AIRBORNE LAW ENFORCEMENT ASSOCIATION

Small Unmanned Aircraft Systems

Resource Guide

AIRBORNE LAW ENFORCEMENT ASSOCIATION

50 Carroll Creek Way | Suite 260 | Frederick, MD 21701
Office: (301) 631-2406 | Fax: (301) 631-2466
www.alea.org

July 2014

The Airborne Law Enforcement Association (ALEA) has embraced the use of small Unmanned Aircraft Systems (sUAS) as a force multiplier for public safety agencies. ALEA believes that sUAS can enhance the safety of public safety personnel and citizens, provide an economical option to traditional aircraft for agencies, enhance the situational awareness of ground personnel, assist in Search and Rescue (SAR) missions and be used for crime scene and crash scene imaging. In addition, sUAS can also be utilized on many governmental missions that are performed by traditional aircraft. This includes aerial mapping, airborne environmental sampling, zoning or code enforcement, environmental resource management and land management, to name a few.

To this extent, the ALEA has compiled the attached Small Unmanned Aircraft Resource Guide for its members. The Resource Guide contains information that is valuable to an agency that is considering implementing a sUAS program. The Resource Guide can be utilized as a "roadmap" to guide the agency through the research, aircraft selection, COA application, policy development, training and evaluation and finally, the operational use of a sUAS.

The ALEA remains committed to providing its members with the most up-to-date information and training regarding the use of sUAS by public safety entities.

Table of Contents

Section 1……………………………………………………….AUVSI Benefits of Unmanned Systems in Law Enforcement

Section2………………………………………………………………………………………………….AUVSI UAS in Public Safety

Section 3……………………………………….Various Articles from "AirBeat" Magazine on sUAS in Law Enforcement

Section 4……………."Police Chief" Magazine Article "UAS: All the Boxes Checked, but Challenges Remain

Section 5……………………………………………Article "The Truth about Remotely Piloted Vehicles and Privacy"

Section 6……………………………………………………FAA/DOJ Memorandum of Understanding Concerning UAS

Section 7……………………………………………………………..FAA Unmanned Aircraft Systems Integration Roadmap

Section 8…………………………………………….IACP Recommended Guidelines for the Use of Unmanned Aircraft

Section 9……………………………………………………………ACLU Report "Protecting Privacy from Aerial Surveillance"

Section 10………………….Commonwealth of VA Report "Protocols for the Use of UAS by Law Enforcement"

Section 11…US Department of Homeland Security "Privacy Impact Assessment for the Aircraft Systems"

Section 12……………………………….FAA Document "Public UAS Operations in the National Airspace System"

Section 1

AUVSI
ASSOCIATION FOR UNMANNED VEHICLE SYSTEMS INTERNATIONAL

2700 South Quincy Street, Suite 400 • Arlington, VA 22206 • 703.845.9671 • 703.845.9679 fax

Benefits of Unmanned Systems in Law Enforcement

The public safety professionals working for America's 18,000 domestic law enforcement agencies are committed to keeping our communities safe. The unmanned systems industry is committed to giving them the tools, including unmanned ground, maritime and aircraft systems to do their jobs as safely as possible, while helping them save time, save money and even save lives.

Keeping Public Saftey Officers Safe. Public Safety officers do their jobs in incredibly dangerous environments. Unmanned systems can minimize the risks they face, while helping them to act faster and with the best information available. Unmanned systems are designed to do dangerous and difficult tasks while keeping the user out of harm's way.

- In inclement weather, an unmanned aircraft system (UAS) could provide aerial support when a helicopter could not.
- An UAS could be used to document a traffic accident on a busy highway, reducing the amount of time law enforcement officers spend roadside in close proximity to moving traffic.
- UAS can support tactical operations, offering crucial situational awareness in dangerous or difficult situations.
- The Massachusetts State Police bomb squad at Logan International Airport have used unmanned ground systems to safely screen for explosives.
- In a September 2012 SWAT operation in Bellevue, Neb., a suspect shot an unmanned ground robot with four rounds from a 12-gauge shotgun. The unmanned system was able to provide officers with the suspect's position and disposition, while keeping them out of harm's way.
- Tactical teams in Alameda County Sheriff's Office in Northern California and the Des Plaines, Ill., Police Department are just two of the more than 125 U.S. law enforcement agencies that have adopted using unmanned ground robots in SWAT operations to reduce the risk to officers and the public.

"[Unmanned Systems] are a tool that every law enforcement agency would like to have. Whether it's a lost child, a lost Alzheimer's patient, a shooter from a window, law enforcement needs to have the tools to get the job done." Eric Holdeman, Emergency Management Expert

Aiding search and rescue. Unmanned systems have the potential to survey large areas for a missing child, acres of land consumed by wild fires or vast expanses of water where a boat might be adrift. Bad weather and difficult terrain can prolong search and rescue efforts, lowering chances for survival while raising the financial cost.

Responding to emergencies. Unmanned systems provide public safety officers a tool to safely respond to natural disasters and other emergencies.

- In May 2012, the Mesa County (Colo.) Sheriff's office flew its UAS over a church that had caught fire. Images captured by a thermal camera attached to the UAS provided responders with information about remaining "hot spots", so firefighters could efficiently concentrate their efforts. Photographs taken of the fire also assisted arson investigators determine the direction the fire had traveled through the building.
- The Grand Forks Sheriff's Department used a UAS to gather real-time images of flooding along the Red River in eastern North Dakota.
- Several law enforcement agencies have expressed interest in using UAS to respond to dangerous spills, such as when a tipped-over truck or derailed train spills hazardous material.

- A tornado or severe storm can knock down power lines, making impacted areas harder to access. A UAS could safely fly over such an area, search for survivors and assess conditions without subjecting officers to danger.
- Unmanned maritime systems have enhanced the U.S. Navy's mine-hunting capability by detecting and identifying floating and sea-floor mines.
- The New York Police Department employs four unmanned underwater vehicle for port security.
- Boston PD used dozens of robots throughout the four-and-a-half day span after the Boston Marathon bombing to help investigate suspicious activity in the area and to clear the scene in Watertown where the last suspect was captured.

"These devices can save the lives of first responders and also citizens of Alameda County... In this time of austerity, we are always looking for sensible and cost-effective methods to improve public safety." Capt. Tom Madigan, Alameda County Sheriff's Department

Saving the Government and Taxpayers Money. Each year, our nation's state and local governments spend millions of dollars on search and rescue, disaster preparedness, law enforcement, fire prevention and other critical services. Unmanned systems allow those agencies to accomplish those same tasks more efficiently, saving time, taxpayer dollars and lives in the process.

- Operating manned helicopters can cost between $200 and $400 per hour, while operating a UAS can cost as little as $25 to $75 per hour.
- The purchase price of a UAS is also significantly less than a manned aircraft. A small UAS can cost less than $50,000, which is about the price of a patrol car with standard gear.
- Mesa County, Colo., spends nearly $10,000 on a manned aerial survey of a landfill to determine the increase in waste over the previous year. The Mesa County Sheriff's Office was able to complete the same survey with an unmanned aircraft for a mere $200.

Section 2

UAS IN PUBLIC SAFETY

AUVSI
ASSOCIATION FOR UNMANNED VEHICLE SYSTEMS INTERNATIONAL

The unmanned systems industry is committed to providing America's public safety professionals with tools to do their jobs as safely as possible, while helping them save time, save money and even save lives.

2009

A UAS was used to stem a massive wildfire spreading across Alaska, taking infrared images of the fire at night to identify hotspots in the darkness and providing firefighters situational awareness

125+

U.S. law enforcement agencies have adopted using unmanned ground robots to reduce the risk to officers and the public

88%

of the public support UAS use in search-and-rescue operations

The average cost of a small UAS is comparable to the price of a patrol car with standard police gear.

UNMANNED SYSTEMS CAN HELP ...

- SURVEY LARGE AREAS FOR MISSING PERSONS
- IDENTIFY WILDFIRE HOTSPOTS
- PROVIDE AERIAL SUPPORT IN INCLEMENT WEATHER
- SUPPORT TACTICAL AND DANGEROUS OPERATIONS
- ENABLE POST-DISASTER ASSESSMENT
- RESPOND TO DANGEROUS SPILLS OF HAZARDOUS MATERIALS

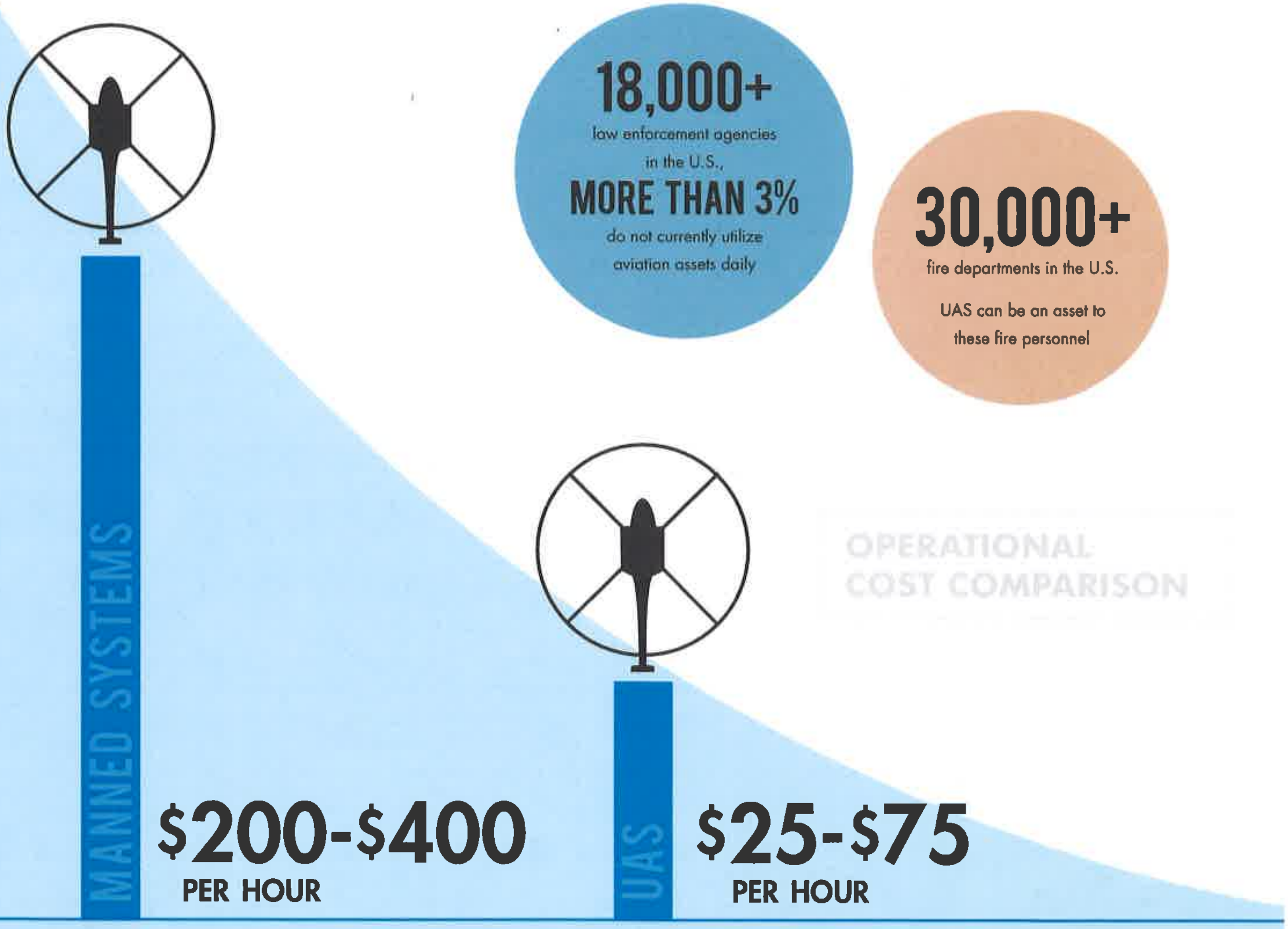
UAS: SAFE AND EFFICIENT

The Mesa County Sheriff's Office spent nearly $10,000 on a manned aerial survey of a landfill to determine the increase in waste. The same survey was completed for a mere $200 with an unmanned aircraft.

18,000+
law enforcement agencies in the U.S.,
MORE THAN 3%
do not currently utilize aviation assets daily

30,000+
fire departments in the U.S.
UAS can be an asset to these fire personnel

OPERATIONAL COST COMPARISON



Each year, U.S. state and local governments spend millions on search and rescue, disaster preparedness, law enforcement, fire prevention and other critical services. Unmanned systems could help accomplish those tasks more efficiently, saving time, money and lives.

FOR MORE INFORMATION,
VISIT WWW.INCREASINGHUMANPOTENTIAL.ORG

Section 3

Draganfly X4-ES sUAS First Look:

Agency Tests Draganfly for Varied Public Safety Missions

By Alan Frazier, *Deputy Sheriff, Grand Forks (ND) County Sheriff's Office, Assistant Professor, University of North Dakota's John D. Odegard School of Aerospace Sciences*

Photos courtesy of Mesa County (CO) Sheriff's Office, Shawna Widdel, *UND Aerospace* **and Bob Cary,** *UND Aerospace*

No, "Draganfly" is not a misspelling. The small unmanned aircraft system (sUAS) is named for Zenon Dragan, founder and owner of Draganfly Innovations based in Saskatoon, Canada.

Founded in 1998 as a hobby remote-controlled helicopter company, Draganfly has grown to be one of the leading manufacturers of sUAS for public safety agencies. The company has manufactured more than 8,000 small helicopters. Currently, 15 public safety agencies in five countries deploy Draganfly sUAS. A Draganfly X4-ES sUAS operated by Royal Canadian Mounted Police is credited with the first "save" by an sUAS, when the Mounties used a FLIR TAU-640 infrared camera payload on the aircraft to locate an injured and disoriented man who had walked away from a roll-over traffic collision in below freezing temperatures near St. Denis, Saskatchewan.

