents to guide model aircraft users on safety, model aircraft size and speed, and use. For example, the Academy's National Model Aircraft Safety Code specifies that model aircraft will not be flown in a careless or reckless manner and will not carry pyrotechnic devices that explode or burn, or any device that propels a projectile or drops any object that creates a hazard to persons or property (with some exceptions).[21] The Academy of Model Aeronautics also provides guidance on "sense and avoid" to its members, such as a ceiling of 400 feet above ground of aircraft weighing 55 pounds or less. However, apart from FAA's voluntary safety standards for model aircraft operators, FAA has no regulations relating to model aircraft. Currently, FAA does not require a license for any model aircraft operators, but according to FAA, the small UAS Notice of Proposed Rule Making, under development and expected to be published late 2012, may contain a provision that requires certain model aircraft to be registered.

- *GPS jamming and spoofing*.[22]—The jamming and spoofing of the communication signal between the UAS and ground control station could also interrupt the command and control of UAS operations. In a GPS jamming scenario, the UAS could potentially lose its ability to determine where it is located and in what direction it is traveling. Low-cost devices that jam GPS signals are prevalent. According to one industry expert, GPS jamming would become a larger problem if GPS is the only method for navigating a UAS. This problem can be mitigated by having a second or redundant navigation system on-board the UAS that is not reliant on GPS. In addition, a number of Federal UAS stakeholders we interviewed stated that GPS jamming is not an issue for the larger, military-type UAS, as they have an encrypted communications link on the aircraft. A stakeholder noted that GPS jamming can be mitigated for small UAS by encrypting its communications, but the costs associated with encryption may make it infeasible. Recently, researchers at the University of Texas demonstrated that the GPS signal controlling a small UAS could be spoofed using a portable software radio. The research team found that it was straightforward to mount an intermediate-level spoofing attack but difficult and expensive to mount a more sophisticated attack.[23] The emerging issues we identified not only may exist as part of efforts to safely and routinely integrate UAS into the National airspace, but may also persist once integration has occurred. Thus, these issues may warrant further examination both presently and in the future.

---

[19] This prohibition on FAA model aircraft rules or regulations only applies where the aircraft is: (1) Flown strictly for hobby or recreational use, (2) operated in accordance with a community-based set of safety guidelines and within the programming of a Nation-wide community-based organization, (3) limited to not more than 55 pounds (unless otherwise certified through a design, construction, inspection, flight test, and operational safety program administered by a community-based organization), (4) operated in a manner that does not interfere with and gives way to any manned aircraft, and (5) when flown within 5 miles of an airport, prior notice of the operation is given to the airport operator and the air traffic control tower.

[20] Pub. L. No. 112–95, § 336, 126 Stat. 11.77 (2012).

[21] The Academy of Model Aeronautics National Model Aircraft Safety Code allows members to fly devices that burn producing smoke and are securely attached to the model aircraft and use rocket motors if they remain attached to the model during flight. Model rockets may be flown but not launched from a model aircraft.

[22] GPS spoofing is when counterfeit GPS signals are generated for the purpose of manipulating a target receiver's reported position and time. Todd E. Humphreys, *Detection Strategy for Cryptographic GNSS Anti-Spoofing, IEEE Transactions on Aerospace and Electronics Systems* (August 2011).

[23] The presentation "Assessing the Civil GPS Spoofing Threat" by Todd Humphreys, Jahshan Bhatti, Brent Ledvina, Mark Psiaki, Brady O'Hanlon, Paul Kintner, and Paul Montgomery sought to assess the spoofing threat of a small civil UAS. The team built a civilian GPS spoofer and tested some countermeasures. They concluded that GPS spoofing is a threat to communications security and civil spoofing has not been the focus of research in open literature.

Chairman McCaul, Ranking Member Keating, and Members of the subcommittee, this concludes my prepared statement. We plan to report more fully this fall on these same issues, including the status of efforts to address obstacles to the safe and routine integration of UAS into the National airspace. I would be pleased to answer any questions at this time.

Mr. MCCAUL. Thank you, Dr. Dillingham, for your good work. The Chairman now recognizes another fellow Texan, Chief McDaniel.

STATEMENT OF CHIEF DEPUTY WILLIAM R. MC DANIEL, MONTGOMERY COUNTY SHERIFF'S OFFICE, CONROE, TEXAS

Chief MCDANIEL. Thank you, sir.

The Montgomery County Sheriff's Office is the seventh-largest in the State of Texas, and is responsible for law enforcement services for a county that covers over 1,000 square miles and has a population of over 471,000. As indicated, it is an extremely fast-growing county. The county is diverse in geography as well as population, with an extremely urban area with a very dense population on our Southern Border with Houston and Harris County, to an extremely rural area in the northern portion of our county.

The sheriff's office is committed to protecting the lives and the property of the people we serve, and since my sheriff took office in 2005, we have sought out new and better technology to enhance both our efficiency as well as our effectiveness in carrying out our public safety mission. I believe the UAV systems now available to public safety agencies are exactly the type of technology that will make us more successful. It is not just a law enforcement tool, but a public safety asset that can now be used by fire departments, emergency management offices, and probably other governmental units as well.

The sheriff's office has owned a Shadow Hawk UAV since December 2011, having purchased it through a Homeland Security grant. Although we have not used it for an operational mission to date, we absolutely see its benefit and its mission profile for SWAT operations, high-risk warrants, locating lost persons, manhunts, hazardous material spills, fire scene, traffic accident investigations, or traffic management and observation due to hurricane evacuations.

We did not obtain this for the purpose of surveillance. I do not believe small UAVs such as our Shadow Hawk are particularly designed or suited for that type of mission.

Although the FAA has expertise in the aeronautical field, they do not have the necessary public safety mission experience to effectively oversee this type of operational environment. If Federal oversight is necessary, it would seem appropriate to establish it under the Department of Homeland Security. Different from the aeronautical component the FAA would continue to manage, DHS would manage the operational aspect by setting and enforcing operational guidelines and procedures, establish a database relating to the UAVs, agencies using them, mission results, and act as a resource and information tool for current and interested public safety agencies.

Current case law supports the use of air assets by law enforcement, and I do not believe that it is necessary to introduce new legislation that would severely restrict the UAV's effectiveness. I encourage you to recognize unmanned aerial vehicle systems as an

important tool for public safety agencies. I believe in this technology and its mission of protecting the citizens of my county, my State, and this Nation.

[The prepared statement of Chief McDaniel follows:]

PREPARED STATEMENT OF WILLIAM R. MCDANIEL

JULY 19, 2012

Montgomery County is directly north of Houston and contiguous to Harris County. The county is diverse in both geography and population. The current census lists the population at over 471,000. It is approximately 1,042 square miles in size with highly populated urban areas in the southern portion of the county (The Woodlands) to very rural areas in the north. Sam Houston National Forest, situated in the northwestern portion of the county encompasses 47,609 acres. Situated in the middle of the county is Lake Conroe, a large lake (21,000 acres), with a significant population surrounding it.

In 2005, the Montgomery County Sheriff's Office began to explore various avenues to enhance our operational effectiveness. One idea was to obtain air assets for public safety response needs. We envisioned having an air asset that was multi-purpose and could be utilized in a variety of critical incidents to improve our ability to respond. Initially we looked at small aircraft (i.e. Cessna's, etc.) as well as helicopters. We looked at both new and used aircraft and quickly realized we did not have sufficient funding to purchase nor maintain such an item. As an example, a "law enforcement" helicopter, with associated equipment, would require over $2 million for the initial cost. We would be unable to fund full-time personnel to operate and maintain the aircraft. A small, fixed-wing aircraft would be less costly, around $400,000, but we would still have the same staffing issues. In addition, we compared operational costs and determined the hourly cost alone would be prohibitive, based on our budget.

We are fortunate to be situated in an area with agencies (Houston PD, State Police, and DEA) that do have air assets and we have certainly called upon them to assist us in a variety of ways. It has been problematic; however, since these agencies also have budget constraints which limit their operational flight hours as well as their ability to respond. The problem has been further compounded by the need for these air assets to cover large areas or, because it may be a State or Federal asset, it is deployed to other areas of the State or country. They are, therefore, unavailable at times.

We continued to review opportunities over the next few years. One such opportunity was a pilot project through the Department of Justice. The program was offering certain types of "ultra-light" aircraft for testing by law enforcement. A letter was sent to the DOJ representative on two different occasions; however, no response was ever received.

In 2008, a call was received from the CEO of Vanguard Defense Industries (VDI) requesting a meeting to discuss the concept of a UAV for law enforcement. During our first meeting, a discussion was held regarding the practicality of using a UAV for law enforcement purposes. The platform being proposed was a small helicopter with a color video camera and Forward Looking Infrared (FLIR) capabilities. The aircraft could be launched quickly, provide an aerial view during a critical incident, and be economical to purchase and operate. We discussed at length the types of incidents we thought would be appropriate for its use. These included SWAT call-outs, high-risk warrants, manhunts, lost persons, and accident scene investigation (aerial photography). In meetings that followed, we expanded on its use to an overall public safety response instead of being geared strictly towards law enforcement. In addition to a law enforcement use, we envisioned fire departments and emergency management offices as agencies that would benefit from such an asset. We then added to the types of incidents it would be suitable for to include hazardous materials spills, fires, damage assessment, or traffic management observation due to hurricane evacuations.