The Grand Forks County Sheriff's Department (GFSD), collaborating with the University of North Dakota's (UND) Law Enforcement Unmanned Aircraft Systems Research Project, began utilizing a Draganfly X6 sUAS in February 2010. In May 2013, GFSD took delivery of a Draganfly X4-ES sUAS. Also in May 2013, the UND was designated as a factory-training center for Draganfly sUAS flight training.

UND pilots have logged more than 70 hours of flight time with the X6 and X4-ES. During that time, the Draganfly airframes have proven to be stable and easy to fly.

Exploring the X4-ES

The X4-ES is a 5.7-pound quad-rotor sUAS with four brushless electric motors powered by a lithium-polymer battery that allows average flight times of 20 minutes. Its 11 separate sensors contribute to its stability and controllability. The X4-ES is a "pilot's aircraft" in that it requires direct pilot control for some operations (principally landing), yet it has the ability to remain stationary through the use of a hold function enabled by its GPS reception capability.

The X4-ES is controlled via Draganfly's proprietary multi-function ergonomic hand controller/ground control station. The hand controller places both flight and payload controls in logical and easy to manipulate locations. Control use is intuitive and straightforward. A left mounted joystick controls throttle and yaw while a right mounted joystick controls pitch and roll. Top mounted buttons control motor engagement and disengagement, as well as the camera shutter. Two rear-mounted buttons control camera zoom. The center area of the hand controller is occupied by a large LCD screen, which provides aircraft telemetry information and a live video from the aircraft's camera. The screen is bright and viewable during

The Draganfly X4-ES in Brief

List Price:	$25,000
Price as tested:	$25,000 (including Sony DSC-RX100 digital camera)
Range:	1 km
Endurance:	20 minutes
Length:	36.25 inches
Weight:	5.7 pounds (with Sony Camera Payload)
Payload:	Sony RX-100, Sony NEX5R Low Light, FLIR TAU 640 thermal imaging

sunny conditions. The entire system is transported in a 19 x 24 x 10-inch polycarbonate case that complies with airline checked baggage requirements.

The X4-ES has been flown in over 25-knot winds by factory personnel. GFSD-UND pilots have flown the sUAS successfully in 15-knot winds. GFSD-UND flight policies and procedures dictate the use of a pilot and separate sensor system operator. To accomplish this, sensor system operators utilize the handheld ground control station while the pilot flies the aircraft with a less sophisticated hand held controller that does not offer a live video feed. GFSD-UND personnel have not found this to impede operations but provided an added safety bonus as the pilot is not distracted by the video. The sensor system operator, who also serves as a visual observer, operates the camera. Crew resource management is critical, as the pilot and sensor system operator must communicate succinctly and clearly to accomplish.

The X4-ES uses a gimbaled, gyro-stabilized payload mount capable of carrying a variety of payloads, including a combination still/video camera, a low-light camera or an infrared camera. High definition video and still photos are captured on an SD card within the camera. Standard definition photos are stored in the memory of a global cache service, which creates folders for each flight and stores associated data and standard definition photos. This has proven to be the best sorting and data storage protocol GFSD-UND personnel have experienced with the four different sUAS they fly. The system saves many man-hours when it is time to remove and either delete or store data files.

Comparisons With the X6

Both the Draganfly X6 and X4-ES have been utilized dozens of times by public safety agencies in missions as varied as searching for victims to identifying hot spots at structure fire scenes. In September 2011, the Mesa County (CO) Sheriff's Office used an X6 with a FLIR Tau 640 infrared camera to identify hot spots and locate the point-of-origin of an arson fire that destroyed a historic hall in Grand Junction, CO. Two years later, in September 2013, Mesa County used the X6 to locate the body of a victim who fell 450 feet to her death from a scenic overview point. Images taken from the aircraft allowed the recovery team to formulate a safe plan for recovery of the body. In June 2013, GFSD utilized an X6 to aid in a search for a drowning victim in a large flooded area that was largely inaccessible to ground teams due to mud and debris. Although the victim was not located at the time, the aircraft saved many man-hours searching a difficult and dangerous area.

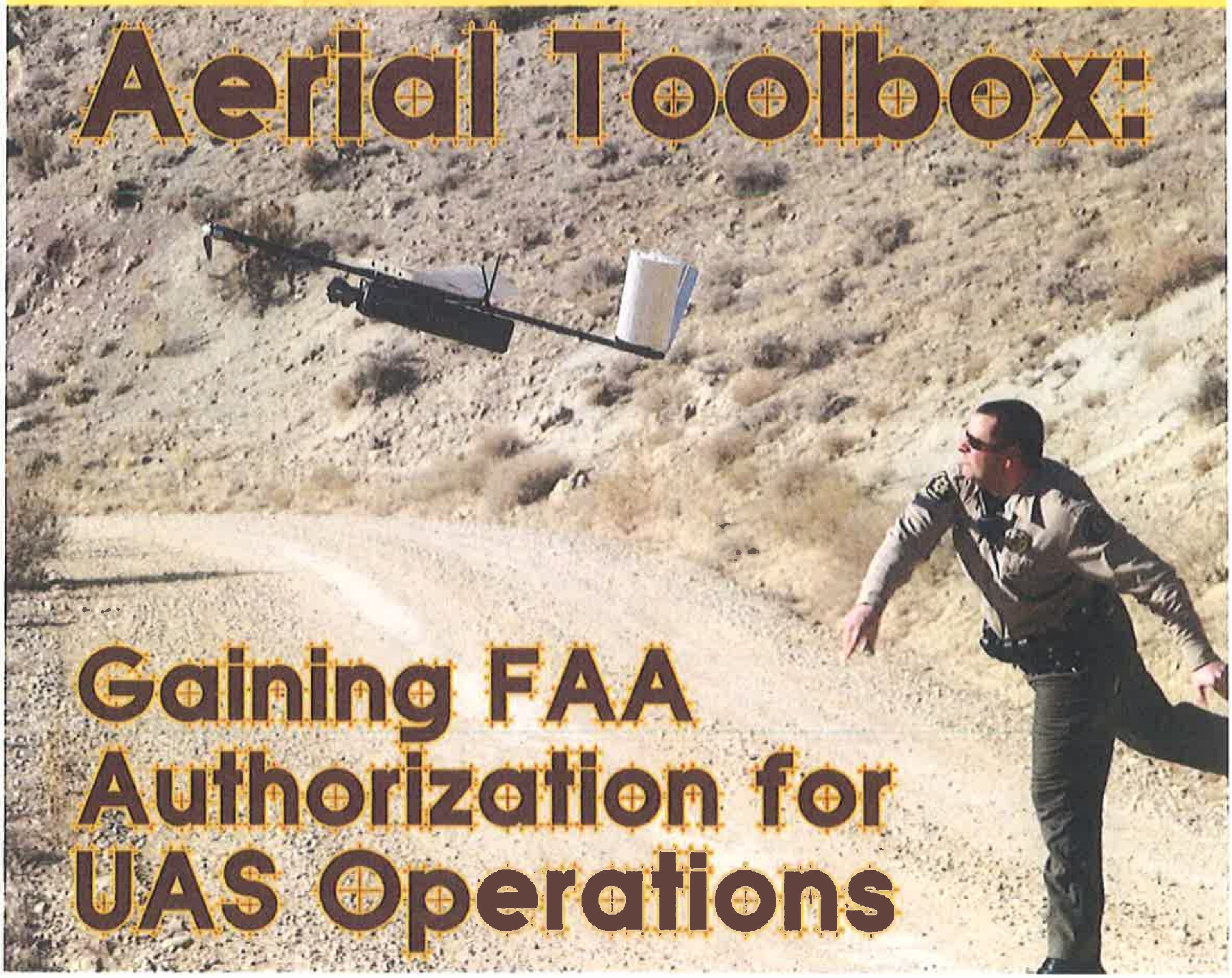
In comparing the X6 and X4-ES, UND-GFSD pilots prefer the X4-ES's handling and performance in high winds, as well as its increased battery capacity (an additional 8-10 minutes of flight time). While flight time is directly proportional to wind velocity (higher winds require more electricity to produce more thrust), UND-GFSD pilots have routinely achieved flight times of 18-24 minutes with the larger battery. Another significant improvement in X4-ES is the ability to program the lost link protocol to return the aircraft to "home" (the takeoff location). Previous Draganfly aircraft initiated a landing at the lost link location, which could be problematic if the aircraft was over difficult to access terrain or water.

The X6 and X4-ES payloads offer both strengths and weaknesses. The available off-the-shelf cameras are well designed, robust and affordable, and all of them offer good resolution photos and video. The cameras are complimented by Draganfly's gyro-stabilized mount, which keeps them level regardless of aircraft attitude. However, only one payload can be carried at a time. If an operator wishes to switch from a visual to infrared camera, the aircraft must land first. Although a payload swap can be done within minutes, the lack of ability to instantly switch from visual to infrared imagery is a limitation.

Training to fly the Draganfly airframes consisted of traditional ground and flight instruction conducted by Draganfly Factory Personnel. The two-day course was comprehensive and focused on hands-on activities. Draganfly is a relatively small company currently employing 17 personnel. This size yields high levels of customer service, and UND-GFSD personnel have indicated factory support has been outstanding.

Both the Draganfly X6 and X4-ES have been utilized dozens of times by public safety agencies in missions as varied as searching for victims to identifying hot spots at structure fire scenes.

Aerial Toolbox: Gaining FAA Authorization for UAS Operations



By Alan S. Frazier, *Assistant Professor, University of North Dakota John D. Odegard School of Aerospace Sciences*

The aviation community is full of acronyms: FAA, IFR, VFR, ILS, ATC—the list goes on and on. The unmanned aircraft portion of the aviation community is also well-stocked with acronyms—UAS (unmanned aircraft system), UAV (unmanned aerial vehicle), RPV (remotely piloted vehicle).

If you are considering establishing an unmanned aircraft systems unit, one very important acronym you should be familiar with is "COA." Certificates of authorization or waiver are multi-page documents that provide your organization with Federal Aviation Administration authorization to fly unmanned aircraft within the National Airspace System.

COAs were initially introduced to provide a process that would allow airshow performers to receive a waiver of certain federal aviation regulations during their performances in the vicinity of large crowds. With the advent of public agency use of UAS, the FAA employed the process as a method for granting the aircraft, which lacked airworthiness certificates and had limited "see and avoid" capability, access to the National Airspace.

Several years ago, the COA process could be summed up in one word: obstructionist. However, it has improved significantly and is now much more user friendly and efficient. This is partly because of UAS-related clauses within the *FAA Modernization and Reform Act of 2012,* which became law on Feb. 2, and partly because of the efforts of two individuals assigned to FAA's Unmanned Aircraft Program Office, Steve Pansky and Dave Morton, who have been integral in implementing the intent of the legislation.

Starting the Process

The COA process should begin with the requesting agency conducting a significant amount of research. Most of this research can be performed via the internet. However, attendance at UAS seminars presented at venues such as the recent Airborne Law Enforcement Association Annual Conference and the Association of Unmanned Aircraft Systems International annual expositions can be informative. Attendance at UAS-related seminars during the 2012 ALEA Annual Conference quadrupled in comparison to similar seminars at the 2011 conference.

Research and preparation should include gathering the following:

- The proponent's contact information, including the name of the agency chief executive (usually the police chief or sheriff).
- The model and manufacturer of the selected UAS.
- A concept of operations (what you plan to do with the UAS).
- Level of aviation experience of the involved personnel.
- Whether the program is being developed in-house or utilizing a consultant.
- Obtaining a letter from your state's attorney general verifying your agency's host government is a "political subdivision" of the state in which the UAS will be operated. The letter should state the host government is a political subdivision of the state as specified within Title 49 USC Section 40102 and that the UAS will only be operated for non-commercial purposes pursuant to Title 49 USC Section 40125. If you work for a county or city, you may think that it is self-evident that your organization is a political subdivision. However, the FAA is adamant about the requirement to submit the letter.

Once the initial research has been completed, the agency should contact the FAA to apply for an online COA application account. Currently, the appropriate FAA contact is Steve Pansky. In your initial email to Pansky, provide the information listed above and attach the political subdivision letter. Upon review of your account request email, Pansky will either provide you with account access or work with you to fine tune your plan to meet account access requirements.

The online COA application link is intuitive and well-designed. Information that must be provided includes:

- Types of missions to be flown.
- Launch, operations and recovery locations.
- Altitudes to be utilized.
- Flight procedures.
- Communication procedures.
- Lost communications and lost-link procedures.
- Pilot-in-command/visual observer minimum qualifications.

Many of the questions provide a free-form text box in which the applicant has an unlimited text field available to write an answer. In addition, many of the queries have attachment links which allow the applicant to upload documents. This can be especially useful when answering questions regarding equipment specifications. The attachment links will accept a variety of documents, including Microsoft Word, Excel and PDFs.

"After an agency completes initial and law enforcement mission-oriented training and feels competent to perform actual law enforcement missions, the FAA will schedule an operational demonstration and records review."

The radio frequency segment of the application may require additional documentation. If the selected UAS does not communicate within the portion of the radio spectrum assigned to remote control aircraft, the applicant must provide documentation of Federal Communications Commission approval to utilize the command and control and data transmission frequencies used by the selected UAS.

The FAA strives for a 60-day turnaround on COA applications. However, many require 90-120 days. The current FAA model for COA issuance results in the initial authorization to operate for the purpose of training. After the agency completes initial and law enforcement mission-oriented training and feels competent to perform actual law enforcement missions, the FAA will schedule an operational demonstration and records review. This phase will require the agency to successfully complete a simulated law enforcement UAS mission while being observed by FAA personnel.

The FAA will also review the agency's policies and procedures related to UAS operations. Upon successful completion of this demonstration and review, the FAA will issue an operational COA. These operational COAs will generally include the entire jurisdictional area of the applicant agency. The agency will then be able to deploy its UAS during daytime VFR conditions at and below 400 feet AGL with as little as one hour notification to FAA. The one-hour notification time is a significant improvement over the former minimum 48-hour notice requirement. In reality, if the agency makes the notification as soon as it believes it may need to deploy a UAS, response time, pre-flight and launch times will quickly use that hour.

Be aware that the FAA has its own vocabulary. The administration refers to the "applicant" as the COA "proponent." When you are ready to forward your online application to the FAA, you probably will consider that "submitting" the application. The FAA calls that step "committing."

Finally, when conducting UAS operations, a copy of the COA must be on-site. It is essential that all operators are fully aware of and comply with all COA conditions.

Alan Frazier is an assistant professor within the University of North Dakota's John D. Odegard School of Aerospace Sciences. He teaches aviation management and pilot training courses, including "Public Safety Aviation." Alan is an ALEA member and the former officer-in-charge of the Glendale (CA) Police Air Support Unit. Questions or comments may be directed to him at afrazier@aero.und.edu.

COAs Online

The following links will be helpful when working on your UAS certificate of authorization:

- FAA's Interim Guidance Document 08-01 will provide valuable information on UAS COAs. It is available online at **www.faa.gov/about/initiatives/uas/.**
- Steve Pansky, the appropriate FAA contact for UAS COAs, can be reached at **steven.ctr.pansky@faa.gov.**

Grand Forks Gets First Look at AeroVironment Qube

By Alan Frazier, *Deputy Sheriff, Grand Forks (ND) County Sheriff's Office, Assistant Professor, University of North Dakota's John D. Odegard School of Aerospace Sciences*

The Grand Forks County (ND) Sheriff's Department (GFSD) was selected in July 2012 as one of five evaluation sites for the Qube, AeroVironment's newest small unmanned aircraft system (sUAS).

While AeroVironment maintains a low-key corporate profile, it is a significant player in the sUAS industry. Founded in 1971 by innovator Dr. Paul MacCready, the company has grown to be the world's largest manufacturer of sUAS, with FY2012 revenues of $325 million. Based in Monrovia, CA, AeroVironment has more than 700 employees, most of whom are dedicated to designing and manufacturing sUAS like the Raven, Wasp and Puma.

GFSD collaborates with the University of North Dakota's (UND's) Law Enforcement Unmanned Aircraft Systems Research Project in the administration of a UAS Unit serving public safety agencies in 16 eastern North Dakota counties. Pilots are provided by the university, and sensor system operators/visual observers are provided by area law enforcement agencies. The unit currently operates three sUAS: the AeroVironment Qube and Raven-B DDL and the Draganfly Innovations X6.

In May 2013, the first production model of the Qube was delivered to GFSD, factory OEM training for pilots and visual observers was conducted, and the Qube flew its first mission.

Taking Off in the Qube

When GFSD-UND pilots began working with Gabriel Torres, AeroVironment's Qube program manager, over several months of Qube development, some were skeptical of its advertised capabilities. Now, since unit members have received Qube OEM training and deployed the sUAS on an actual mission, it's clear the Qube does everything promised and more.

The 5.5-pound quad rotor helicopter is stable and predictable. Aircraft control is

sUAS

Photos courtesy of Brenda Riskey, UND Aerospace

provided through a robust Panasonic "Tough Book" tablet computer with a user friendly, proprietary software interface. Touch screen technology enhances the simplicity of the user interface. Simple and intuitive icons and checklists populate the computer screen while still leaving room for a primary and secondary display. The two displays allow the pilot to simultaneously view a map of the area of operations and live video feed from the aircraft. The arrangement allows the pilot to view all vital Information and control the aircraft without needing to scroll through multiple screens. To direct the camera, the pilot simply touches a spot on the primary display. The aircraft then turns toward the location and the camera slaves to the selected spot. The pilot can then advance the aircraft using simple forward and aft buttons. A left or right orbit of the camera focal point can be initiated by touching a button. Easy to interpret icons and warning messages keep the pilot apprised of GPS signal quality, aircraft battery condition, ground control station battery condition and link strength.

The Qube in Brief

List Price:	$50,000
Price as tested:	$65,000 (including color (EO) and thermal (IR) cameras)
Range:	1 km
Endurance:	40 minutes
Length:	36 inches
Weight:	5.5 pounds (with EO/IR camera payload)
Payload:	Dual high-resolution color (EO) and Thermal (IR) cameras

Training Curriculum

Factory training begins with AeroVironment providing access to an online Qube training course. The nine course segments include safety, assembly, launch and recovery, operation of the tablet computer, and malfunctions/emergencies. Each segment concludes with a quiz on the information presented. GFSD-UND's five pilots completed the course in six hours on average.

AeroVironment intends to provide future users with a Qube simulator that resides on the same tablet computer as the Qube Control System Software, as well as copies of the Qube manual prior to face-to-face training. While GFSD-UND trainees did not receive these training aids, each pilot indicated he could assemble, pre-flight and safely fly the Qube based solely on the online training program.

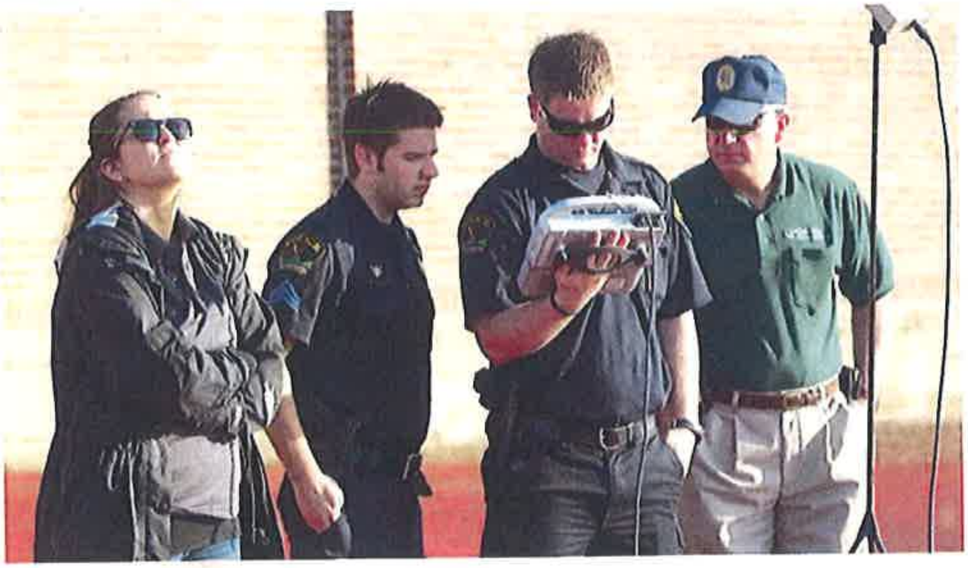
Face-to-face training for the GFSD-UND pilots was administered by Brian Hall, AeroVironment's chief sUAS flight instructor, accompanied by the Qube program manager and a Qube product engineer. The training consisted of PowerPoint-supported briefings, Qube simulator use, and hands-on outdoor Qube training within the GFSD Qube COA area of operations. Day one flights consisted of basic aircraft and ground control station assembly and use, pre-flight procedures, and multiple flights within a half-mile radius. Malfunction procedures, such as lost link and lost GPS, were also practiced. Day two was conducted indoors, as high winds precluded flying. Day three consisted of flying multiple simulated law enforcement mission flights within a large outdoor football stadium.

Using the System

The entire Qube system can be routinely assembled, pre-flighted and ready for operation in less than 10 minutes, even by inexperienced users like the GFSD-UND trainees. AeroVironment's claim of 40-minute flight endurance was routinely achieved during training.

A unique feature of the Qube is its ability to pre-program a defined flight radius and maximum operating altitude prior to launch. This "Geo-Net" easily permits operations to be conducted within a defined incident perimeter while remaining below the maximum altitude specified in an agency's FAA-issued COA. A remote video terminal, supported by a second tablet computer that provides real time video and can be linked to a larger monitor, was also used during flight training. The use of the terminal allows the pilot/visual observer team to maintain a sterile flight operations area while other personnel view the video feed at a nearby location.

GFSD-UND trainees reported the video quality was generally good but occasionally choppy and broken. AeroVironment representatives said this was because the Qube uses an unlicensed portion of the frequency spectrum. Although utilization of that portion



> "Day one flights consisted of basic aircraft and ground control station assembly and use, pre-flight procedures, and multiple flights within a half-mile radius."

of the frequency spectrum eliminates the need for a specific Federal Communications Commission Radio License, it also exposes the Qube to potential radio frequency interference from other devices, such as wireless intercoms, WiFi networks and garage door opener remote controls. AeroVironment intends to experiment with a small radio frequency analyzer, which would identify which of the Qubes's five available channels would work best in a particular area. Users would activate the frequency analyzer prior to a flight and select the most interference-free Qube channel for operations. Still, even while the video was experiencing interference, high definition digital photos taken from the Qube were crystal clear when reviewed after the flight.

On two of GFSD-UND's 23 test flights, the Qube software experienced a glitch with the Panasonic Tablet operating system, and a malfunction procedure was used to recover the aircraft. The sUAS performed as required, returning to the launch point and landing within a couple of feet of the original takeoff location. While one type of glitch was considered to be good performance for the first production model of the Qube, AeroVironment identified and corrected the error within one month. GFSD has flown the Qube extensively since the software was fixed and has experienced no problems.

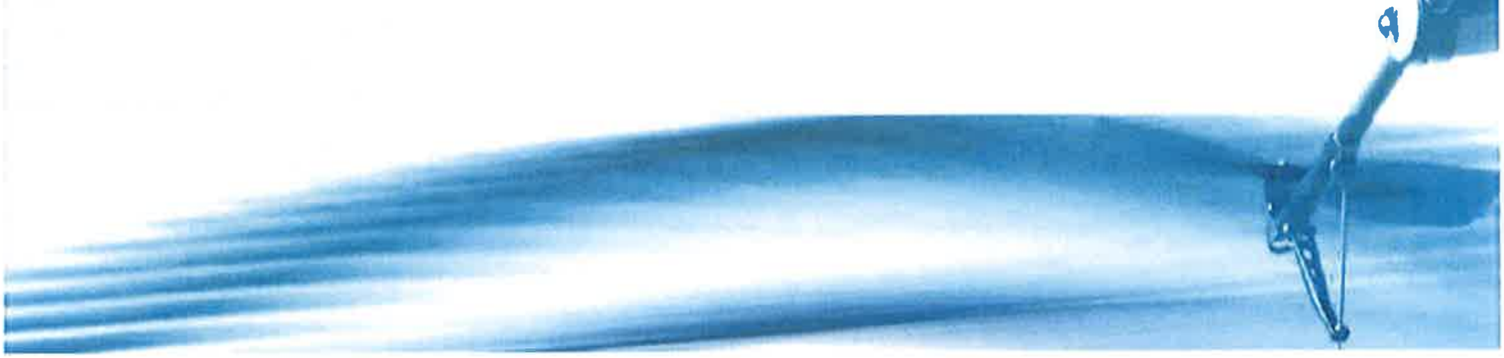
GFSD-UND operators indicated an area for improvement would be the cases used to transport the Qube and Qube Control Station. Although the interior of the cases are well organized, the hinges on the cases were less robust than expected. AeroVironment is searching for a more durable case and anticipates resolving the issue in the near future.

Throughout GFSD-UND's training and use of the Qube, AeroVironment representatives provided thoughtful support. They listened patiently to the trainees' input and made extensive notes on constructive comments. The company's customer service and support has also been good since the training.

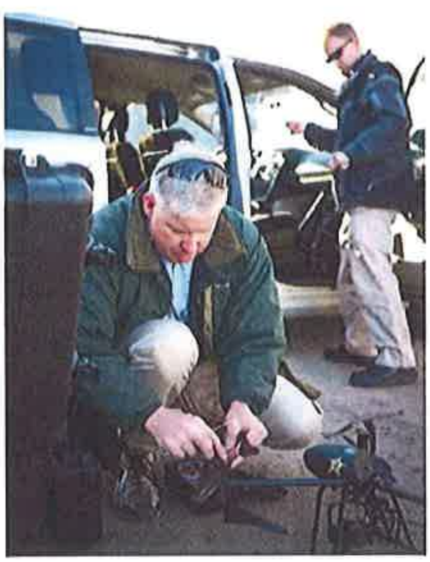
The Qube is a step in the right direction for public safety sUAS. It is compact, easy to use, has good mission endurance, appears robust, and is backed by a company with a considerable amount of sUAS experience.

UAS and Regio Where Unmanned Aircr Fit Between Agencies

By Alan Frazier, *Deputy Sheriff, Grand Forks (ND) County Sheriff's Office, Assistant Professor, University of North Dakota's John D. Odegard School of Aerospace Sciences*



Years ago, when I was an undergraduate at Middle Tennessee State University, I was struggling through a basic computer programming course. I complained to my older sister about it, making the argument that I hated computers and wanted no part of them. Her wise response was something like, "Alan, it really does not matter what you think of computers. They are coming whether you like it or not. If you don't want to be left standing on the platform when the train leaves the station, you will take time to learn about them."



My sister was right about computers, and I am glad I took her advice to learn a bit about those despicable machines. The same case can be made for UAS. No matter how we feel about them, they are coming in a big way. Now is the time for us all to learn about UAS and exert some influence on how they mature and are used in public safety and other applications.

One application in which UAS are ideal is regional air support units. The Grand Forks County (ND) Sheriff's UAS Unit is a regional asset serving 16 counties in northeastern North Dakota. Personnel from the University of North Dakota, Grand Forks County Sheriff's Department (GFSD) and Grand Forks Police Department have operated three different UAS over a variety of public safety incidents, including searches for suspects and victims, traffic accidents and crime scenes. The unit has existed on a very small budget (an average of $11,000 per year) since 2010. Grants and donations have provided the modest funding required to run the unit. Full-time law enforcement personnel are granted release time to participate in call-outs and monthly training sessions. In addition, firefighters and police officers from 11 additional agencies have been trained as visual observers/sensor system operators. A UAS familiarization class has been incorporated into the local police academy curriculum, and every Grand Forks County deputy sheriff and Grand Forks police officer has received UAS familiarization training (all North Dakota POST certified). None of this was difficult; it just took determination to implement.