While VDI was working on the manufacturing component, we began to research funding sources and eventually submitted a grant proposal through the Department of Homeland Security's Urban Areas Security Initiative (UASI) program in December, 2010. The UASI project goal, identified in the grant project was, "to enhance regional response capability." The grant was approved in June, 2011, and the delivery of the Shadowhawk was made in December, 2011. The total funding for the grant was $220,000. This included a 1-year maintenance agreement and air crew training for two personnel. Within a few months the Sheriff's Office purchased an

upgraded guidance system, as well as an LED lighting system, to better identify the aircraft.

In 2010, we also initiated our Certificate of Authorization (COA) application to the FAA. The web-based application process was relatively simple to complete and many email exchanges and phone conversations took place with FAA personnel. It was clear to us that this was somewhat "uncharted waters" for them and we were warned on several occasions that it would be a lengthy process. Once the final application was submitted, it was a number of months before the application was approved. The initial COA was renewed in 2012.

To date, the Montgomery County Sheriff's Office has only had one opportunity to utilize the Shadowhawk for an operational mission; however, the FAA denied our request for an emergency COA, citing there had to exist a "loss of life or potential loss of life" before they would approve it. We certainly believed there to be a potential danger to the law enforcement officers who were going to conduct the mission. We opted to not press the issue at that point. To some critics, this would seem to be a waste of Federal tax dollars. I would point out, however, public safety operations are not static or particularly consistent. This is especially true with "special missions." As an example, our SWAT unit responded 23 times in 2011 but has not been "called out" in 2012. The need is there; however, and will continue to be. Those types of incidents we identified as being ideal for the Shadowhawk are actual types of incidents we have experienced over and over again in the past. It is only a matter of "when" the next such incident will occur.

We continue to think of ways to deploy our UAV and one such example is utilizing a UAV to deliver a cellular phone or an emergency medical kit to a flood victim, stranded on the roof of a house. (Currently, the FAA prohibits this type of activity.) It would appear to be highly effective to send a UAV in to deploy a cellular phone, have a first responder explain to the victim what the procedures will be to be picked up by a helicopter or boat (excellent safety protocol) and then continue with the rescue operation or; be able to drop a first aid kit to a victim with a UAV in a timely manner so they can immediately address their basic first aid needs as opposed to forcing them to wait on medical help to be delivered by aircraft or boat (not very timely). In discussions we have had with the manufacturer of the Shadowhawk, it would be relatively easy to build the necessary platform for the Shadowhawk to "drop" supplies as stated. There are still, no doubt, scenarios we have not even dreamed of wherein the UAV could be used to benefit public safety.

There has been a knee-jerk reaction to the use of UAV's by public safety agencies in the United States with National media outlets painting a dark picture of tens of thousands of "drones" being used daily to "spy" on citizens. We believe there is sufficient case law in place to establish, for the UAV community, the legal requirements and procedures for operation and also the necessary repercussions for those agencies who fail to comply with the legal mandates. UAV's operate just like their manned counterparts. Obviously, the primary difference is having a crew on the ground operating it as opposed to a crew operating the airborne aircraft. There has been case law developed over the years to deal with manned aircraft operations for public safety agencies. We believe these same laws would absolutely apply to UAV operations.

Governmental entities, as identified and approved by the FAA, must follow strict guidelines and protocols and are extensively scrutinized by the FAA hierarchy for improper operations. The problem exists in the rank-and-file FAA hierarchy having no real concept of the needs of public safety agencies. It is my perception they tend to look at the use of UAV's with myopic vision. This was fine for past years as new technology, in the FAA domain, was scarce. Now that UAV technology is here, the FAA does not have the experience in its application. FAA staffers do not have the law enforcement, fire, or emergency management background to be able to relate to the mission of these agencies. The sole purpose of the FAA is to monitor them from an aeronautical standpoint only. Obviously, they are the experts in this environment; however, we believe they have no real understanding regarding the "critical mission" aspect of UAV operations. If UAV operations remain under the oversight and control of the FAA, as is currently the case, domestic UAV operations will continue to be severely hampered or limited to the point of being useless.

If it is necessary to require Federal oversight of UAV operations within the United States, it would seem to be most appropriate that The Office of State and Local Law Enforcement within DHS would be the likely agency at the Federal level to be tasked with this role. DHS would serve as a database, keeping track of the types of UAV's in use, agencies using them, types of missions the UAV is being flown, mission results, keeping track of case results (if used in response to a criminal offense—narcotics warrant/SWAT operation), etc. To this end, we would propose having DHS work as a liaison for local agencies that use UAV's. DHS could provide

contact information, act as a resource and information tool, and as a monitoring/approving agency for public safety agency operations. Obviously, it is incumbent on such agencies to work through the COA approval process to allow the FAA the opportunity to scrutinize the aircraft, the associated operating systems, locations, etc. The FAA, however, does not need to go beyond that, other than the regular, routine review of agency flight operations to insure flight safety rules are being followed.

UAV systems for public safety agencies are extremely viable, effective, and economical means to enhance the public safety response to critical incidents. The use of drones by public safety agencies is, ultimately, about protecting and making safe the citizens we serve. Too much focus is being made on the impractical application of UAV's and not about its true design and purpose.

Mr. MCCAUL. Thank you, Chief.

The Chairman now recognizes Ms. Stepanovich.

STATEMENT OF AMIE STEPANOVICH, LITIGATION COUNSEL, ELECTRONIC PRIVACY INFORMATION CENTER

Ms. STEPANOVICH. Mr. Chairman and Members of the subcommittee, thank you for the opportunity to testify today concerning the use of drones in the United States. My name is Amie Stepanovich. I am Association Litigation Counsel at the Electronic Privacy Information Center, a nonpartisan research organization in the District of Columbia that is focused on focusing public attention on emerging issues in privacy and civil liberties. We thank you for holding this hearing today, and believe it is very important to address these issues early.

Drones greatly increase the capacity for domestic surveillance. Drones are specifically designed to carry highly invasive surveillance technology. They are cheaper to buy, maintain, and operate than typical aerial surveillance vehicles, and they can operate undetected in both urban and rural environments. Sensitive information collected by drones is particularly vulnerable to unlawful access. As previously discussed, drones are not secure.

EPIC observed in comments to the FAA on drone test site locations that drone hacking poses a threat to the security of lawful drone operations. Hackers are not only able to gain control of drone movements, but they are also able to intercept the date feeds transmitted by a drone.

We recognize that drone technology has very positive uses in the United States. It can be used to monitor for environmental abuse, help prevent the spread of forest fires, and assist in search-and-rescue operations. However, there are substantial legal and Constitutional issues involved in the deployment of aerial drones by Federal agencies.

As drone technology becomes cheaper, it will also become more widespread and the threat to privacy will become more substantial. EPIC supports compliance with current Federal law for the deployment of drone technology and limitations for Federal agencies and other organizations that obtain drones for a specified purpose, but the current state of the law is insufficient to address the drone surveillance threat. Legislation is needed to protect against the use of drones in surveillance tools and to provide for redress against drone operators who fail to comply with those protections.

Congress has directed the FAA to develop regulations that will encourage widespread deployment of drones in the United States. The forthcoming regulations will address licensing procedures for both public and private drone operators, including DHS, and the

Customs and Border Protection Bureau, a DHS component. Earlier this year in a formal petition to the FAA, EPIC urged the agency to conduct a rulemaking to implement privacy rules for domestic drones. EPIC's petition was joined by more than 100 other organizations, experts, and members of the public who also believed that privacy rules are necessary before drones enter our domestic skies in a more widespread way. The FAA has not yet responded to EPIC's request for agency action, and this failure to act means that there is also no administrative framework in place to regulate drones in our skies.

As has previously been mentioned, CBP currently operates 10 drones in the United States. The DHS Inspector General recently assessed CBP's practice in making drones available by other Federal agencies, including the Department of Defense, the FBI, the Secret Service, many local law enforcement agencies, and others.

Regarding privacy concerns, the Inspector General said that a standardized process was needed to request CBP drones for non-CBP purposes in order to provide transparency. To the extent that DHS chooses to operate drones within the United States, the agency must develop appropriate regulations to safeguard privacy. As you have indicated, Chairman McCaul, the privacy and security concerns arising from the use of drones needs to be addressed. Several of your colleagues have made efforts to address some of the privacy threats of drone. However, we believe those efforts are not sufficient.

There are several simple steps that we believe can protect privacy as the use of drones increases in our skies. First, Congress should pass targeted legislation. An initial step would be the passage of Congressman Austin Scott's bill to limit drone surveillance in the United States in cases where a warrant has not been first obtained. However, to fully address the invasive nature of drones, new legislation must prohibit nonspecific untargeted drone surveillance, limit the use of drone surveillance data collected, transmitted, stored, or shared, and require notice of drone surveillance operations and policies. The law should also provide for independent audits and oversight.

Second, Congress should expressly require Federal drone operators, including DHS and its components, to implement regulations subject to public notice and comment that address the privacy implications of drone use.

Finally, I think Congress should clarify the circumstances under which drones purchased by CBP in pursuit of its mission may be deployed for other purposes. The failure to make clear the circumstances when Federal and State agencies may deploy drones for aerial surveillance has already raised significant concerns about the agency's programs.