Determination has been required to implement UAS in all sorts of airborne operations, and progress is now being made on two Federal Aviation Administration (FAA) issues that have hampered law enforcement use of UAS: night operations and second-class medical certificate requirements. Until recently, FAA had not granted authorization for UAS night operations to any non-federal law enforcement agency. In November

nal Units:

raft

2013, the Montgomery County (TX) Sheriff's Department and GFSD both obtained FAA approval to conduct night training UAS operations in specific areas. In addition, GFSD has a pending certificate of authorization application for nighttime operations throughout its 16-county mutual aid area.

FAA guidance documents mandate that both UAS pilots and visual observers must possess FAA second-class medical certificates. This is nonsensical, as second-class medicals are required for commercial operations. Since the FAA currently forbids commercial UAS operations, why would such a requirement exist? In fact, since UAS are classified as "public aircraft," no medical should be required. David Morton of FAA's UAS Integration Office reports he is working with FAA rulemaking teams to revise this requirement. Hopefully, Morton's efforts will lead to something sensible like the elimination of this requirement or at least substantial revision of the guideline. Light sport aircraft, glider and lighter-than-air pilots can operate their aircraft with a valid state issued driver's license in lieu of an FAA medical certificate. Current pending federal legislation would extend this privilege to non-commercial pilots of much larger aircraft. The time is right for FAA to parallel the pending legislation and reduce the medical requirement of UAS pilots and visual observers to possession of a valid state driver's license.

UAS are coming whether we like it or not. It is up to us as professional law enforcement aviators to help guide the technology. Consider the recent use of UAS by the Arlington (TX) Police Department. The department utilized its Leptron Helicopter UAS to provide enhanced situational awareness on an active-shooter call in North Arlington. The operation required an "Emergency Certificate of Authorization" to operate in the Dallas-Ft. Worth Class-B Airspace. Suzan Cogswell of Arlington PD provided the following account.

"In the early morning hours of Oct. 28, 2013, midnight officers were dispatched to a shots-fired call in an apartment complex on the city's far north side, just inside Class Bravo airspace. Upon arrival, officers advised dispatch that they were hearing multiple shots being fired and requested backup. Morning officers, just coming on shift, logged in and began running code to the location. Dispatch notified officers that a caller reported a body in a pool of blood lying on the ground. Officers were still taking fire and could not immediately reach the body. With the assistance of multiple callers from the apartment complex, officers were able to locate the suspect's apartment, which had both a rear balcony and front door that was tucked inside an interior stairwell. Each time officers gave verbal commands to exit the apartment, the suspect responded by firing multiple rounds at the officers. Perimeters were established and tactical units were engaged, at which point a request to use the department's small, unmanned helicopter asset was made through the chain of command. Because Arlington's citywide certificate of authorization does not currently permit flights in Class B airspace, an emergency application to fly this mission was made to the FAA. Authorization was granted, and the fly team was scrambled. Video images from the small helicopter's onboard camera sent real-time images to the on-site command center. Incident command was able to refute the report that there was a second body in the apartment stairwell, as well as to confirm the shooting suspect's location and to obtain an aerial overview for tactical purposes. Officers remained on scene until negotiators were successful and the suspect surrendered."

This is only one way in which UAS can be beneficial for law enforcement units. Many more are on their way. If you wish to learn more about using UAS, you may want to consider attending ALEA's UAS Operations Course which will be held July 14-16 in conjunction with ALEA EXPO 2014 in Phoenix, Arizona.

***Author's Note:** This is the first installment of a column focused on the use of unmanned aircraft systems in public safety applications. I am indebted to the ALEA Board of Directors for recognizing the need for such a column and for making space available in Air Beat.*

***About the Author:** Alan Frazier spent 31 years as a full-time law enforcement officer, including several as a TFO, pilot and OIC of a police air support unit. Frazier retired in 2010 and now teaches aviation courses and conducts UAS research at the University of North Dakota. He works part-time as a Grand Forks County (ND) Deputy Sheriff and North Dakota Park Ranger. He has been a pilot since his teenage years, flying airplanes, helicopters and gliders, making him a cop and pilot first and a "UAS guy" second. If you have input for this column, please feel free to call or email him at (701) 777-2959 or afrazier@aero.und.edu.*

DOES FAA HAVE THE AUTHORITY TO GOVERN UAS OPERATIONS?

By Alan Frazier, *Deputy Sheriff, Grand Forks (ND) County Sheriff's Office, Assistant Professor, University of North Dakota's John D. Odegard School of Aerospace Sciences*

I have had the opportunity to speak on the topic of unmanned aircraft systems (UAS) at many venues throughout the country. During these presentations, the most common question I hear is, "Does the Federal Aviation Administration have the authority to govern UAS operations?" The answer to this question differs greatly depending on whom you ask. FAA maintains UAS are "aircraft" and fall within the jurisdiction of their agency. However, the assertion is based on FAA guidance documents (05-01, 07-01, 08-01 and the latest, 7210.846), rather than regulations.

The matter is further clouded by FAA's 1981 issuance of *Advisory Circular 91-57*, which requests model aircraft operator's voluntary compliance with a maximum altitude of 400 feet AGL, avoidance of overflight of people and noise-sensitive areas, and notification to the airport operator or affected ATC facility when operating within three miles of an airport. Additionally, FAA requires government agencies operating UAS to declare the devices "public aircraft," which should exempt them and their operators from most FAA regulations.

FAA vs. Raphael Pirker

On Oct. 17, 2011, Raphael Pirker flew a Ritewing Zephyr over the University of Virginia (UVA) in Charlottesville, VA. The purpose of the flight was to collect airborne video for Lewis Communications, which intended to use the video in a promotional piece for the university. Pirker was compensated for the flights. The video was subsequently posted on YouTube, causing FAA to initiate an investigation. The administration's findings were communicated to Pirker in an April 2012 notice of proposed assessment and again in a June 2013 order of assessment.

FAA alleged Pirker had operated the Zephyr in a careless and reckless manner in violation of FAR 91.13(a) and cited 13 actions, including operating the aircraft "within approximately 15 feet of a UVA statue" and "within approximately 50 feet of railway tracks." FAA assessed Pirker a $10,000 civil penalty. Pirker appealed the civil assessment. On March 6, the Honorable Patrick Geraghty, a National Transportation Safety Board administrative judge, granted Pirker's motion to dismiss and vacated FAA's $10,000 civil penalty. Geraghty's ruling did not address the allegation of careless and reckless operation. Instead, it simply addressed the content of Pirker's appeal, which maintained that, in the absence of pertinent law, FAA does not have jurisdiction over model aircraft.

On March 7, 2014, FAA appealed Geraghty's ruling to the full NTSB Board. The appeal has the effect of staying Geraghty's ruling until the full board review is completed. If the NTSB Board affirms Geraghty's ruling, the answer to the question regarding FAA jurisdiction over small UAS is a fairly clear "no."

Debriefing the Decision

The real losers in this decision are the less than one dozen law enforcement agencies that have jumped through every hoop and hurdle FAA has imposed on small UAS operations. Requirements for letters from state attorney generals, filling out lengthy FAA certificates of authorization (COA) applications, FAA on-site inspections, night operations restrictions, and second class medicals will have all been for naught.

"Does FAA have the authority to govern small UAS? More importantly, is it appropriate for FAA to have a role in governing small UAS?"

Now, don't get me wrong. Even though my agency has jumped through all the FAA hoops, I am a strong proponent of a rule that would allow unrestricted line-of-sight VFR operations of small UAS in Class E and G airspace below 400 feet AGL. A 12-year-old model aircraft operator possessing no FAA pilot certificate, medical or COA can do all of that and more pursuant to *Advisory Circular 91-57*. Why should a law enforcement agency operating a similar model aircraft not be extended the same privileges?

FAA currently contends its interpretation of small UAS as being "aircraft" vs. "model aircraft" is solely based on the desire to ensure safety within the national airspace system. However, why does FAA differentiate between hobby and commercial/public safety missions? Why is it "safe" for a 12-year-old hobbyist to operate a small UAS in a public park, but it is "unsafe" for a law enforcement agency to operate a similar model aircraft in the same park? This is the type of non-sequitur that makes FAA's current position on small UAS untenable to law enforcement.

What then is the answer? Does FAA have the authority to govern small UAS? More importantly, is it appropriate for FAA to have a role in governing small UAS? The answer to the first question hinges on NTSB Board review of the Pirker decision. However, even if the NTSB affirms the decision, it is likely the effect on FAA will merely be to accelerate their issuance of a notice of proposed rule making (NPRM) addressing small UAS.

The answer to the second question is more subjective. FAA should have a role in

governing small UAS access to the National Airspace System. However, the administration needs to be more pragmatic and realistic. An important element of such an approach would be to allow public safety agencies open access to Class E and G airspace, below 400 feet AGL, during VFR conditions. In turn, the public safety agency would be required to operate the UAS only over a defined incident perimeter in which it can ensure the aircraft does not overfly people. In addition, agencies should be granted access to Class D, C and B airspace with the additional requirement that all flights must be coordinated with the affected air traffic control tower and/or radar facility.

The current system of COAs is unnecessary. A simple letter of agreement between FAA and a public safety agency should suffice. This would allow a reduction in paperwork of approximately 24 pages, as the average COA is 27 pages, and a letter of agreement could likely cover all required topics in three pages or less.

It is likely the NTSB will issue a ruling on the Pirker case in the very near future. Regardless of the ruling, it is important that public safety agencies closely watch for FAA's issuance of an NPRM addressing small UAS. Once the notice is issued, it is extremely important that public safety agencies thoroughly review and comment on the proposed regulations. If we remain silent, we forfeit our right to complain later about enacted regulations.

Section 4

The PoliceChief
The Professional Voice of Law Enforcement

send to a friend

Unmanned Aircraft Systems: All the Boxes Checked, but Challenges Remain

By Brett Davis, Vice President of Communications and Publications, Association for Unmanned Vehicle Systems International, Arlington, Virginia; and Don Roby, Captain, Baltimore County, Maryland, Police Department, and Chair, IACP Aviation Committee

A recent article in Police Chief magazine outlined factors to consider when purchasing technology. Is it cost effective? Is it training intensive? Will it require service and maintenance? What is the operational need—does it make the jobs of officers safer, easier, or more effective?[1]

These are the questions to ask when a police department considers whether or not to procure a new technology. And with public resources at stake, it is critical to carefully weigh the benefits of the technology and how it will enhance the department's ability to protect the communities it serve.

Draganflyer in flight.
Photo courtesy of the Mesa County Sheriff's Office.

It is no wonder why more and more law enforcement agencies across the United States are interested in unmanned aircraft systems (UAS). UAS have the potential to help law enforcement agencies save time, save money, and most importantly, save lives. They are ideal for dangerous or difficult situations like executing high-risk warrants;

responding to barricaded subjects; gaining situational awareness in difficult terrain; or responding to the damage caused by emergencies such as natural disasters, downed power lines, or hazardous material incidents.

Deputy Amanda Hill prepares to launch the department's Draganflyer X6 UAS.
Photo courtesy of the Mesa County Sheriff's Office.

UAS check all the boxes of the technology check list. First, they are cost effective. Many systems cost about the same amount as a squad car with standard law enforcement equipment. Their operational costs can provide police departments with remarkable savings. Ben Miller is the unmanned aircraft program manager with the Mesa County Sheriff's Office, one of the few law enforcement agencies in the country with a certificate of authorization (COA) from the Federal Aviation Administration (FAA) to fly unmanned systems. During a recent hearing before the U.S. Senate Judiciary Committee, Miller told senators about the cost effectiveness of UAS.

Constable Marc Sharpe of the Ontario Provincial Police operating a Draganflyer X-6 UAS.
Photo courtesy of Scott Hlady and the Airborne Law Enforcement Association.

"I estimate unmanned aircraft can complete 30 percent of the missions of manned aviation for 2 percent of the cost," said Miller. "The Mesa County Sheriff's Office projects the direct cost of unmanned flight at just $25 an hour as compared to the cost of manned aviation that can range from $250 to thousands of dollars per hour."[2]

The costs associated with UAS for training, as well as maintenance, are not prohibitive. The systems, which are often small and weigh less than five pounds, are much more affordable and easier to use than the unmanned aircraft designed for use by the military.

Most importantly, UAS help check the last box—they help make an officer's job safer, easier, and more effective. Whether it is a barricaded subject or a hostage situation, providing an aerial view of a search area or assessing damage from a natural disaster, UAS provide critical situational awareness without putting a human in harm's way.

However, expanding the use of UAS among public safety agencies is a challenge. vThe use of UAS domestically by law enforcement remains in its infancy because of the arduous FAA authorization process. Despite growing interest within the law enforcement community regarding the use of UAS, only a small handful of departments have obtained a COA to permit them to fly a UAS in civilian airspace.

"The process was rigorous; it was long," said Miller at the Senate Judiciary Committee hearing. "It took us approximately eight months to get the certificate that allows us to fly."[3]

Fortunately, last year Congress passed and the president signed into law the FAA Modernization and Reform Act, which streamlines this process and directs the FAA to plan for the expanded use of unmanned aircraft by 2015.

Not only will the new law make the COA application process easier, it will help advance the technology itself, making it more effective for use by law enforcement and others. The law directed the FAA to establish six test sites around the country for the development of UAS. As of the end of March, 50 applicants from 37 states had applied to receive a test site, eyeing the economic benefit a test site would bring to a local economy. Once the sites are established, manufacturers and end users including law enforcement will be able to test the technology for a variety of applications, honing it to help assist search and rescue, crime scene documentation, disaster response, or other specific public safety missions.

While the COA process is being streamlined, another issue looms large over the use of UAS—privacy. The ink of the president's signature on the FAA bill had barely dried when privacy groups and civil liberties advocates voiced concerns about how the technology would be used. While acknowledging the value of UAS for search and rescue missions or helping battle wild fires, these groups specifically want limits on law enforcement's use of UAS. Last year, several bills were introduced in the U.S. Congress that would have severely restricted the use of UAS by law enforcement, limiting their ability to effectively use the technology to keep communities safe.

In a recent column in the Washington, D.C., publication *The Hill*, Tim Adelman, a legal expert on the use of UAS by law enforcement, called many of these bills "ill-conceived."

"The dozen or so bills introduced in recent months addressing unmanned aircraft and the issue of privacy not only demonstrate a misunderstanding of current law, but could have unintended consequences that hamper law enforcement officers' ability to safely and efficiently do their jobs," wrote Adelman.[4]

Privacy concerns are legitimate. However, while there is plenty of case law built upon the foundation laid out by the Fourth Amendment to the U.S. Constitution protecting U.S. citizens from unreasonable searches, the use of UAS by law enforcement is a new development and a reasonable conversation about their use is entirely appropriate.

Last year, the Association for Unmanned Vehicle Systems International (AUVSI) published a "Code of Conduct" emphasizing safety, respect, and professionalism in the use of UAS technology by those who design, manufacture, and operate the technology. The code explicitly states that we will respect the privacy of individuals.[5]

"Safeguarding people's privacy is important to my industry, as well," said AUVSI President and CEO Michael Toscano during testimony before the Senate Judiciary Committee. "AUVSI believes all stakeholders can work together to advance this technology in a thoughtful way that recognizes the benefits and fuels job creation, while protecting Americans' safety, as well as their rights."[6]

In August 2012, the International Association of Chiefs of Police (IACP) took an important step when it released a set of guidelines for the use of UAS by law enforcement. The guidelines cover a range of issues including community engagement, system requirements, operational procedures, and image retention. They encourage community engagement and transparency with regard to how and when UAS will be used, as well as protections put in place to uphold citizens' rights.

"Despite their proven effectiveness, concerns about privacy threaten to overshadow the benefits this technology promises to bring to public safety," the IACP stated. "From enhanced officer safety by exposing unseen dangers, to finding those most vulnerable who may have wandered away from their caregivers, the potential benefits are irrefutable. However, privacy concerns are an issue that must be dealt with effectively if a law enforcement agency expects the public to support the use of UAS by their police."[7]

Soon after the IACP released the guidelines, they were endorsed by AUVSI and adopted by several law enforcement agencies. The Airborne Law Enforcement Association (ALEA), the FBI Law Enforcement Executive Development Association (FBI–LEEDA), and the FBI National Academy Associates (FBINAA) endorsed the guidelines that same month.

The guidelines were well received, even by those voicing concerns about law enforcement's use of UAS. For example, an analyst with the American Civil Liberties Union called them "quite strong" and wrote that "the IACP is to be applauded for addressing the issue."[8]

The guidelines provide a comprehensive road map for any law enforcement agency looking to deploy UAS technology while safeguarding people's rights. After all, many law enforcement agencies considering using UAS want to do so in instances when individual privacy is not at issue.

However, despite the publication of the guidelines, it quickly became clear that challenges remained. Residents in several communities across the country including Seattle, Washington, and Alameda County, California, have raised concerns with the use of UAS by law enforcement, however unfounded.

These concerns have led to legislation being introduced in state legislatures that would deny public safety agencies a potentially life-saving tool. The Arlington, Texas, Police Department successfully petitioned the FAA for approval to use unmanned aircraft for missions including search and rescue, surveys of flooded areas and other natural disasters, clearing traffic crashes more quickly, and analysis of hazardous material spills. However, legislation introduced in Texas could hinder the department's ability to use the technology.

"While we understand and support the intent of this proposed bill, and other similar bills, we strongly believe that the passage of this bill would significantly impede law enforcement's ability to protect and serve our community," wrote Arlington Police Chief Will Johnson in a letter to a state legislator who introduced restrictive legislation.[9]

It is clear that the perception of unmanned aircraft is still largely shaped by how the public sees it being used in counterterrorism missions abroad, even though their domestic use would be quite different. This is why communication about how unmanned aircraft will actually be used domestically from those who will use it is critical. By adopting and publicizing guidelines for the use of UAS, law enforcement agencies give the public a clear picture of how, when, and why law enforcement is using UAS. Allaying the public concern is a critical step in putting the technology to use keeping officers safe as they do their jobs.

When the public sees the reality of public safety's use of UAS, rather than the sensationalism, it is supportive. According to a national poll conducted last year by Monmouth University, 80 percent of Americans support the use of unmanned aircraft to help in search and rescue missions, while about two-thirds of Americans support their use in tracking down runaway criminals and protecting U.S. borders. Another poll conducted by the Associated Press found that more people support allowing police forces to use UAS to assist in their work than oppose. That same poll found that more people are concerned that social networking sites like Facebook will cause them to lose privacy than police departments using UAS.

In the not too distant future, UAS technology will be a fixture in missions to find a lost child, respond to a devastating earthquake, or defuse a dangerous situation. But in order to get there, lawmakers, the public, and other stakeholders must understand why public safety agencies' use of UAS will benefit not only the agencies, but the communities they serve as well. This will require an open and consistent dialogue between law enforcement agencies and their communities about the benefits afforded by UAS, and the measures—as outlined in the IACP guidelines—by which citizens' rights will remain protected. ♦

Notes:

[1]Paul D. Schultz, "The Future Is Here: Technology in Police Departments," The Police Chief 75 (June 2008): 20–25, www.policechiefmagazine.org/magazine/index.cfm?article_id=1527&fuseaction=display&issue_id=62008 (accessed May 1, 2013).

[2]Ben Miller, "The Future of Drones in America: Law Enforcement and Privacy Concerns," written testimony before the U.S. Senate Judiciary Committee Hearing, March 20, 2013, www.judiciary.senate.gov/pdf/3-20-13MillerTestimony.pdf (accessed April 22, 2013).

[3]Ibid.

[4]Tim Adelman, "Flurry of 'Drone' Bills Shows Congress Has Much to Learn," *The Hill*, September 20, 2012, thehill.com/blogs/congress-blog/foreign-policy/250597-%20flurry-of-drone-bills-shows-congress-has-much-to-learn (accessed April 22, 2013).

[5]Association for Unmanned Vehicle Systems International, "Unmanned Aircraft System Industry 'Code of Conduct,'" www.auvsi.org/conduct (accessed April 22, 2013).

[6]Michael Toscano, "The Future of Drones in America: Law Enforcement and Privacy Considerations," opening statement before the U.S. Senate Judiciary Committee Hearing, March 20, 2013, www.judiciary.senate.gov/pdf/3-20-13ToscanoTestimony.pdf (accessed April 22, 2013).

[7]IACP Aviation Committee, *Recommended Guidelines for the Use of Unmanned Aircraft* (August 2012), www.theiacp.org/portals/0/pdfs/IACP_UAGuidelines.pdf (accessed April 22, 2013).

[8]*Free Future: Protecting Civil Liberties in the Digital Age*, "Police Chiefs Issue Recommendations on Drones; A Look at How They Measure Up," blog entry by Jay Stanley, August 17, 2012, www.aclu.org/blog/technology-and-liberty/police-chiefs-issue-recommendations-drones-look-how-they-measure (accessed April 22, 2013).

[9]William Johnson, "Opposition to HB 912 Texas Privacy Act," letter to Representative Lance Gooden, March 25, 2013.

Please cite as:

> Brett Davis and Don Roby, "Unmanned Aircraft Systems: All the Boxes Checked, but Challenges Remain," *The Police Chief* 80 (June 2013): 60–63.

Top

From The Police Chief, vol. LXXX, no. 6, June 2013. Copyright held by the International Association of Chiefs of Police, 515 North Washington Street, Alexandria, VA 22314 USA.

Return to Article

send to a friend

Section 5

The Truth About Remotely Piloted Vehicles and Privacy.

By: Tim Adelman

May 23, 2012

The media and privacy groups have two well-known tendencies. First, they are more than willing to make dogmatic pronouncements based on limited information and limited effort to determine the facts, and second, they tend to sensationalize everything to try to get everyone's attention. Both of those attributes have come into play as attacks have been launched on the use by law enforcement agencies of remotely piloted vehicles, known as RPVs, or "drones" as the media prefers to refer to them.

Recently, the Electronic Frontier Foundation (EFF) took on the crusade to find out which law enforcement agencies were using RPVs in the United States. When the FAA provided the list of agencies in response to a Freedom of Information Act request, EFF celebrated as if it were finally breaking the government conspiracy to spy on citizens. EFF has targeted the FAA for allegedly creating a system that would result in a privacy invasion pandemic. Unfortunately, EFF did not take the time to ask questions before shooting off its press releases.

Currently, the average citizen can buy a remote control helicopter with a camera system or attach their high quality camera. With the simple addition of a commercially available autopilot, they can have autonomous RPVs capable of taking pictures of your backyard. Unfortunately, there is very little the local police or you can do to stop this invasion of privacy beyond pursuing claims through existing civil laws. The FAA regulations do not currently regulate the remote controlled helicopter with a camera used by the average citizen. Similarly, the paparazzi could build their own RPV with autopilot features and cameras using the information on www.diydrones.com, or a host of other websites. The technology permitting private citizens to spy on others is abundant. A simple YouTube search will reveal hundreds of homemade videos using what EFF would consider to be a drone.

The FAA recognized long ago that the use of remotely piloted vehicles would continue to grow exponentially with the decrease in cost of equipment and the availability of high resolution low cost, light weight cameras. The FAA set up the Unmanned Aircraft Program Office, now the FAA's UAS Integration Office, to help identify the issues with the use of RPVs and to work on developing updated regulations to encompass this technology. The FAA has already conducted an advisory rulemaking committee to help provide input into a small unmanned aircraft system rule. The FAA is now working through the information provided by the rulemaking committee in the hopes of publishing regulations.

Based on a number of recent stories in the media, members of Congress sent a letter to the Federal Aviation Administration asking how the FAA will protect individuals' privacy rights in response to the new legislation requiring the FAA to take steps to assist in the integration of

RPVs into the National Airspace. The letter stated, "we are writing to express our concerns about the law's potential privacy implications and to requisition information about how the FAA is addressing these important matters." Similarly, Jay Stanley, a Senior Policy Analyst with the ACLU, wrote that the FAA needs to "impose some rules (such as those we proposed in our report) to protect Americans' privacy from the inevitable invasions that this technology will otherwise lead to." However, everyone seems to be overlooking the fundamental principle that it is not the FAA's responsibility to protect privacy. It was best said by Justice Sandra Day O'Connor in her concurring opinion in the Supreme Court of the United States' Florida v. Riley when she stated that the FAA regulations are intended to promote air safety and not to protect the right to be secure against unreasonable search and seizures. Even though the FAA is not responsible for ensuring our privacy rights, its efforts to regulate and increase the safety of the use of RPV has an indirect benefit of adding protection to our privacy rights.

As previously stated, the average citizen can fly a drone now and use it to take pictures of his neighbor. Such use would likely not violate any FAA regulation. However, if the FAA is able to enact the small unmanned aircraft system regulations which address air safety, those regulations could have the additional benefit of significantly restrict this unwanted privacy invasion. In fact, if the FAA added a provision that made a violation of the regulations a criminal act, local law enforcement could help enforce the proper use of civil drones. Without these beneficial regulations, there is very little that can be done to stop civil homemade drone use.

Now to address the groups that believe our domestic law enforcement agencies are an offshoot of Stalin's secret police. I find it disappointing that privacy groups presume guilt, i.e. that law enforcement will inappropriately spy on citizens, without any evidence that inappropriate spying is occurring, yet law enforcement abides by the requirement to obtain probably cause before conducting a search for possible illegal activities. The mere fact that someone could do something illegal is not enough for law enforcement to conduct a search. Yet, the mere fact that someone could use an RPV to "spy" on a citizen results in condemnation of an entire industry.

The ability for law enforcement to observe what happens in your backyard from the sky has been around for years. In fact, there have been many court cases argued over the scope of a "search" from the air by law enforcement without a warrant. The Supreme Court of the United States stated, "what a person knowingly exposes to the public, even in his own home or office, is not a subject of *Fourth Amendment* Protection." Katz v. United States. In addition, the Supreme Court noted "as a general proposition, the police may see what may be seen from a public vantage point where they have a right to be." Florida v. Riley. In Riley the plurality opinion focused on the fact that the helicopter that hovered over the defendant's house looking for marijuana plants did so at 400 feet above the ground. The Court noted that flying over the defendant's house was permitted by FAA regulations; and, therefore, the police were observing from a position the general public also could observe from. Substituting an RPV for a manned helicopter in no way changes the equation from a privacy perspective.

Applying the rationale in Riley, the FAA's recent collaboration with DOJ'S NIJ is an effort to provide guidance and structure to law enforcement operations that will increase, not decrease, our right to privacy. Under the current FAA regulations, there is a strong argument that a law enforcement entity could fly a RPV without any permission from the FAA. A public entity does not need a civil airworthiness certificate issued from the FAA and the operator of the public aircraft does not need an airman certificate. As long as the law enforcement agency complies with the Part 91 rules of the road, no further FAA input is needed. Recently, Amie Stepanovich, legal counsel to the Electronic Privacy Information Center ("EPIC") was quoted by Shaun Waterman in his article "Drones over U.S. Get OK by Congress" in the Washington Times stating, "currently, the only barrier to the routine use of drones for persistent surveillance are the procedural requirements imposed by the FAA for the issuance of certificates." Actually, Ms. Stepanovich is not correct. The FAA has very limited authority right now to prevent a government owned RPV from operating as a public aircraft. The FAA's certificate of authorization ("COA") process is a process created by FAA policy to help government agencies operate RPVs in a safe manner consistent with the FAA's "rules of the road" regulations.

The recent efforts by the FAA and the Department of Justice, through the National Institute of Justice, to create a public safety focused COA process are intended to address the risk associated with RPV operations and provide a common structure for those public safety entities wanting to use RPV to assist in routine missions. However, the FAA's focus is, as it should be, on ensuring safe operations in the National Airspace, not privacy matters. The benefit of the FAA and DOJ's effort in establishing a public safety specific COA process is that it provides notice to the public about unmanned aircraft operations through the Airport Facilities Directory and Notice to Airman sources accessible by the public. Moreover, if the Supreme Court is going to look at FAA guidance to help determine when it is appropriate for law enforcement to be flying an RPV over someone's house, the COA process would be the only guidance at this point.

Using the structure of the COA process, we can then look at the Constitution and the numerous court opinions to determine the implication on privacy protections. For example, the use of RPVs to conduct surveillance can be analogous to the Supreme Court's handling of thermal imaging.