Once again I thank you for the opportunity to testify today, and I will be pleased to answer your questions.

[The prepared statement of Ms. Stepanovich follows:]

PREPARED STATEMENT OF AMIE STEPANOVICH

JULY 19, 2012

Mister Chairman and Members of the subcommittee, thank you for the opportunity to testify today concerning unmanned aerial systems, or drones, in the

United States. My name is Amie Stepanovich. I am the associate litigation counsel at the Electronic Privacy Information Center.

EPIC is a non-partisan research organization, established in 1994, to focus public attention on emerging privacy and civil liberties issues.[1] We work with a distinguished panel of advisors in the fields of law, technology, and public policy.[2] We have a particular interest in the protection of individual privacy rights against Government surveillance. In the last several years, EPIC has taken a particular interest in the unique privacy problems associated with aerial drones. We have urged the Federal Aviation Administration ("FAA"), as it considers new regulations to permit the widespread deployment of drones, to also develop new privacy safeguards.[3]

In my statement today, I will describe the unique threats to privacy posed by drone surveillance, the problems with current legal safeguards, the EPIC petition to the FAA, and the need for Congress to act.

We appreciate the subcommittee's interest in domestic drone use and its substantial impact on the privacy of individuals in the United States.

I. AERIAL DRONES POSE A UNIQUE THREAT TO PRIVACY

An unmanned aircraft, or drone, is an aerial vehicle designed to fly without a human pilot on board. Drones can either be remotely controlled or autonomous. Drones can be weaponized and deployed for military purposes.[4] Drones can also be equipped with sophisticated surveillance technology that makes it possible to identify individuals on the ground. Gigapixel cameras used to outfit drones are among the highest-definition cameras available, and can provide "real-time video streams at a rate of 10 frames a second."[5] On some drones, sensors can track up to 65 different targets across a distance of 65 square miles.[6] Drones may also carry infrared cameras, heat sensors, GPS, sensors that detect movement, and automated license plate readers.[7] Drones are currently being developed that will carry facial recognition technology, able to remotely identify individuals in parks, schools, and at political gatherings.[8]

In a report on drones published by EPIC in 2005, we observed, "the use of [drones] gives the federal government a new capability to monitor citizens clandestinely, while the effectiveness of the . . . surveillance planes in border patrol operations has not been proved."[9] Today, drones greatly increase the capacity for domestic surveillance.

Much of this surveillance technology could, in theory, be deployed in manned vehicles. However, drones present a unique threat to privacy. Drones are designed to undertake constant, persistent surveillance to a degree that former methods of surveillance were unable to achieve. Drones are cheaper to buy, maintain, and operate than helicopters, or other forms of aerial surveillance.[10] Drone manufacturers have

---

[1] *About EPIC,* EPIC, *http://www.epic.org/about* (last visited July 16, 2012).

[2] *EPIC Advisory Board,* EPIC, *http://www.epic.org/epic/advisory_board.html* (last visited July 16, 2012).

[3] *Unmanned Aerial Vehicles (UAVs) and Drones,* EPIC, *http://www.epic.org/privacy/drones* (last visited July 16, 2012).

[4] See, e.g., *Predator B UAS,* General Atomics Aeronautical, *http://www.ga-asi.com/products/aircraft/predator_b.php* (last visited June 25, 2012); *X–47B UCAS,* Northrop Grumman, *http://www.as.northropgrumman.com/products/nucasx47b/index.html* (last visited July 16, 2012).

[5] *US Army Unveils 1.8 Gigapixel Camera Helicopter Drone,* BBC News Technology (Dec. 29, 2011), *http://www.bbc.co.uk/news/technology-16358851.*

[6] Id.

[7] Customs and Border Protection Today, Unmanned Aerial Vehicles Support Border Security (July/Aug. 2004), available at *http://www.cbp.gov/xp/CustomsToday/2004/Aug/other/aerial_vehicles.xml.*

[8] Clay Dillow, *Army Developing Drones that Can Recognize Your Face From a Distance,* PopSci (Sept. 28, 2011, 4:01 PM), *http://www.popsci.com/technology/article/2011-09/army-wants-drones-can-recognize-your-face-and-read-your-mind.*

[9] *Spotlight on Surveillance: Unmanned Planes Offer New Opportunities for Clandestine Government Tracking* (August 2005), EPIC, *http://epic.org/privacy/surveillance/spotlight/0805/* (last visited July 16, 2012).

[10] Nick Wingfield and Somini Sengupta, *Drones Set Sights on U.S. Skies,* NY Times (Feb. 17, 2012), available at *http://www.nytimes.com/2012/02/18/technology/drones-with-an-eye-on-the-public-cleared-to-fly.html?pagewanted=all; http://www.wired.com/autopia/2012/05/drone-auto-vids/;* Sabrina Hall, *Shelby County Sheriff's Department Wants Drones,* WREG (May 3, 2012), available at *http://wreg.com/2012/05/03/shelby-county-sheriffs-department-wants-drones/.* Drones can run from $300 for the most basic drone, able to record and transmit video, to $18 million for a General Atomics Predator B drone, the model owned by the United States Bureau of Customs and Border Protection. See *Parrot AR.Drone 2.0,* Apple, *http://store.apple.com/us/product/H8859ZM/A* (last visited July 16, 2012); Office of the Inspector Gen., Dep't Homeland

Continued

recently announced new designs that would allow drones to operate for more than 48 consecutive hours,[11] and other technology could extend the flight time of future drones out into weeks and months.[12] Also, "by virtue of their design, size, and how high they can fly, [drones] can operate undetected in urban and rural environments."[13]

The ability to link facial recognition capabilities on drones operated by the Department of Homeland Security ("DHS") to the Federal Bureau of Investigation's Next Generation Identification database or DHS' IDENT database, two of the largest collections of biometric data in the world, exacerbates the privacy risks.[14] Drones could be deployed to monitor individuals in a way that was not possible previously.

Sensitive information collected by drones is particularly vulnerable to unlawful access. In comments addressing the issue of drone test site locations, EPIC observed, "drone hacking," or the process of remotely intercepting and compromising drone operations, poses a threat to the security of lawful drone operations.[15] Recent examples have highlighted the ease with which drones may be "hacked". The University of Texas was able to use GPS signals in order to gain full control of a drone.[16] The researchers indicated that the method could be use on any drone operated over the civilian GPS band, which include the majority of drones in the United States.[17] Hackers are also able to intercept video and audio feeds, as well as other information collected and transmitted by surveillance drones.[18]

Within DHS, the Bureau of Customs and Border Protection ("CBP") is the primary operator of unmanned aerial drones. CBP operates ten drones in the United States, including the Predator B and its maritime variant the Guardian, at a cost per unit of about $18 million each.[19] By 2016, CBP plans to operate 24 drones, with the ability to deploy one anywhere in the continental United States within 3 hours.[20]

But there are problems with the CBP program. According to a recent report of the DHS Inspector General, CBP "needs to improve planning of its unmanned aircraft systems program to address its level of operation, program funding, and resource requirements, along with stakeholder needs."[21] The Inspector General assessed CBP's practice of making the drones available for use by other Federal and State agencies, including the Bureau of Land Management, the Department of Defense, the Federal Bureau of Investigation, the Texas Rangers, the United States Forest Service, the National Oceanic and Atmospheric Administration, the Office of Border Patrol, the United States Secret Service, the Immigrations and Customs Enforcement, the Federal Agency Management Agency, and local Law Enforcement Agencies.[22]

The Inspector General concluded that all purchases of new drones should be suspended until CBP develops a plan that addresses "necessary operations, maintenance, and equipment."[23] Regarding privacy concerns, the DHS Inspector General

---

Security, OIG–12–85, *CBPs Use of Unmanned Aircraft Systems in the Nation's Border Security* (May 2012), available at *http://www.oig.dhs.gov/assets/Mgmt/2012/OIG_12-85_May12.pdf* [hereinafter DHS OIG Report] at 2.

[11] Mark Brown, *Lockheed Uses Ground-Based Laser to Recharge Drone Mid-Flight* (July 12, 2012), available at *http://www.wired.co.uk/news/archive/2012-07/12/lockheed-lasers.*

[12] Steven Aftergood, *Secret Drone Technology Barred by "Political Conditions"* (Mar. 22, 2012), available at *http://www.fas.org/blog/secrecy/2012/03/sandia_drone.html.*

[13] Jennifer Lynch, *Are Drones Watching You?,* Electronic Frontier Foundation (Jan. 10, 2012), available at *https://www.eff.org/deeplinks/2012/01/drones-are-watching-you.*

[14] See Next Generation Identification, Federal Bureau of Investigation, *http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi/ngi2/* (last visited July 16, 2012); Privacy Impact Assessment, Department of Homeland Security, Automated Biometric Identification System (IDENT) (July 31, 2006), *http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_ident_final.pdf.*

[15] Comments of EPIC to the FAA re: Request for Comments on Unmanned Aircraft System Test Sites (May 8, 2012), available at *http://epic.org/privacy/drones/EPIC-FAA-2012-0252.pdf.*

[16] Alex Fitzpatrick, *Researchers Prove Drones Can Be Hacked,* Mashable (June 29, 2012), available at *http://mashable.com/2012/06/29/drone-hacking/.*

[17] Id.

[18] Siobhan Gorman, Yochi Dreazen, and August Cole, *Insurgents Hack U.S. Drones,* Wall St. J. (Dec. 17, 2009), available at *http://online.wsj.com/article/SB126102247889095011.html.*

[19] See *DHS OIG Report,* supra note 11 at 2.

[20] William Booth, *More Predator Drones Fly U.S.-Mexico Border,* WASH. POST (Dec. 21, 2011), available at *http://www.washingtonpost.com/world/more-predator-drones-fly-us-mexico-border/2011/12/01/gIQANSZz80_story.html.*

[21] See *DHS OIG Report,* supra note 11 at 1.

[22] Id. at 6–7.

[23] Id. at 8

said that a standardized process was needed to request CBP drones for non-CBP purposes, in order to "provide transparency."[24]

II. CURRENT PRIVACY SAFEGUARDS ARE INADEQUATE

Current regulations permit civil organizations to operate a drone within the United States only pursuant to a special "experimental" designation.[25] However, Government operators of drones do not have a similar restriction.[26] Recent policy changes at the FAA, the administrative agency in charge of licensing both Governmental and non-Governmental drones to operate in the National airspace, are designed to "streamline" the process by which Government agencies, including law enforcement, receive drone licenses.[27]

The CBP currently operates drones with few regulations concerning privacy. No current legislation limits the visual surveillance that a DHS drone may engage in. And while the Privacy Act of 1974 expressly prescribes the circumstances under which agencies can retain personally identifiable information, the agency may still exempt itself from the Privacy Act provisions that limit the collection and use of personal information.[28] DHS has not sought public comment on or published any specific rules or guidelines that restrict the surveillance practices of its drone program. Also, despite recent releases of records, the FAA's process for the application for and approval of a drone license are still mostly opaque, preventing any transparency or accountability for operators.[29]

There are substantial legal and Constitutional issues involved in the deployment of aerial drones by Federal agencies that need to be addressed. And, as we have noted, no legislation currently provides adequate safeguards to protect privacy rights against the increased use of drones in the United States.

As drone technology becomes cheaper and more proliferate, the threat to privacy will become more substantial. High-rise buildings, security fences, or even the walls of a building are not barriers to increasingly common drone technology.

The Supreme Court is aware of the growing risks to privacy resulting from new surveillance technology but has yet to address the specific problems associated with drone surveillance. In *United States* v. *Jones,* a case that addressed whether the police could use a GPS device to track the movement of a criminal suspect without a warrant, the Court found that the installation and deployment of the device was an unlawful search and seizure.[30] Justice Sotomayor in a concurrence pointed to broader problems associated with new forms of persistent surveillance.[31] And Justice Alito, in a separate concurrence joined by three other Justices, wrote, "in circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."[32]

As you have indicated, Mister Chairman, the privacy and security concerns arising from the use of drones needs to be addressed.[33] Several of your colleagues in the House of Representatives have made efforts to address some of the privacy threats of drones, and we support these initiatives.

---

[24] Id. at 7.

[25] See Fact Sheet, FAA, Unmanned Aircraft Systems (UAS) (Dec. 1, 2010), available at *http://www.faa.gov/news/fact_sheets/news_story.cfm?newsid=6287* ("A Special Airworthiness Certificate in the Experimental Category is the only certification available to civil operators of UAS.").

[26] See Id. ("The COA process is available to public entities, such as government agencies (including local law enforcement and state universities), who want to fly a UAS in civil airspace.").

[27] See *FAA Makes Progress with UAS Integration,* Federal Aviation Administration, (May 14, 2012, 3:09 PM) *http://www.faa.gov/news/updates/?newsId=68004* ("The FAA has been working with its government partners to streamline COA procedures as part of the effort to ensure [drones] are safely integrated into the [national airspace system].").

[28] See e.g. 5 U.S.C. § 552a(j) (allowing agencies to exempt themselves from maintenance requirements pursuant to law enforcement reasons).

[29] See *FAA Releases Lists of Drone Certificates—Many Questions Left Unanswered,* Electronic Frontier Foundation, (Apr. 19, 2012) *https://www.eff.org/deeplinks/2012/04/faa-releases-its-list-drone-certificates-leaves-many-questions-unanswered* (listing information about the FAA's drone authorization process that remains unknown).

[30] *United States* v. *Jones,* 132 S.Ct. 945, 949 (2012). See also *U.S.* v. *Jones,* EPIC, *http://epic.org/amicus/jones/*.

[31] Id. at 954–57.

[32] Id. at 964.

[33] Press Release, United States House of Representatives Committee on Homeland Security, A Look Ahead: House Committee on Homeland Security (July 13, 2012), available at *http://homeland.house.gov/press-release/look-ahead-house-committee-homeland-security-34* ("However, no Federal agency is taking responsibility for creating comprehensive policies and regulations concerning the use of these systems domestically. Additionally, vulnerabilities to 'drone' hackers exist, as recently demonstrated by researchers at the University of Texas, raising concerns these vehicles could be commandeered by terrorists or others with ill intent.").

An amendment to the National Defense Authorization Act of 2013, introduced by Congressman Jeff Landry (R–LA) and passed by the House, would prohibit information collected by drones operated by the Department of Defense from being used in court as evidence if a warrant was not obtained.[34] In June, House Representative Austin Scott (R–FL) introduced legislation to expand this protection, requiring all law enforcement to first obtain a warrant before conducting any criminal surveillance.[35] Also, Congressman Markey (D–MA) and Congressman Barton (R–TX) sent a letter to the FAA raising concerns about the increased use of drones in the United States, noting, "there is . . . potential for drone technology to enable invasive and pervasive surveillance without adequate privacy protections."[36]

However, these measures are not sufficient to protect the myriad of privacy interests implicated by increased drone use.

III. EPIC HAS URGED THE ADMINISTRATIVE ACTION TO ADDRESS DRONE USE

The FAA has been directed by Congress to develop regulations in order to permit more widespread deployment of drones in the United States.[37] The forthcoming regulations will address licensing and procedures for both public and private drone operators, including DHS and CBP. Experts, including Professor Ryan Calo, the former Director of Privacy and Robotics at the Center for Internet and Society at Stanford Law School, have noted that this effort will have significant privacy implications.[38]

Earlier this year, in a formal petition to the agency, EPIC urged the FAA to conduct a privacy rulemaking on the use of drones, with the aim of creating regulations to ensure baseline privacy protections.[39] EPIC's petition was joined by more than 100 organizations, experts, and members of the public who also believe that drones should not be more widely deployed until privacy safeguards are established.[40]

The FAA has thus far failed to respond to EPIC's request for agency action. The FAA's failure to act means that there is no framework in place that ensures that civilian operators and Federal agencies, such as DHS, utilize drone technology in a privacy-protective manner. To the extent that DHS, as well as other agencies, chooses to operate drones within the United States, we believe that the DHS should also develop appropriate regulations to safeguard privacy.

Specifically, the Department of Homeland Security must utilize its Privacy Office, one of the most robust, well-funded Privacy Offices in the Federal Government. The Privacy Office at DHS "conducts [Privacy Impact Assessments] on technologies, rulemakings, programs, and activities . . . to ensure that privacy considerations and protections are incorporated into all activities of the Department."[41]

However, despite a DHS component operating one of the largest, and definitely the most well-publicized drone fleet in the United States for the past 7 years, a Privacy Impact Assessment has never been conducted on the privacy impact of drone surveillance. At a minimum, we believe that if the CPB plans to continue the drone program, the DHS privacy office must assess the privacy impact of the program and publish a report for public review.

---

[34] See H.R. 4310, 112th Cong. § 1084 (2012), available at *http://www.gpo.gov/fdsys/pkg/BILLS-112hr4310rfs/pdf/BILLS-112hr4310rfs.pdf;* see also Pete Kasperowicz, *House Approves 20 en bloc Amendments to Defense Reauthorization, Including Satellite Language,* the Hill (May 17, 2012), available at *http://thehill.com/blogs/floor-action/house/228147-ndaa-update-1-house-approves-20-en-bloc-amendments-including-satellite-language.*

[35] Preserving Freedom from Unwarranted Surveillance Act of 2012, H.R. 5925, 112th Cong. (2012), available at *http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.5925:.*

[36] Letter from Congressmen Edward J. Markey and Joe Barton to Michael Huerta, Acting Federal Aviation Administration Administrator (Apr. 19, 2012) available at *http://markey.house.gov/sites/markey.house.gov/files/documents/4-19-12.Letter%20FAA%20Drones-%20.pdf.*

[37] See FAA Modernization and Reform Act of 2012, Pub. L. 112–95 § 324(c)(1) (2012), available at *http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.658:.*

[38] See, M. Ryan Calo, *The Drone as a Privacy Catalyst,* 64 Stan. L. Rev. Online 29 (2011), available at *http://www.stanfordlawreview.org/online/drone-privacy-catalyst;* see also Ryan Calo and John Villasenor, *Ten Myths About Drones,* Huffington Post (May 22, 2012), *http://www.huffingtonpost.com/ryan-calo/drones-myths_b_1537040.html; Drones Over America: What Can They See,* NPR (Mar. 12, 2012), available at *http://www.npr.org/2012/03/12/148293470/drones-over-america-what-can-they-see.*

[39] Petition from EPIC, et al., to Michael P. Huerta, Acting Administrator, FAA (Feb. 24, 2012), available at *http://epic.org/privacy/drones/FAA-553e-Petition-03-08-12.pdf* [hereinafter EPIC Petition to FAA].