In the case of Kyllo v. United States the Supreme Court addressed whether the use of thermal imaging to detect the heat emitted from a house indicating possible marijuana plant grows constituted a search under the *Fourth Amendment.* The basic facts of the case involved the use of a thermal imager by a police office to scan a house from across the street at 3:20 am. The results of the scan indicated that the garage was producing excessive heat in comparison with the rest of the house and other houses in the neighborhood. Based on tips from an informant, the utility bills and the thermal scan, a warrant was issued to search the home. The Supreme Court held that the use of the thermal scanner, a sense-enhancing technology that was not in general public use, was a search that required a warrant.

The Kyllo Court noted:

> It would be foolish to contend that the degree of privacy secured to citizens by the *Fourth Amendment* has been entirely unaffected by the advance of technology. For example, as the cases discussed above make clear, the technology enabling human flight has exposed to public view (and hence, we have said, to official observation) uncovered portions of the house and its curtilage that once were private… The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.

The Court struggled with the emergence of technology and the protections of privacy. In determining whether privacy has been invaded by the use of technology by law enforcement, the Court analyzed whether such technology was readily available to the public.

> We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area,… constitutes a search -- at least where (as here) the technology in question is not in general public use.

The standard set forth by the Kyllo Court was flexible enough to be adapted to future advance in technology, such as the use of RPVs. To the extent law enforcement is using an RPV with unique technology available to the public, then the use of the unique RPV technology to search the privacy of a home could be considered a search. If the civilian small unmanned aircraft rule were implemented in a manner that limited the ability for the average citizen to fly over another's property at low levels for observation, then the FAA's issuance of a COA to permit police to fly low level for observation would likely be considered a search, i.e. law enforcement using technology in a manner not available to the public, and a warrant would be needed. In other words, the FAA is not the privacy rights enemy. If anything, the FAA, as an incidental benefit to its legitimate safety role, is providing a frame work to secure our right to privacy.

So where do we go from here? The uproar that adequate laws are not in place to protect the privacy of individuals from spying drones is misleading and uninformed. The *Fourth Amendment* is the foundation of our right to privacy. The Supreme Court and many local courts have offered countless opinions defining when the use of technology by law enforcement constitutes a search. Public safety agencies have been using aircraft for decades to provide situational awareness and eyes in the sky to aid in their missions. The use of RPVs provides no further capabilities than what already exist. In fact, a Cessna 206 (single engine six passenger aircraft) with a high powered camera is more effective at surveillance, and therefore potentially more intrusive, than most RPVs available to law enforcement because the camera system is of substantially better quality; it can see finer detail at high altitudes and it does not have the operational limitations imposed on the use of RPVs. Even with aviation assets available to law enforcement for the past decades, our privacy has not been unreasonably invaded. We have not had a pandemic of privacy invasions from aircraft because the Constitution along with the judicial system have routinely provided rigorous protections.

Demanding that the FAA address the privacy implications of RPVs is like asking your car mechanic to perform open-heart surgery. The FAA's expertise is aviation safety. We should look to those tasks with protecting our civil rights, the Department of Justice, to help identify the issues with privacy as they relate to the use of RPVs by law enforcement. Moreover, we should look to the expansive body of case law that has already established the standards for limiting unconstitutional searches. If the privacy groups' concerns are truly limited to how law enforcement may use RPVs in their daily missions, then a technology acceptance panel hosted by the National Institute of Justice would be the perfect avenue for addressing those concerns. A technology acceptance panel brings together interested parties, i.e. law enforcement, privacy groups, regulators and others, to discuss the use of the technology, the public's concerns over the technology and hopefully arrive at best practices for effectively using the technology while at the same time protecting the public's interests.

I would also recommend that the FAA consider inserting criminal penalties for violation of the small unmanned aircraft rule when it comes out in the near future. This rule will hopefully capture the current unlimited use of RPVs by civilians and provide law enforcement with a means to enforce improper use of RPVs by civilians. On that note, I would highly recommend that FAA be given the necessary resources to quickly implement the small unmanned aircraft rule to further enhance our privacy protections from the spying civilian.

Finally, instead of taking punches at the FAA, DOJ or other government entities for working to implement a technology safely, I would suggest that interested parties start acting collaboratively. The FAA and DOJ's NIJ spent many months working together to develop a process for the safe operation of RPVs. Such government collaboration should be applauded. Instead of making assumption that the local sheriff is now going to be spying on you, why not provide suggested guidance on how to address the public concerns. The privacy uproar over the use of RPVs by law enforcement reminds me of a brilliant line by Michael Douglas in the movie *American President*:

> We have serious problems to solve, and we need serious people to solve them. And whatever your particular problem is, I promise you, [my opponent] is not the least bit interested in solving it. He is interested in two things and two things only: making you afraid of it and telling you who's to blame for it. That, ladies and gentlemen, is how you win elections.

I cannot help but think as I read the articles about the use of RPVs to invade your privacy that the articles attempt to prey on peoples' fears and tell you who to blame, yet they offer no substantive suggestions on how to address the issue. If privacy groups take the position that RPVs should never be used, then it is difficult to argue logic with them. If the privacy groups understand that there is a real value to the use of RPVs, such as using an RPV to patrol a school campus during an active shooter incident to identify possible hostiles or potential victims, then hopefully through their thoughtful assessment of the situation they could provide meaningful suggestions on the proper use of RPVs.

Section 6

MEMORANDUM OF UNDERSTANDING
BETW EEN
FEDERAL AVIATION ADMINISTRATION, UNMANNED AIRCRAFT SYSTEMS INTEGRATION OFFICE AND THE U.S. DEPARTMENT OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, NATIONAL INSTITUTE OF JUSTICE
CONCERNING
OPERATION OF UNMANNED AIRCRAFT SYSTEMS BY LAW ENFORCEMENT AGENCIES

I. PURPOSE: This Memorandum ofUnderstanding (MOU) sets forth an agreement between the Department of Transportation, Federal Aviation Admi nistration (fAA) Unmanned Aircraft Systems Integration Office, and the Department of Justice (DOJ), Office of Justice Programs (OJP), National Institute of Justice (NIJ), hereinafter, "the Parties," to implemen t a streamlined tTaining and authorization process to enable nonfederal1aw enforcement agencies (LEAs) to operate unmmmed aircraft systems (UAS) within the United States safely, effectively, and lawfully.

II. AUTHORITY: This MOU is entered into on the part ofNIJ pursuant to Titles II, 111, and V of the Homeland Security Act of 2002 (6 U.S.C. *§§* 121 *et seq.* and 182 *el seq.);* and Title I of the Omnibus Crime Control and Safe Streets Act of 1968 (42 U.S.C. §§ 371 1 *et seq.),* and on the part of the FAA pursuant to the Federal Aviation Act of 1958 (49 U.S.C. *§§* 40101,40103, and§§ 44701-44735).

III. BACKGROUND:

The FAA is charged with regulating the use of U.S. airspace to ensure its safety and efficient use. With regard to public UAS, including those used by LEAS and other public safety agencies, Public Law 112-95, the FAA Modernization and Reform Act of2012, directs the FAA to issue guidance regarding the operation of publ ic UAS to—

1) Expedite the issuance of a certificate of authorization (COA) process.
2) Provide for a collaborati ve process with public agencies to allow for an incremental expansion of access to the national airspace system as technology matures and the necessary safety analysis and data become available and until standards are completed and teclmology issues are resolved.
3) Facili tate the capabili ty of public agencies to develop and use test ranges, subject to operating restrictions req uired by the FAA, to test and operate unmanned aircraft systems.
4) Provide guidance on a public entity's responsibili ty when operating an unmanned aircraft without a civil airworthi ness certificate issued by the FAA.

It further requires that the FAA shall, not later than December 31, 2015, develop and implement operational and certification requirements for the operation of public UAS in the national airspace system.

NIJ is the research, development, and evaluation arm of the U.S. Department of Justice and is dedicated to researching crime control and justice issues. NIJ provides objective, independent, evidence-based knowledge and tools to meet the challenges of crime and justice particularly at the state and local level. Through its Office of Science and Technology, NIJ, in part, serves as the national focal point for research, development, testing, and evaluation of technology for law enforcement. NIJ identifies the needs of the law enforcement community for new technologies and tools and develops solutions. NIJ develops standards and conducts testing to evaluate technologies that may be used by law enforcement agencies. NIJ works with other federal agencies to establish a coordinated federal approach on issues relevant to law enforcement and with government agencies at all levels and professional associations to foster the adoption into practice of new tools and technologies. The activities NIJ sponsors in this regard include development of relevant training materials, best practice guides, and policies.

Through a research project aimed at identifying low-cost aviation solutions for small and rural agencies that cannot afford the costs associated with operating traditional fixed-rotary-wing aircraft, NIJ determined that UAS could provide an affordable solution for those agencies that need "eyes in the sky" but lack the budget or for those agencies that need to supplement their current aviation units with more cost effective aircraft for specific missions.

NIJ and the FAA have a shared mission to ensure the sate and effective use of UAS in public aircraft operations. It is in the interest of both agencies to meet or exceed the goal set by Congress to develop and implement operational and certification requirements for the operation of public UAS in the national airspace system (NAS). To that end, they have collaborated since 2005 to develop the attached streamlined training and authorization process, which reflects the input of the state, local and federal law enforcement conml0nity gathered and represented by NIJ. The result of this collaboration will allow for real-time access to the (NAS) for agencies responding to emergency circumstances.

IV. SCOPE: To further this shared mission, the parties will now collaborate to implement the attached streamlined training and authorization process for LEAs' use of UAS, particularly those agencies without prior aviation experience.

V. IMPLEMENTATION:

A. NIJ will:

1. Prepare and coordinate with the FAA UAS Integration Office (FAA UASIO) and the Department of Homeland Security Science and Technology (DHS S&T) the distribution of a technical bulletin that addresses the utilization of UAS in the NAS for LEAs and other public safety agencies, which NIJ will maintain and update as

necessary.

2. In coordination with FAA UASIO, develop and promulgate a process for collecting, analyzing and publishing UAS training and operational mission data that specifically captures and assesses mission capability of the technology (to include ·'Lessons Learned").

B. The FAA UASIO will:

Through the COA validation process, FAA will assess each LEA applying to operate under this agreement to ensure that it demonstrates a level of capability to operate its specific UAS safely and competently within the NAS. The FAA assessment of the proposed UAS operations' impact on the level of safety in the NAS will evaluate whether adequate mitigations are available to compensate for any inability to comply with 14CFR §§91.111 and91.113(b).

C. Each Party to this MOU will fund its expenses associated with pallicipation covered by this MOU. This MOU in no way restricts any Party from participating in similar activities or arrangements with other public or private agencies, organizations or individuals.

D. Each Party will provide personnel and resources as appropriate to implement its responsibilities under this MOU.

E. Each Party will take appropriate steps to ensure that its employees, agents, contractors, and consultants involved in projects conducted under this MOU comply with any pertinent provisions of this MOU.

F. Each Party will handle and expend its own funds. The responsibilities each Party assumes under this MOU are subject to the availability of funds for such purposes. Nothing in this MOU, in and of itself, obligates any Party to expend appropriations or to enter into any contract, assistance agreement, interagency agreement or other financial obligations. Any endeavor involving reimbursement or contribution of funds between the Parties will be handled in accordance with applicable laws, regulations and procedures, and will be subject to separate interagency agreements that will be effected in writing by representatives of the Parties.

G. Management Points of Contact. The Parties designate the following individuals to serve as their management points of contact for matters related to this MOU. Each Party may change the individual designated as its management point of contact upon notice to the other Parties of such change.

National Institute of Justice
Office of Science and Teclmology
Program Manager
202-305-7954

Federal Aviation Administration
UAS Integration Office
Air Traffic Manager
202-385-4661

VIII. MODIFICATION AND TERMINATION:

A. Amendments or modifications to this MOU must be approved by each of the Parties in writing in accordance with applicable policies, procedures and legal requirements.

B. Any Party may terminate its participation in this MOU at any time, but should provide thilty (30) days written notice to the other Party. Disposition of any efforts in progress at the time of notification will be determined by agreement of the Parties.

C. In the event of disagreement between the Parties with respect to this MOU, the Parties will each undertake to attempt a good faith effort to resolve the disagreement. Nothing in this MOU, however, will take precedence over, or negate or affect in any way, the policies, procedures and directives of the respective Parties or any applicable laws or regulations. If a disagreement cannot be resolved, the palties may modify or terminate this MOU.

IX. NATIONAL SECUIUTY INFORMATION: Security classification guidance for activities undertaken pursuant to a subsequent interagency agreement will be determined in accordance with the laws, regulations and policies governing the lead agency for those activities.

X. PUBLIC INFORMATION COORDINATION: Public disclosures of information regarding projects and activities conducted under this MOU are subject to the Freedom of Information Act (5 U.S.C. § 552). The Parties will consult with each other prior to any public disclosure of information.

XI. EFFECTIVE DATE: The provisions ofthis MOU become effective as of the date of the last signature hereunder, and will remain in effect for five (5) years, unless terminated earlier in accordance with the provisions of this MOU.

Agreed:

J m s H. (Jim) Williams
n anned Aircraft Systems Integration Office
• /\ Aviation Safety Organization
Federal Aviation Administration

Date: :.>}4/13

Gregory ·ageway, Ph.D
Acting Director
National Institute of Justice
Office of Justice Programs
U.S. Department of Justice

Date: 2/Z7/J3

ATTACHMENT TO THE MEMORANDUM OF UNDERSTANDING
BETWEEN
FEDERAL AVIATION ADMINISTRATION, UNMANNED AIRCRAFT SYSTEMS INTEGRATION OFFICE AND
THE U.S. DEPARTMENT OF JUSTICE,
OFFICE OF JUSTICE PROGRAMS,
NATIONAL INSTITUTE OF JUSTICE
CONCERNING
OPERATION OF UNMANNED AIRCRAFT SYSTEMS
BY LAW ENFORCEMENT AGENCIES

PART 1 —LEA UAS Operational Requirements. Elements. and Procedures

I. **UAS Safety Risk Analvsis Plan (SRAP) and Defined Incident Perimeter**

a. For the purpose of identifying and mitigating risks arising from UAS operations, any LEA wanting to use the stream lined LEA UAS authorization process would be required to submit a formal SRAP as an attachment to its Certificate of Waiver or Authorization (COA) application that specifically identifies the boundaries of the agency's jurisdiction and all unique operational areas within that jurisdiction and attendant hazards *(e.g., ailports. motor speedways, large sports complexes, major highways, strategic/sensitive il?(rastructures, university campuses with airspace, obstruction clearance, public access, evacuation mitigation, rush hour heavily trafficked roads, or other incumbent hazard).* The SRAP must include a description of specific risk controls to be employed to mitigate any attendant hazard for UAS operations within the jurisdiction in the vicinity of those identified unique operational areas.

b. All UAS operations will be conducted within the boundaries specified in the LEA's COA. These boundaries will fall within the area of the LEA'sjurisdictional control. Further, the operation will be conducted within a nonmoving "Defined Incident Perimeter" that is controlled by the LEA and identified by geographic coordinates (pursuit missions arc not authorized).

c. The use of the streamlined LEA UAS authorization process may be used only by LEA's deploying UAS with a gross take-off weight that does not exceed 25 lbs.