[40] Id.

[41] Guide to Implementing Privacy, Department of Homeland Security (June 2010), *http://www.dhs.gov/xlibrary/assets/privacy/dhsprivacyoffice-guidetoimplementingprivacy.pdf* at 14.

IV. CONGRESS SHOULD ESTABLISH SAFEGUARDS RELATED TO THE USE OF DRONES

There are several strategies to provide meaningful privacy protections that address the increased use of drones in our domestic skies. First, Congress should pass targeted legislation, based on principles of transparency and accountability. A first step would be the consideration and passage of Congressman Scott's bill to limit the use of drone surveillance in criminal investigations without a warrant.

State and local governments have also considered laws and regulations to further prevent abuses of drone technology.[42] These proposals would serve as a good basis for Federal legislation. Drone legislation should include:

- *Use Limitations*.—Prohibitions on general surveillance that limit drone surveillance to specific, enumerated circumstances, such as in the case of criminal surveillance subject to a warrant, a geographically-confined emergency, or for reasonable non-law enforcement use where privacy will not be substantially affected;
- *Data Retention Limitations*.—Prohibitions on retaining or sharing surveillance data collected by drones, with emphasis on identifiable images of individuals;
- *Transparency*.—Requiring notice of drone surveillance operations to the extent possible while allowing law enforcement to conduct effective investigations. In addition, requiring notice of all drone surveillance policies through the Administrative Procedure Act.

These three principles would help protect the privacy interests of individuals. In addition, the law should provide for accountability, including third-party audits and oversight for Federally-operated drones and a private right of action against private entities that violate statutory privacy rights.

Second, Congress should act to expressly require Federal agencies that choose to operate drones, such as DHS and its components, to implement regulations, subject to public notice and comment, that address the privacy implications of drone use. Recently, in *EPIC* v. *DHS,* the D.C. Circuit Court of Appeals ruled that the Department of Homeland Security violated the Administrative Procedure Act when it chose to deploy body scanners as the primary screening technique in U.S. airports without the opportunity for public comment.[43] The Court observed that there was "no justification for having failed to conduct a notice-and-comment rulemaking."[44] We believe that the public has a similar right to comment on new surveillance techniques, such as unmanned aerial vehicles, undertaken by Federal agencies within the United States.

Finally, Congress must clarify the circumstances under which the drones purchased by the CBP in pursuit of its mission may be deployed by other agencies for other purposes. The failure to make clear the circumstances when Federal and State agencies may deploy drones for aerial surveillance has already raised significant concerns about the agency's program.[45]

V. CONCLUSION

The increased use of drones to conduct surveillance in the United States must be accompanied by increased privacy protections. We recognize that drone technology has the potential to be used in positive ways. For example, drones may be used to monitor for environmental abuse, prevent the spread of forest fires, and assist in the rescue of individuals in dangerous situations.[46]

However, the current state of the law is insufficient to address the drone surveillance threat. EPIC supports legislation aimed at strengthening safeguards related

---

[42] See, e.g., Erika Neddenien, *ACLU Teams with Lawmaker to Push Regulation of Unmanned Drones in VA,* WTVR (July 12, 2012) *http://wtvr.com/2012/07/12/aclu-working-with-lawmaker-to-push-regulation-of-unmanned-drones-in-va/* (last visited July 16, 2012); Press Release, Seattle City Council, Seattle City Council Committee to Discuss Drones in Seattle and the Issues They Present (May 1, 2012), available at *http://council.seattle.gov/2012/05/01/seattle-city-council-committee-to-discuss-drones-in-seattle-and-the-issues-they-present/*.

[43] See *EPIC* v. *DHS,* 653 F.3d 1 (D.C. Cir. 2011).

[44] Id. at 8.

[45] See Jason Koebler, *First Man Arrested with Drone Evidence Vows to Fight Case,* US News (Apr. 9, 2012), available at *http://www.usnews.com/news/articles/2012/04/09/first-man-arrested-with-drone-evidence-vows-to-fight-case.*

[46] See, e.g., Tim Wall, *Flying Drones Fight Fires,* Discovery News (Nov. 10, 2011), available at *http://news.discovery.com/earth/flying-drones-fight-fires-111110.html;* Meghan Keneally, *Drone Plane Spots a River of Blood Flowing From the Back of a Dallas Meat Packing Plant,* Daily Mail Online (Jan. 24, 2012), available at *http://www.dailymail.co.uk/news/article-2091159/A-drone-plane-spots-river-blood-flowing-Dallas-meat-packing-plant.html;* Sean Holstege, *Drones' Good Flies Hand in Hand with Bad, Experts Fear,* AZCentral (July 7, 2012), available at *http://www.azcentral.com/12news/news/articles/2012/07/07/20120707arizona-unmanned-drones-concerns.html.*

to the use of drones as surveillance tools and allowing for redress for drone operators who fail to comply with the mandated standards of protection. We also support compliance with the Administrative Procedure Act for the deployment of drone technology and limitations for Federal agencies and other organizations that initially obtain a drone for one purpose and then wish to expand that purpose.

Thank you for the opportunity to testify today. I will be pleased to answer your questions.

Mr. MCCAUL. Thank you, Ms. Stepanovich.

Let me start first with Mr. Dillingham. You mentioned, as I did in my opening statement, TSA identified a potential terrorist threat through the use of these UAV systems, the FARC in Colombia, and they talk about Hezbollah. Then, of course, their concerns really came to fruition last September when it was reported by the Associated Press: Man to blow up Pentagon and U.S. Capitol is arrested, and this was a drone that he was going to use to do that.

Mr. DILLINGHAM. Yes, sir.

Mr. MCCAUL. The United States Capitol and the Pentagon, the very targets of 9/11. Yet the Department and as you recommended through the GAO, the Department has a role in this to provide a security assessment and a National policy. The Department apparently disagrees with you and frankly disagrees with me as the Chairman, and has refused to provide testimony before this committee here today. I find that reprehensible. I believe the Department should come before this committee to answer why they believe they should not have a role in this, when they had a direct threat to the United States Capitol and the Pentagon, and yet they don't see it as a role of the Department of Homeland Security to come up with a policy and a security assessment to monitor the threat that these domestic drones can pose to the American people.

Do you have any idea what their rationale is?

Mr. DILLINGHAM. Mr. Chairman, we specifically followed up in preparation for this hearing. But before that, the GAO has a policy of once we issue a recommendation that we do periodic follow-ups because those agencies are not only responsible for reporting to the GAO, but they also report to the Congress. So we followed up most recently and asked the TSA again about their position: Had their position changed? They indicated that their position had not changed, but they added—their added comments were that they were doing, they were taking actions that they thought were sufficient to address the issue.

As you know, one of the central tenets of TSA's security are risk analysis or risk assessment so that they know where they would best deploy their resources. So we asked for some evidence of risk assessment that was done with regard to UAVs or UASs. We were not able to obtain that from DHS.

So we still think that our recommendation is valid and needed to be addressed. For balance, though, let me say that DHS is participating with the Joint Planning and Development Office as part of the cross-Government-wide development for plans. But in terms of exactly what the nature and scope of that participation is beyond being members of that particular group, we were not able to ascertain at this point. But we continue to work that issue for our full report.

Mr. MCCAUL. Well, I can't ascertain it either. If they won't come before this committee to describe what they are doing, how can we

possibly know what they are doing? You said they have taken certain precautions, but yet they will not come before this committee to tell us what precautions they are taking. They have defied not only you but I think the will of this committee and the will of the American people. I am not pleased about that, obviously.

Let me go to Chief McDaniel. You actually received Homeland Security grants to purchase these drones; is that correct?

Chief MCDANIEL. That is correct.

Mr. MCCAUL. But yet they have no role?

Chief MCDANIEL. No, sir.

Mr. MCCAUL. I hope you are saying that facetiously. You said you believe that there needs to be Federal oversight by the Department of Homeland Security; is that correct?

Chief MCDANIEL. Yes, sir. There is a difference between the aviation aspect of it that certainly the FAA is entitled to as experts in that environment, but they do not have the understanding and the expertise that I believe an agency such as the DHS would have in understanding the operational roles and missions that, in our case, law enforcement would have and the needs that we would have.

Mr. MCCAUL. I tend to agree with you. I think FAA provides the safety of the routes but not security.

Tell me just very briefly the legitimate law enforcement purposes. I do believe there is a legitimate law enforcement purpose for the use of these domestically. Can you expand on that?

Chief MCDANIEL. Well, we have periodic needs for our SWAT team to be called out and respond to critical incidents involving barricaded suspects, high-risk warrants, and this is an asset that provides that incident commander with a situational awareness to see everything that is going on within that incident so that he can better manage that incident and bring it to a safe conclusion.

Mr. MCCAUL. I agree. I think it should be limited to a specific instance or mission within a legitimate law enforcement purpose. I think what most American people do not want to see are thousands of these drones being eyes of the skies, sort of spying on the American people.

That takes me to you, Ms. Stepanovich. When it comes to the privacy issues, which I think are of legitimate concern, I think people can accept if these are being used for a manhunt, as we use law enforcement helicopters. They are used in the sky for various legitimate law enforcement purposes. What they don't want to see is sort of spying without any mission involved in the plan. So there is no policy.

The Department of Homeland Security has an Office of Privacy. Don't you believe they should be involved in working with people like yourself and people like the sheriff and people like the GAO to develop a privacy policy?

Ms. STEPANOVICH. EPIC does believe that. In fact, we believe that a great first step, DHS has the most robust privacy office in the Federal Government, and they have not even done a privacy impact assessment on their own drone program, which is also one of the most robust and definitely one of the most well-publicized programs in the Federal Government. So they have not even gone in to determine what impact these drones will have on the American public as they use them. We think that would be a great first

step, and then after that has been completed, to really go in and to monitor these and determine what they can be used for and what they cannot be used for.

Mr. MCCAUL. Let me just conclude by saying that while you all may not agree on all of the issues, one thing you do agree on is that DHS has a role here to play, whether it is providing a security analysis, working with the State and locals and with privacy. I hope this hearing gets their attention. I hope your testimony gets their attention to step up to the plate and do something about this.

With that, I recognize the Ranking Member, Mr. Keating.

Mr. KEATING. Thank you, Mr. Chairman.

Chief McDaniel, I am not saying by any stretch of the imagination you would do this, but just a question for you: If there was a law enforcement person, chief or other official, for instance, who wanted to replace the rubber bullets with real bullets, do you know of any State law, rule, regulation, that could stop anyone from doing that in place right now?

Chief MCDANIEL. I am not aware of any law within the State of Texas that would prevent that; no, sir.

Mr. KEATING. I would suggest that that is probably typical for all States. Do you think that we should be looking at this both at the Federal and State level?

Chief MCDANIEL. Certainly I can understand it as being a concern. The actuality of that ever occurring is slim and none, in my view, based upon the platform, the accuracy that would be required, all of those things that go into a lethal or less-than-lethal-force situation. I do not believe these UAVs are appropriate for that type of a weapons platform.

Mr. KEATING. Thank you.

A question for Ms. Stepanovich. I can just envision, probably in the more extreme example, the paparazzi or someone else—you know how they invade someone's privacy right now—abusing these vehicles. Is there any way even besides criminal law and other law, is there a way that we could trace someone who is photographing or doing video cam work on people in their private lives out in their backyard or in front of a pool or wherever, is there any way we can trace that so there can be civil action? Do you think there is available civil action that could be brought forward?

Ms. STEPANOVICH. On the State level, there could be civil action in some States. You would have to look to the Peeping Tom laws. However, some of those are very, very specific and they require the motivation to catch a person in a state of undress. Other than that, there really is no legislation that would address those circumstances. Right now with the opaque process for licensing these drones to be used and the fact that hobbyists can gain control of a drone and use it without getting a license at all, there is additional barriers too, especially the paparazzi using these.

Mr. KEATING. In addition to Homeland Security, do you believe the FAA should be involved in setting these kinds of regulations?

Ms. STEPANOVICH. I believe the FAA has a role. It do not believe that they are set up to go the full distance that the Department of Homeland Security can go. However, they are the licensing authority, and in their authority they have the ability to request the description of what a drone is going to be licensed for and what

they will be used for and to hold the licensee to task for that purpose. We don't believe that is taking place right now, and we think that would be an appropriate function of the FAA.

Mr. KEATING. I will just conclude by commenting that I agree with the Chairman as well. There is some need of some kind of oversight because people's privacy rights are in danger. There is a potential for terrorist activities that are involved and misuse that way. There should be some kind of control other than the good common sense of law enforcement as to how this is used as well. We are hopeful we can follow up this hearing with that kind of input from Homeland Security and perhaps FAA.

Mr. MCCAUL. I thank the Ranking Member for his comments.

The Chairman now recognizes Mr. Duncan from South Carolina.

Mr. DUNCAN. Thank you, Mr. Chairman. I do want to follow up. I think we do need a hearing with the FAA to bring them forward and ask questions about what they are doing to implement permitting and certificates in this country with the flying of unmanned aerial systems because we have got a robust civilian aviation population in this country. If you have visual flight rules and you have got a civilian aviator that goes up in his Cessna 172, he is not filing a flight plan. He is generally currently probably not looking to see if there is a certificate whether the sheriff is flying a drone in the area. These drone pilots, they are not looking forward for other aircraft in their air space, they are looking down at whatever they are surveilling. So I think there is a real threat to civilian aviation with unmanned aerial systems, especially if we see a dramatic increase that is projected based upon the information that has been provided today. So I think that is a valid question that we need to talk with the FAA about with regard to civilian aviation and VFR flight rules.

The gist of my concern about drones and unmanned aerial systems is the privacy issue. It is a real issue and it is a real concern to the constituents I represent and it is a real concern to Americans all across this great land on what the Government is surveilling. We just had recently an episode in Nebraska where farmers were upset that the EPA was flying aircraft and possibly UAVs to check their fencing and whether their cattle were getting into streams, and enforcement issues, are they going to use UASs for that going forward. I am a cosponsor of Austin Scott's bill, which I think is an important piece of legislation.

When I think about privacy issues, I think about what we have done in the war on terror and surveillance of people that we suspect are involved in terrorism. In order to listen in on their phone conversations, whether cell phone or landline, the FISA court is involved. Well, is the FISA court going to be involved in unmanned aerial systems surveilling American citizens in this country on what their activities are, whether it is terrorist activities or narcotic activities? Where is the right of privacy and where does a court such as FISA get involved in this?

I think these are legitimate questions that we need to ask. We have an Office of Privacy within Homeland Security that the Chairman mentioned earlier. That Office of Privacy is there for a reason. It is to make sure that the Department of Homeland Security is involved in making sure that the privacy rights of American citizens

are not violated as we try to protect this great country. Is that Office of Privacy involved with the Department of Homeland Security with regard to unmanned aerial systems?

I think it is a valid question for us to ask, and I want to thank Amie for being here. I want to ask you: What methods of civil liberty protection are best to cooperate with this growth in UAS?

Ms. STEPANOVICH. We think that the best principles to always look at are transparency and accountability. So we are looking at, again, procedures at FAA to make sure that drone operators aren't allowed to utilize their drones for purposes outside of what they have initially been licensed for. We want to see DHS implement regulations protecting privacy and ensuring that they cannot be used for generalized surveillance. We think that that is not in line with Constitutional principles and should not be used. Then we would like to see, as we have proposed in our longer statement, legislation that is really geared towards protecting these rights. We think that it is important to do this now, as previous witnesses have stated. Violations have not occurred yet, and if we wait for the drones to go up in the air before we act, I think that we are going to regret it.

Mr. DUNCAN. Well, thank you for protecting civil liberties in this country and what you are doing.

I come from South Carolina. We are on the coast. There is the threat of hurricanes. I can see and understand a certificate is issued for, whether it is the EPA or whether it is Homeland Security or some organization, to fly the coastline prior to a hurricane coming in to assess changes in the environment, take real-time actual aerial photos that can be used. I can understand a certificate being issued for Custom and Border Patrol if they know that there is an area of the border that is being exploited, a one-time certificate. I can understand the need for some sort of privacy committee to issue those certificates. I can understand a one-time certificate or a temporary certificate being issued to a sheriff if you had a prison break or you had a lot of drug activity. But these are isolated incidents. They are not carte blanche flying of unmanned aerial systems across this country.

Mr. Dillingham, why has the Department of Homeland Security been so slow to develop policies and guidance related to the domestic use of drones?

Mr. DILLINGHAM. That is a good question, sir. We have not been able to get an answer from DHS or TSA why they have not followed our recommendations.

We have been told by many stakeholders that it is better to act on these potential issues before we have a crisis or before some of these things occur because oftentimes not only does it take regulations 2 or 3 years to be enacted, but oftentimes when regulations are enacted in a crisis situation, sometimes they are not the best work that the agencies do. So we continue to follow-up with DHS and point out that we think they have a role in the UAV situation as well, both in terms of privacy as well as security.

Mr. DUNCAN. Well, I don't want to wait for a crisis situation. If I know this Chairman as well as I think I know him, I believe we will have the Department of Homeland Security sitting where you are sitting to answer these tough questions, and I yield back.

Mr. MCCAUL. I thank the gentleman for his confidence in his Chairman. Let me just say that not only have they been slow, they have completely disregarded Mr. Dillingham and the GAO and they have defied this committee by refusing to testify on the issue, indicating that they have no role, no role whatsoever in the domestic use of UAVs.

With that, I now recognizes Ms. Clarke.

Ms. CLARKE. Thank you very much, Mr. Chairman. Let me add my voice to that of my colleague about concern with respect to DHS and their response to this committee. Clearly this is an emerging threat, and it is certainly within the jurisdiction of DHS to respond to this committee, this subcommittee, in its request to know where they stand with regards to this. It is not acceptable to not participate, to not share with us their thinking when you think about the implications of these devices.

Dr. Dillingham, you note in your testimony that currently no Federal agency has specific statutory responsibility to regulate privacy matters related to UAS. Do you agree with Ms. Stepanovich that the responsible agency should be DHS? In your opinion, which agency is best positioned to take this on, and why?