II. <u>**UAS Airworthiness. Emplovment. and Safety of Operations**</u>

a. The accountable executive (e.g., agency head) of each LEA will acknowledge in writing that the UAS the LEA intends to deploy is airworthy and in a condition for safe operation based on the manufacturer's specifications, maintenance recommendations and operating procedures of the aircraft, control station, communications links and lost link procedures. This process docs not constitute an Airworlhiness Certification by the FAA.

b. Upon the first application by each LEA, the applicant must submit a legal determination that it is eligible to operate a public aircraft under the applicable paragraph of 49 U.S.C. § 401 02(a)(4 1) (citing the applicable paragraph and support in its determination), that the UAS will be operated in accordance with 49 U.S.C. § 40125 (will not receive compensation or reimbursement for operation except as specified in the statute) and will not operate the aircraft in any manner that endangers life or property in accordance with 14 CFR § 91.1 3.

c. These airworthiness, operational safety and public aircraft statements will be on LEA letterhead stationery, signed and dated by the agency head making the acknowledgements, and must be included as an attachment to the COA application. In the event of a LEA leadership change, a new or revised statement must be submitted to ensure that the new leadership is fully aware and informed of the COA.

III. Pilot & Observer Qualifications for UAS operations at and below 400 feet AGL

a. Each UAS pilot must be an FAA-certificated airman or successfully pass either the FAA's pilot knowledge exam or complete an FJ\1\-approved UAS pilot training curriculum. If operating in an area that requires Air Traffic Controller (ATC) communication, additional pilot training may be required if the UAS pilot is not a certificated manned-aircraft ainnan.

b. Pilots will receive training specific to the UAS to be operated. This training must be conducted and documented by a qualified instructor designated by the proponent as being the individual(s) trained and certified by the manufacturer to provide training on the specified UAS.

c. Pilots are prohibited from flying any public safety miSSion without having completed three UAS flight events within the preceding 90 days.

d. Observers must successfully complete a UAS observer training cun·iculum that includes, at a minimum, instruction on rules and responsibilities described in 14 CFR § 91.111, Operating Near Other Aircraft, 14 CFR § 91.113, Right of Way Rules, Cloud Clearances, and that emphasizes "See and Avoid" concepts and fundamental radio communications, including standard ATC phraseology. Observer training must include thorough instruction regarding manned aircraft traffic conflicts and pilot communications for any maneuvers/actions required to avoid traffic conflicts.

e. Pilots and observers must not perform duties for more than one UAS at a time and are not allowed to perform concurrent duties both as pilot and observer.

f. LEA standard operating procedures (SOP) must include Crew Resource Management (CRM) techniques to ensure the highest possible situational awareness and effective communication by pilots and observers during each flight operation. Pilots and observers must be trained in these procedures and techniques.

g. All pilot and observer training must be conducted and documented by a qualified instructor designated by the proponent as being an individual trained and certified by the manufacturer to provide training on the specified UAS.

h. Pilots and observers must be medically qualified and have in their possession a second class (or higher) airman medical certificate that has been issued under 14 CFR Part 67, Medical Standards and Certification.[1]

i. 14 CFR § 91.17, Alcohol and Drugs, applies to UAS pilots and observers.

[1] Tlle FAA. at thl! request of OOJ/NIJ, is working to change the requirement for a second-class aim :m medical ccnillcation to ..self-certification.. as to being hcalthy to fly and a letter from a competent medical authority conllnning the operator's eyesight to the second-class medical certification requirements of correctable to 20/20.

IV. UAS Flight Operations

a. The pilot-in-command (PIC) will conduct a thorough premission briefing prior to commencing any UAS flight operation. At a minimum, the briefing must include a review of the SRAP for the specific hazards within the area of operations, the LEA's standard operating policies and procedures, specific objective(s) of the mission, expected duration of the mission, operating limitations/restrictions, specific duties of each crew member, specific communications plan including a lost communications procedure, and emergency procedures.

b. VAS operations, within the area of jurisdiction, must remain within a nonmoving "Defined Incident Perimeter" at or below 400 feet above ground level (AGL). The LEA will identify and manage all potential air and ground hazards inside the "Defined Jnciclent Perimeter." especially concerning overflight of people and private property. "See and Avoid" is paramount to safe UAS operations, and all flights will remain within the visual line of sight of the pilot and employ at least one observer, not including the PIC. All of the risks and associated liabilities that exist within the "Defined Incident Perimeter" must be legitimately mitigated, and the safety of people and property assured.

c. VAS flight operations will only be conducted during daylight hours and must adhere to Day Visual Flight Rules (VFR) with Visual Meteorological Conditions (VMC) with visibility and cloud clearances specified for Class E airspace.

d. Use of visual observers in a linear fashion away from the control station (daisy chaining) is prohibited.

e. Moving "Defined Incident Perimeters" to acconunodate pursuit missions are prohibited. UAS pursuit missions arc NOT authorized outside of the "Defined Incident Perimeter."

f. Only one LEA UAS will be flown at a time within the "Defined Incident Perimeter."

g. The UAS will not fly over outdoor assemblies of people or heavily trafficked roadways. LEA UAS flight operations must be offset as needed to ensure the orbit or flight path of the UAS does not incur a risk of injury to persons or property along its flight path. A mitigation strategy may include, but is not limited to, evacuation of persons from within the defined incident perimeter by legal police authority.

h. The PIC shall comply with all ATC instructions and/or clearances.

i. Operations within Class A and B airspace are prohibited. *(Note: A description of classes of airspace is included as an attachment at the end of this document)*

j. UAS operations within Class C and D airspace are prohibited. unless the LEA has a Letter of Agreement (LOA)/procedure with the controlling ATC facility, the ATC facility has given the proponent specific approval to operate without a transponder at the time of the notification of the operation, two-way communications are maintained with the ATC for the duration of the UAS operation, and the UAS is configured with an independent flight termination system.

k. The PIC or his designee will monitor Universal Communications (UNICOM) or appropriate ATC frequencies during all flights. The LEA will not fly in airspace other than Class G inside the area of jurisdiction without the approval of the managing ATC facility.

l. The PIC will maintain two-way radio communications when flying within five nautical miles of an operational control tower. During the period of time a control tower is closed, the PIC will monitor the appropriate UNICOM or Common Traffic Advisory Frequency (CTAF). Operations will not be conducted within a one-half-mile radius of noncontrolled airports, heliports or water landing areas without ATC or airport management approval.

m. For operations within 5 NM from any airport or heliport, the PIC shall hold, at a minimum, an FAA private pilot certificate.

n. In accordance with 14 CFR § 91.3 and § 91.111, the PIC is responsible at all times for collision avoidance with other aircraft and the safety of all operations, persons and property. In the event of a potential conflict with other aircraft, the PIC will immediately terminate the flight and land the UAS to ensure safety. LEA will not conduct UAS flight operations if a manned LEA aircraft is operating within the "Defined Incident Perimeter."

o. The PIC must coordinate with the ATC facility having jurisdiction over the airspace above the "Defined Incident Perimeter" no less than 2 hours prior to commencement of flight operations for routine (noncritical and training) missions and normally 60 minutes, but no less than 30 minutes, for missions requiring critical/immediate response.

V. Requirements

It is understood that because of the immediacy of some tactical operations, the timeliness of Notice to Airmen (NOTAM) notification may need to be reduced to accommodate the criticality of the mission. For those missions where response to the event is critical, a distance (D) NOTAM must be filed with ATC no later than 1 hour prior to commencing UAS flight operations. This NOTAM must provide:

a. Name and contact data of entity conducting UAS operations.
b. Location and altitude of the specific operating area ("defined incident perimeter").
c. Name of PIC.
d. Time and nature of the UAS activity.

Additionally, to use the 1-hour notification timeframe for these critical operations, the proponent must place a notice in the Airport Facility Directory (AFD) advising of the possibility of Unmanned Aircraft Operations in the operational area during the period of time this COA is valid. Until the AFD entry is published, the 48-hour minimum NOTAM requirement remains in effect, unless otherwise authorized. For all UAS missions NOT classified as a critical or immediate response (e.g., currency/proficiency or training missions), a distance (D) NOTAM shall be issued 48 to 72 hours prior to normal unmanned aircraft operations being conducted.

An LEA does not need to file a NOTAM for a specific mission if it is detennined that issuing the NOTAM could reasonably place the safety of officers or the success of the mission at jeopard y. Such determinat ion shall be documented in the UAS flight log. Immediate, critical operations below 100 feet AGL, not exceeding 15 minutes in duration, are authorized provided a notice of UAS operations within the jurisdiction has been published in the AFD, UAS operations will not commence within 5 NMs of an airport or heliport without ATC coordination, and UAS operations are not being conducted within Class B airspace. The proponent must contact the appropriate ATC facility prior to the operation to obtain approval.

VI. Formal Training Program

a. Each LEA shall establish a training program that addresses the initial and refresher training of all pilots and observers assigned to the UAS program, crew members, or individuals who may be used for missions of the LEA UAS program. The training program will include the identification/location of a UAS training site that is confined to Class G airspace remaining well clear (as specified in the minimum requirements of 14 CFR § 91.1 19) of housing areas, roads, and any persons or watercraft within the specific operating location. This training site will be used for the development and exercising of scenarios that address the utilization of the UAS technology integrated with other internal and external agencies and organizations that may use the UAS technology for operational missions.

b. Each LEA's formal training program for UAS crew members and grou nd crew will concentrate on scenario based training exercises that focus on, but are not limited to; Standard Operating Procedures (SOP), Crew Resource Management (CRM), emergency and abnormal procedures, and coordination and communication between operational elements. All pilot, observer and crew member training must be fonnally documented, including initial manufacturer training and LEA training and currency. Instructors and evaluators must be designated by LEA in writing, including manufacturer personnel.

c. Initially, the COA will restrict LEA UAS operations to the training and evaluation of LEA pilots, observers and crew members using the UAS technology. When the LEA believes its personnel are sufficiently proficient to safely conduct LEA operational missions, the LEA will request the *FAA* to conduct a thorough program review, including a review of all training records, flight manuals, standard operating procedures and other supporting program documentation. The FAA will work to conduct an onsite evaluation of a LEA UAS exercise to demonstrate the competency and safety of the LEA UAS program and the coordination and control among LEA supporting elements within 30 days of notification by the agency. After a successful program review and evaluation by the FAA of an actual exercise for safety and competency, the FAA will issue an operational COA approving UAS operation within the jurisdictional boundaries. It is understood that training of ATC personnel may need to precede the implementation of the COA.

VII. Standard Operating Procedures

SOPs are essential to the successful growth and maturity of a safe program. LEAs must create, distribute, implement and provide training on UAS SOPs for each phase of flight operation from notification for deployment through preflight, launch, recovery, postflight and mission recordkeeping. Effective SOPs must include, at a minimum, emergency procedures and standards for expected scenarios (e.g., lost link, lost communications between observers and the (PIC) or between the PIC and the ATC, medical emergencies), CRM, sterile cockpit protocols, standard communications between the PIC and the observer, and any special mitigation procedures.

VIII. Safety/Mission Analysis

a. In an effort to assist NIJ in gathering technology application data regarding the integration of UAS in the NAS, the LEA will provide NIJ with an Unmanned Aircraft Aviation Operations Report (AOR) that includes the description of the operations; the areas of operations, the nature, dates and flight durations of the missions; and any system malfunctions, discrepancies or incidents (e.g., lost communications, lost link, flyaway or unintentional termination of flight where no damage was sustained by the UAS, CRM breakdowns, UAS issues) noted during a mission. Additionally, to assist the FAA in gathering safety data regarding the integration of UAS in the NAS, the AOR will include a "Lessons Learned" section that contains specific issues experienced or discovered during each UAS flight operation (training or operational). This reporting requirement is in addition to the requirements related to incident/accident and normal operational reporting provisions currently required on all COAs.

b. In the event of a UAS accident or incident (i.e., damage to property, the UAS or other aircraft; injury to persons; or fatality), the LEA shall immediately notifY the appropriate regional FAA office and the UAS fntegration Office via the Washington Operations Control Center at 202-493-4170 or 202-267-3333, and provide the LEA activity name, address and contact information, date, time, location, and UAS nomenclature, along with a brief preliminary description of the circumstances. A summary response will be provided to FAA via the COA online procedures.

PART 2 — FAA Administrative Strategy Supporting Streamlined UAS Authorization Process

I. **LEA-Centric Streamlined COA Application** Process

a. In order for LEAs to achieve more rapid authorization for the employment of UAS technology within their respective jurisdictions, the current COA authorization process may be restructured or "streamlined" to address unique LEA operational constraints which would permit LEAs to provide only specific operational and administrative information in the online filing of the COA application. This streamlined process would recognize an acceptable, predefined, UAS description, performance characteristics and operational avionics/equipment technologies verified by an approved third party testing organization. These approved teclmologies would be contained and maintained within a data library contained and updated within a DOJ and/or DHS online library.

b. The particular UAS to be employed would be selectable via the library. The "streamlined" LEA-unique CO/\ authorization process would also include standardized operational elements. LEAs would be required to formally acknowledge their agreement to accept and abide by preapproved operational guidelines that would include predetermined flight operations processes, procedural and operating limitations or restrictions, pilot and observer qualifications, a LEA certification airworthiness statement, and qualification/remedial/recurring training and recordkeeping. These processes, procedures and operating limitations/restrictions would be standardized, would apply to all LEAs, and would be similar to mitigation provisions already imposed in various other UAS COA approvals.