Mr. DILLINGHAM. I think our answer at this point is we are probably not in a position to say who should be responsible, but we think the process that is under way now in terms of the potential agencies, including Justice, Homeland Security, FAA, should be working together to figure out who in fact is going to take the lead in these particular areas. It is in no one's mission at this point because UASs didn't exist in the domestic area before not too long ago, so we think this is something for collaboration and cooperation, but definitely something that needs to be attended to now rather than later.

Ms. CLARKE. Ms. Stepanovich, do you agree?

Ms. STEPANOVICH. We do agree, and we agree that as other agencies implement drones in the United States, we think that those agencies should also take on a role in regulating and protecting the privacy of the people who may come under surveillance because of those operations.

Ms. CLARKE. Ms. Stepanovich, the organization representing UAV manufacturers and operators recently released an industry code of conduct. That included some privacy safeguards. Moreover, compliance with the guidelines is both voluntary and unenforceable. Although the attempt to address concerns in that manner was laudable, can you explain why official action with enforcement is necessary?

Ms. STEPANOVICH. I am holding the voluntary code of conduct right here. It is 1 page front and back. All they say on privacy is we will respect the privacy of individuals. As you mentioned, it is both voluntary and nonenforceable. We believe that without official action, if everything comes down to that one line on this 1 page, that privacy will not be sufficiently protected.

[The information follows:]

ASSOCIATION FOR UNMANNED VEHICLE SYSTEMS INTERNATIONAL: UNMANNED AIRCRAFT SYSTEM OPERATIONS INDUSTRY "CODE OF CONDUCT"

The emergence of unmanned aircraft systems (UAS) as a resource for a wide variety of public and private applications quite possibly represents one of the most sig-

nificant advancements to aviation, the scientific community, and public service since the beginning of flight. Rapid advancements in the technology have presented unique challenges and opportunities to the growing UAS industry and to those who support it. The nature of UAS and the environments which they operate, when not managed properly, can and will create issues that need to be addressed. The future of UAS will be linked to the responsible and safe use of these systems. Our industry has an obligation to conduct our operations in a safe manner that minimizes risk and instills confidence in our systems.

For this reason, the Association for Unmanned Vehicle Systems International (AUVSI), offers this Code of Conduct on behalf of the UAS industry for UAS operation. This code is intended to provide our members, and those who design, test, and operate UAS for public and civil use, a set of guidelines and recommendations for safe, non-intrusive operations. Acceptance and adherence to this code will contribute to safety and professionalism and will accelerate public confidence in these systems.

The code is built on three specific themes: Safety, Professionalism, and Respect. Each theme and its associated recommendations represent a "common-sense" approach to UAS operations and address many of the concerns expressed by the public and regulators. This code is meant to provide UAS industry manufacturers and users a convenient checklist for operations and a means to demonstrate their obligation to supporting the growth of our industry in a safe and responsible manner. By adopting this Code, UAS industry manufacturers and users commit to the following:

SAFETY

- We will not operate UAS in a manner that presents undue risk to persons or property on the surface or in the air.
- We will ensure UAS will be piloted by individuals who are properly trained and competent to operate the vehicle or its systems.
- We will ensure UAS flights will be conducted only after a thorough assessment of risks associated with the activity. This risks assessment will include, but is not limited to:
  - Weather conditions relative to the performance capability of the system.
  - Identification of normally anticipated failure modes (lost link, power plant failures, loss of control, etc) and consequences of the failures.
  - Crew fitness for flight operations.
  - Overlying airspace, compliance with aviation regulations as appropriate to the operation, and off-nominal procedures.
  - Communication, command, control, and payload frequency spectrum requirements.
  - Reliability, performance, and airworthiness to established standards.

PROFESSIONALISM

- We will comply with all Federal, State, and local laws, ordinances, covenants, and restrictions as they relate to UAS operations.
- We will operate our systems as responsible members of the aviation community.
- We will be responsive to the needs of the public.
- We will cooperate fully with Federal, State, and local authorities in response to emergency deployments, mishap investigations, and media relations.
- We will establish contingency plans for all anticipated off-nominal events and share them openly with all appropriate authorities.

RESPECT

- We will respect the rights of other users of the airspace.
- We will respect the privacy of individuals.
- We will respect the concerns of the public as they relate to unmanned aircraft operations.
- We will support improving public awareness and education on the operation of UAS.

As an industry, it is incumbent upon us to hold ourselves and each other to a high professional and ethical standard. As with any revolutionary technology, there will be mishaps and abuses; however, in order to operate safely and gain public acceptance and trust, we should all act in accordance with these guiding themes and do so in an open and transparent manner. We hope the entire UAS industry will join AUVSI in adopting this industry Code of Conduct.

Ms. CLARKE. Is there a particular downside for the manufacturers in not providing a much more robust code of conduct?

Ms. STEPANOVICH. Many privacy experts, including Ryan Calo, a former professor at Stanford and an expert in privacy and robotics, has said that people in the United States will be very hesitant to accept the adoption of this technology if privacy safeguards are not put into place prior to the adoption of it. So we believe that if we don't address this now, that there will actually be a visceral reaction from the American public and that we will not be able to comply with the spirit of the FAA act which requires that drones be allowed into the United States National airspace.

Ms. CLARKE. So from a commercial use standpoint or even a local law enforcement standpoint, is it within the best interest of manufacturers to strengthen their code of conduct?

Ms. STEPANOVICH. We believe it is not only in the best interest for them to strengthen the code of conduct, it is also in their best interest to support large-scale legislation and regulations related to privacy.

Ms. CLARKE. Thank you very much, Mr. Chairman, and I yield back.

Mr. MCCAUL. I thank the gentlelady.

The Chairman now recognizes Mr. Billy Long from Missouri.

Mr. LONG. Thank you, Mr. Chairman.

Any of you can answer. Can you define a drone for me? Is there a certain size or certain altitude that it flies at? What constitutes what we are trying to deal with?

Mr. DILLINGHAM. I guess I will try and start. It varies, sir. It varies from hand-held model airplane types to the ones that we are most familiar with in terms of the Predators and the Global Hawks that are used mostly in the war theater.

What we are talking about here for the most part are what is called the small UAVs, which is what FAA is trying to develop a rule for, and that is I think less than 55 pounds and relatively small in size.

Mr. LONG. A flying trash can, are you familiar with that?

Mr. DILLINGHAM. I have heard that phrase before. It could be the size of a flying trash can, or it could be the size of a hummingbird.

Mr. LONG. I thought you said 55 pounds?

Mr. DILLINGHAM. Right. But I am saying it varies in size, the small UAV rule that is being worked refers to that size, 55 and down.

Mr. LONG. Okay. I know that the flying trash cans, originally when they were developed, I think part of their thought process was to use them for police work. If you are in a neighborhood and you are chasing a suspect through several buildings or whatever where they can fly that over at a fairly low altitude. But I just had a question on that.

To answer Mr. Duncan's question, or part of it, maybe not answer it but I think that the Transportation and Infrastructure Committee has tried to tackle the problem of getting in general airspace, general aviation, and also FAA airspace. So I think that that is a separate issue that hopefully we are trying to handle on that angle.

Generally, to the sheriff, it has always been my understanding that anything that can be seen by anyone driving down the street, flying a helicopter I guess I would say, but if you are driving down

the street and a guy is sitting on his lawn smoking marijuana, then you have a right to arrest that man, correct?

Chief MCDANIEL. That is correct, sir. Yes.

Mr. LONG. If he is in his backyard and he has a privacy fence, you are not allowed to go put a ladder up and look over the fence, are you, because that is not available to people?

Chief MCDANIEL. The norm is to be able to view it from what the public can see.

Mr. LONG. Okay. That is kind of where I was going—that was my hillbilly way of getting there, I guess.

At 30,000 feet or whatever, we always think of the Predator drones that are armed of course that have been successful in a lot of military operations, but my constituents and I think a lot of constituents across the country are concerned with that type of surveillance, albeit they are not armed. You can't see them. You can't hear them, but that is a whole different level, isn't it, than what we were talking about a second ago, being able to see what you can normally see?

Chief MCDANIEL. Certainly the utilization of a UAV up over an area would open it up to view for law enforcement or any other governmental entity.

Mr. LONG. These small ones that we are talking about here today, the 55 pounds and below, the flying trash cans, I have seen those. I think that they would be fairly apparent to people. I have not seen one operate. I have seen them on the shelf where they develop them, but as far as the sounds that they put out and things like that, most of those, are people going to be able to acknowledge there is something flying up over their farm or their house, looking to see if you are shooting doves?

Chief MCDANIEL. Yes, sir. That is an excellent point. The UAVs that public safety agencies, law enforcement, and fire departments are using or looking to utilize are not the Global Hawk or the Predator at $20 million or $30 million a copy. These are very small in stature. The maximum time aloft on our Shadow Hawk is 2 hours and 20 minutes.

Mr. LONG. At what altitude?

Chief MCDANIEL. At no more than 400 feet above ground level.

Mr. LONG. So privacy concerns would be a little bit alleviated I would assume with that type?

Chief MCDANIEL. Absolutely. At that altitude and the type of engine that it has, it sounds like a very powerful weed eater, and you will be able to notice that it is above.

Mr. LONG. Maybe you could make a weed eater out of one of them. That would be kind of handy.

Mr. Chairman, the Department of Homeland Security will not testify before this subcommittee, the Department of Homeland Security; is that correct?

Mr. MCCAUL. That is correct.

Mr. LONG. I rest my case.

Mr. MCCAUL. Thanks for the point well taken, and I will close on that as well.

The Chairman now recognizes for the third time in this hearing Mr. Cuellar from Texas.

Mr. CUELLAR. Thank you very much. It is refreshing to hear my good Republican friends talk about civil liberties. Thank you, I appreciate that. But one more thing on the EPA story by Fox, Fox actually took that back. It was not a UAV, it was actually aircraft that they have been flying for the last 10 years under both Democratic and Republican Presidents, just to make that sort of correction.

Let me say this. I have a border sheriff who happens to be my brother. I have got three peace officers, and I believe that if there is going to be evidence collection techniques, I would assume that your jurisdiction or as a sheriff, you have certain procedures as law enforcement to follow that; is that correct?

Chief MCDANIEL. That is correct, sir.

Mr. CUELLAR. If someone violates that, I would assume that they would be liable for not following that; is that correct?

Chief MCDANIEL. Yes, sir.

Mr. CUELLAR. Okay. Having three peace officers in my family, I put a lot of trust in law enforcement on that. Even though there are some bad apples, you still have to follow the Constitution; is that correct?

Chief MCDANIEL. Absolutely.

Mr. CUELLAR. Talking about the Constitution, there is the Fourth Amendment of the U.S. Constitution that prohibits unreasonable searches and seizures and requires search warrants to be based on probable cause, and the Supreme Court has already interpreted different cases. For example, talking about aircraft—and keep in mind that the Supreme Court has already talked about using cameras on aircraft. This time it is a different platform. It happens to be UAVs. For example, just to make sure we all understand, the Supreme Court has said that there is an expectation of privacy. When it is inside the house, it is a different type of privacy. Once you go outside the house, there is a different type of privacy. A business has less expectation of privacy than inside the home, and the Supreme Court has talked about the open field doctrine, and I believe you understand what I am talking about here. You are familiar with the *Dow Chemical Company* v. *The United States.* I am sure you are also familiar with the open fields doctrine of *California* v. *Serrano* case. The Supreme Court held that the police did not have to obtain a search warrant when observing a person's backyard or curtilage from an airplane more than 1,000 feet above the air; is that correct? That is what the Supreme Court held.

Also, the court also defined aerial searches in *Florida* v. *Riley* that said, and Chief, you mentioned the 400 feet, I think we mentioned the 400 feet, that held that police officers do not need a search warrant when they are flying a helicopter above 400 feet. So in this case a different type of platform, but if you are flying above 400 feet, no search warrant. But if you are flying below 400 feet, and I believe most of the law enforcement and most of those UAVs will be at 400 feet or below. So, therefore, if you are flying at 400 feet in altitude, then at that time you would need a search warrant, whether you use a helicopter or UAV, probably not an airplane. So the Supreme Court has already laid out the law on what it is.

Now, I do agree with my colleagues here that we probably need to look at some legislation but as we draft the legislation, we got to keep in mind that the Supreme Court has already defined open doctrine, home business, and certain expectations; is that correct?

Chief MCDANIEL. Yes, sir, that is absolutely correct. As far as case law is, in my view and from those I have talked with, there is no difference between establishing a separate type of case law for UAVs. The manned aircraft component is nothing more than an aircraft with people in it compared to a UAV that has them on the ground. The case law is the same because they are both aircraft, air assets.

Mr. CUELLAR. In the *Dow Chemical Company* v. *The United States,* it involved airborne use of thermal imaging. So here is another case where technology is being used. Again, I am one of those that is fascinated by the UAVs; but at the same time I do understand there are concerns. The doctor that just testified, I looked at his recommendations and they are very, very good recommendations, and I think we need to look at those recommendations. But all I am saying, Members, there is already some case law on this. The Supreme Court has ruled on this. If we do any legislation, I just say let's look at the legislation of the Supreme Court. Let's use some common sense in applying some of this, and put a little trust in our law enforcement, which I appreciate, and having three brothers and having one who is a border sheriff, I appreciate the work that you all do.

Thank you very much, Mr. Chairman.

Mr. MCCAUL. I thank the gentleman.

In closing, let me thank the witnesses for being here. As a former Federal prosecutor, I understand—is there somebody I missed? Oh, my goodness, Mr. Davis from Illinois, I sincerely apologize.

Mr. DAVIS. I really don't have a lot to ask, but let me ask, Dr. Dillingham, you mentioned in your testimony something about using the instruments to jam signals and that that could become a problem and the use. Would you mention that a little bit more?

Mr. DILLINGHAM. Yes, sir. One of the emerging issues that we have identified is the potential that the signals that control these UAVs in flight, and we are again talking about the small ones as opposed to the encrypted DOD-type, could in fact be jammed and break command-and-control links with the UAV, meaning that the UAV could go off-course, not necessarily—or could include being taken control over, but clearly breaking that command-and-control link with the appropriate persons or organizations that were controlling it. It is something that needs to be addressed now before we have these potentially serious kinds of incidents.

Mr. DAVIS. Thank you very much. Let me ask you, Chief McDaniel, the data that is collected, could you describe what kind of data it is? What is it used for and how long is it kept? Would the individuals have any idea that this data may be collected that involves them?

Chief MCDANIEL. The only data that we are collecting off of our Shadow Hawk is color video. We can convert that to both still photographs or video. Depending upon the situation, we would obviously store that video for criminal purposes; i.e., if our SWAT team is going in on an individual or it is a high-risk warrant, we would

also have that video or those photographs preserved as evidence. It does have a FLIR system, a forward looking infrared camera system, that can identify heat sources in low-light conditions. However, the idea behind that was more for searching for lost persons in our National forests to more readily be able to identify them.

Mr. DAVIS. Let's say you got a tip that a farmer was using some of his or her acreage and they had a little plot of marijuana growing and you wanted to check that out with one of these vehicles. Would there be a way to do that without acquiring a search warrant, or would you be within—and I am going to ask you, Ms. Stepanovich, when he finishes, how would you handle a situation like that?

Chief MCDANIEL. Well, as indicated earlier, the Supreme Court in 1924 established the open fields doctrine which allows for things to be observed that the majority of the public could see. In responding to the example that you present, the reality is, and this is based upon law enforcement, investigation techniques, et cetera, utilizing this drone to try to observe a marijuana field would not be appropriate. It would not be a good investigative tool, A, because of the constraints that the FAA puts on the use of UAVs by law enforcement agencies, flying no higher than 400 feet AGL, and because of the noise and the size of it.

So if we are trying to investigate whether there is a marijuana field to continue with our investigation and to ultimately arrest suspects, the UAV is not it.

Mr. DAVIS. Ms. Stepanovich, are you comfortable that enough attention is being given to the individual rights and civil liberties of citizens given the use of this type of surveillance?

Ms. STEPANOVICH. I am not sure if "comfortable" would be the right term. We do respect the fact that law enforcement at this time does not expect to use drones for broad and untargeted access. We respect the Supreme Court precedent that Representative Cuellar had referred to that allows for aerial surveillance in "open fields."

However, recently the Supreme Court did investigate a case of in *U.S.* v. *Jones* of police using GPS without a warrant to track a suspect. Drones allow for the same type of pervasive and very intensive surveillance that GPS allows for. In that case Justice Alito wrote a very eloquent dissent saying, and I quote: "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative." We agree with Justice Alito in that case, and we believe that drones represent a similar jump in technology from normal tracking of an individual with a policeman in a police car, as drones respect to aerial tracking in a helicopter or airplane.

Mr. DAVIS. Thank you very much.

Thank you, Mr. Chairman, for a very interesting hearing, and I yield back.

Mr. MCCAUL. Thank you, Mr. Davis. I apologize again for my oversight. Speaking of oversight, this has been a real productive hearing and very insightful.

Let me just close by saying as a former Federal prosecutor, I recognize the value of—legitimate law enforcement value of technology. I think as with technology, we have to balance privacy and

security. Obviously, the Fourth Amendment applies here. The case law, as Mr. Cuellar has set forth, is there. I have studied it in my prior career. But this is an evolving field. We have thousands of these things that could be deployed in the skies now. Over the next couple of years, we may see more than a couple of thousand, maybe 10,000 of these things. I think it is incumbent upon the Department of Homeland Security to come up with a policy, to come up with a security analysis.

I think the one thing that we can all agree on, interestingly on both sides of the aisle on this committee, both Republicans and Democrats, and I think all three of these witnesses agree on one thing, and that is that DHS has a role. I think Mr. Dillingham and GAO stated it 4 years ago. Chief McDaniel, you stated it in your testimony here today. I think local law enforcement does need that guidance. I think, Ms. Stepanovich, you as a privacy expert, the Office of Privacy within DHS should be involved in this issue.

So I hope that we can all walk away from here with that common goal and understanding, and I sure hope that this wakes up the Department, that they need to step up to the plate and do something.

With that, I want to thank the witnesses. This has been a very insightful, productive hearing, and I thank the Members also for their questions. Thanks so much, and this hearing now is adjourned.

[Whereupon, at 11:30 a.m., the subcommittee was adjourned.]

○