Section 7

Federal Aviation Administration

Press Release – FAA Releases Unmanned Aircraft Systems Integration Roadmap

For Immediate Release

November 7, 2013
Contact: Les Dorr or Alison Duquette
Phone: (202) 267-3883

Also Finalizes Privacy Policy for UAS Test Sites

WASHINGTON –The U.S. Department of Transportation's Federal Aviation Administration (FAA) today released its first annual Roadmap outlining efforts needed to safely integrate unmanned aircraft systems (UAS) into the nation's airspace. The Roadmap addresses current and future policies, regulations, technologies and procedures that will be required as demand moves the country from today's limited accommodation of UAS operations to the extensive integration of UAS into the NextGen aviation system in the future.

"Government and industry face significant challenges as unmanned aircraft move into the aviation mainstream," said U.S. Transportation Secretary Anthony Foxx. "This Roadmap is an important step forward that will help stakeholders understand the operational goals and safety issues we need to consider when planning for the future of our airspace."

The Roadmap outlines the FAA's approach to ensuring that widespread UAS use is safe, from the perspective of accommodation, integration, and evolution. The FAA's main goal for integration is to establish requirements that UAS operators will have to meet in order to increase access to airspace over the next five to 10 years. The Roadmap discusses items such as new or revised regulations, policies, procedures, guidance material, training and understanding of systems and operations to support routine UAS operations.

"The FAA is committed to safe, efficient and timely integration of UAS into our airspace," said FAA Administrator Michael Huerta. "We are dedicated to moving this exciting new technology along as quickly and safely as possible."

The Roadmap also addresses the evolution of UAS operations once all requirements and standards are in place and are routinely updated to support UAS operations as the National Airspace System evolves over time. The document stresses that the UAS community must understand the system is not static, and that many improvements are planned for the airspace system over the next 15 years.

The FAA plans to select six UAS test sites to begin work on safely integrating UAS into the airspace. These congressionally-mandated test sites will conduct critical research into how best to safely integrate UAS systems into the national airspace over the next several years and what certification and navigation requirements will need to be established.

The use of UAS, both at the designated test sites and in the national airspace generally, raises the issue of privacy and protection of civil liberties. In February, the FAA asked for public comments specifically on the draft privacy requirements for the six test sites. Today, the agency sent a final privacy policy to the *Federal Register* that requires test site operators to comply with federal, state, and other laws on individual privacy protection, to have a publicly available privacy plan and a written plan for data use and retention, and to conduct an annual review of privacy practices that allows for public comment. Information about the test site selection process and final test site privacy policy is available at: http://www.faa.gov/about/initiatives/uas/ (http://www.faa.gov/about/initiatives/uas/)

For the next several years, the FAA will continue to use special mitigations and procedures to safely accommodate limited UAS access to the nation's airspace on a case-by-case basis. The Roadmap notes that this case-by-case accommodation will decline significantly as integration begins and expands, but will continue to be a practical way to allow flights by some UAS operators in certain circumstances.

In addition to the FAA's Roadmap, as required in the 2012 FAA Reauthorization, the Joint Planning and Development Office (JPDO) has developed a comprehensive plan to safely accelerate the integration of civil UAS into the national airspace system.. That plan details a multi-agency approach to safe and timely UAS integration and coordination with the NextGen shift to satellite-based technologies and new procedures.

The UAS Roadmap (http://www.faa.gov/about/initiatives/uas/media/UAS_Roadmap_2013.pdf) (PDF) and UAS Comprehensive Plan (http://www.faa.gov/about/office_org/headquarters_offices/agi/reports/media/UAS_Comprehensive_Plan.pdf) is available on our website.

:

###

This page can be viewed online at: http://www.faa.gov/news/press_releases/news_story.cfm?newsId=15334

U.S. Department
of Transportation
**Federal Aviation
Administration**

Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap

First Edition – 2013

November 7, 2013

Dear Members of the Aviation Community:

I am pleased to present the Federal Aviation Administration's (FAA) Roadmap for *Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS).* The FAA and the UAS Aviation Rulemaking Committee (ARC) worked together for the past year to produce this roadmap. Unmanned aircraft offer new ways for commercial enterprises and public operators to increase operational efficiency, decrease costs, and enhance safety; and this roadmap will allow us to safely and efficiently integrate them into the NAS.

The FAA is committed to the safe and efficient integration of UAS into the NAS. However, as safety is our top priority, UAS integration must be accomplished without reducing existing capacity, decreasing safety, impacting current operators, or placing other airspace users or persons and property on the ground at increased risk. We have made great progress in accommodating public UAS operations, but challenges remain for the safe, long-term integration of both public and civil UAS in the NAS.

This roadmap outlines the actions and considerations needed to enable UAS integration into the NAS. The roadmap also aligns proposed FAA actions with Congressional mandates from the *FAA Modernization and Reform Act of 2012.* This plan also provides goals, metrics, and target dates for the FAA and its government and industry partners to use in planning key activities for UAS integration.

We will update the specific implementation details (goals, metrics, target dates) as we learn from our current UAS operations, leverage ongoing research, and incorporate the work of our government and industry partners in all related areas.

Thank you for your continued support and active participation in the safe and efficient integration of UAS in the NAS.

Michael P. Huerta
Administrator

Table of Contents

Executive Summary 4

1 Purpose and Background of Civil UAS Roadmap 6

1.1 History of UAS 7

1.2 Proposed Civil and Commercial Applications 7

1.3 Definitions 8

1.4 Policy 9

1.4.1 FAA UAS Policy Basis 9

1.4.2 International Civil Aviation Organization (ICAO) Policy 10

1.4.3 Industry Policy Recommendations 11

1.4.4 Privacy and Civil Liberties Considerations 11

1.4.5 National Security Issues 12

2 UAS Operations in the NAS 14

2.1 FAA's Dual Role for UAS Integration 14

2.2 UAS Challenges 14

2.2.1 Policy, Guidance, and Regulatory Product Challenges 14

2.2.2 Air Traffic Operational Challenges 17

2.2.3 Technological Challenges 18

2.2.4 Managing the Challenges 20

3 Perspective 1: Accommodation 22

3.1 Overview 22

3.2 Standards 23

3.3 Rules and Regulations 24

3.4 Airworthiness Certification of the UAS 25

3.5 Procedures and Airspace 27

3.6 Training (Pilot, Flightcrew Member, Mechanic, and Air Traffic Controller) 28

3.7 Research and Development (R&D) / Technology 28

4 Perspective 2: Integration 32

4.1 Overview 32

4.2 Standards 34

4.3 Rules and Regulations 34

4.4 Airworthiness Certification of the UAS 34

4.5 Procedures and Airspace 35

4.6 Training (Pilot, Flightcrew Member, Mechanic, and Air Traffic Controller) 35

4.7 Research and Development (R&D) /Technology 36

4.8 Test Ranges 37

5 Perspective 3: Evolution 38

5.1 Overview 38

5.2 Standards 38

5.3 Rules and Regulations 38

5.4 Airworthiness Certification of the UAS 38

5.5 Procedures and Airspace 39

5.6 Training (Pilot, Flightcrew Member, Mechanic, and Air Traffic Controller) 39

5.7 Research and Development (R&D) / Technology 39

6 Conclusions 42

6.1 Summary 42

6.2 Outlook 42

Appendix A: Acronyms 44

Appendix B: Glossary 46

Appendix C: Goals, Metrics, and Target Dates 50

C.1 Certification Requirements (Airworthiness) 51

C.2 Certification Requirements (Pilot/Crew) 52

C.3 Ground Based Sense and Avoid (GBSAA) 53

C.4 Airborne Sense and Avoid (ABSAA) 54

C.5 Control and Communications (C2) 56

C.6 Small UAS (sUAS) and Other Rules 58

C.7 Test Ranges 60

C.8 Air Traffic Interoperability 60

C.9 Miscellaneous 61

Appendix D: FAA Modernization and Reform Act of 2012 Reference Text 66

Executive Summary

Expanding Operations of Unmanned Aircraft Systems in the NAS

Since the early 1990s, unmanned aircraft systems (UAS) have operated on a limited basis in the National Airspace System (NAS). Until recently, UAS mainly supported public operations, such as military and border security operations. The list of potential uses is now rapidly expanding to encompass a broad range of other activities, including aerial photography, surveying land and crops, communications and broadcast, monitoring forest fires and environmental conditions, and protecting critical infrastructures. UAS provide new ways for commercial enterprises (civil operations) and public operators to enhance some of our nation's aviation operations through increased operational efficiency and decreased costs, while maintaining the safety of the NAS.

As stated in *Destination 2025* (2011):

> *"The Federal Aviation Administration's (FAA) mission is to provide the safest, most efficient aviation system in the world. What sets the United States apart is the size and complexity of our infrastructure, the diversity of our user groups, our commitment to safety and excellence, and a history of innovation and leadership in the world's aviation community. Now we are working to develop new systems and to enhance a culture that increases the safety, reliability, efficiency, capacity, and environmental performance of our aviation system."*

Ultimately, UAS must be integrated into the NAS without reducing existing capacity, decreasing safety, negatively impacting current operators, or increasing the risk to airspace users or persons and property on the ground any more than the integration of comparable new and novel technologies.

The FAA created the Unmanned Aircraft Systems Integration Office to facilitate integration of UAS safely and efficiently into the NAS. Toward that goal, the FAA is collaborating with a broad spectrum of stakeholders, which includes manufacturers, commercial vendors, industry trade associations, technical standards organizations, academic institutions, research and development centers, governmental agencies, and other regulators. Ultimately, UAS must be integrated into the NAS without reducing existing capacity, decreasing safety, negatively impacting current operators, or increasing the risk to airspace users or persons and property on the ground any more than the integration of comparable new and novel technologies. Significant progress has been made toward UAS-NAS integration, with many challenges and opportunities ahead.

A key activity of the FAA is to develop regulations, policy, procedures, guidance material, and training requirements to support safe and efficient UAS operations in the NAS, while coordinating with relevant departments and agencies to address related key policy areas of concern such as privacy and national security. Today, UAS are typically given access to airspace through the issuance of Certificates of Waiver or Authorization (COA) to public operators and special airworthiness certificates in the experimental category for civil applicants. Accommodating UAS operations by the use of COAs and special airworthiness certificates will transition to more routine integration processes when new or revised operating rules and procedures are in place and UAS are capable of complying with them. The FAA has a proven certification process in place for aircraft that includes establishing special conditions when new and unique technologies are involved. This process will be used to evaluate items unique to UAS. In those parts of the NAS that have demanding communications, navigation, and surveillance performance requirements, successful demonstration of UAS to meet these requirements will be necessary.

The process of developing regulations, policy, procedures, guidance material, and training requirements, is resource-intensive. This roadmap will illustrate the significant undertaking it is to build the basis for the NAS to transition from UAS *accommodation* to UAS *integration.* Government and industry stakeholders must work collaboratively and apply the necessary resources to bring this transition to fruition while supporting evolving UAS operations in the NAS.

The purpose of this roadmap is to outline, within a broad timeline, the tasks and considerations needed to enable UAS integration into the NAS for the planning purposes of the broader UAS community. The roadmap also aligns proposed Agency actions with the Congressional mandate in the *FAA Modernization and Reform Act of 2012,* Pub. L. 112-95. As this is the first publication of this annual document, the FAA will incorporate lessons learned and related findings in subsequent publications, which will include further refined goals, metrics, and target dates.

The FAA is committed to the safe and efficient integration of UAS into the NAS, thus enabling this emerging technology to safely achieve its full potential.

Purpose and Background of Civil UAS Roadmap

1 Purpose and Background of Civil UAS Roadmap

Unmanned aircraft systems (UAS) and operations have significantly increased in number, technical complexity, and sophistication during recent years without having the same history of compliance and oversight as manned aviation. Unlike the manned aircraft industry, the UAS community does not have a set of standardized design specifications for basic UAS design that ensures safe and reliable operation in typical civilian service applications. As a result, the UAS community often finds it difficult to apply existing FAA guidance. In some cases, interpretation of regulations and/or standards may be needed to address characteristics unique to UAS. Ultimately, the pace of integration will be determined by the ability of industry, the user community, and the FAA to overcome technical, regulatory, and operational challenges. The purpose of this roadmap is to outline, within a broad timeline, the tasks and considerations needed to enable UAS integration into the National Airspace System (NAS) for the planning purposes of the broader UAS community. The roadmap also aligns proposed Agency actions with the Congressional mandate in the *FAA Modernization and Reform Act of 2012,* Pub. L. 112-95.

> To gain full access to the NAS, UAS need to be able to bridge the gap from existing systems requiring accommodations to future systems that are able to obtain a standard airworthiness certificate

This five-year roadmap, as required by the *FAA Modernization and Reform Act of 2012* (FMRA), is intended to guide aviation stakeholders in understanding operational goals and aviation safety and air traffic challenges when considering future investments. The roadmap is organized into three perspectives that highlight the multiple paths used to achieve the milestones outlined, while focusing on progressive accomplishments. These three perspectives — *Accommodation, Integration,* and *Evolution* — transcend specific timelines and examine the complex relationship of activities necessary to integrate UAS into the NAS. These three perspectives will be explored in more detail in Section 2.2.4.

Although the FMRA requires a five-year UAS roadmap, it is important to view UAS-NAS integration not only in terms of near-term activities and objectives, but also in the context of mid- and long-term timeframes. The timeframes used in this roadmap are defined in the President's National Aeronautics Research and Development Plan, which specifies less than 5 years as the near-term, 5-10 years as the mid-term, and greater than 10 years as the long-term. For this roadmap, the long-term is defined as

1

2022-2026, which is consistent with the Joint Planning and Development Office (JPDO) *National Airspace System Concept of Operations and Vision for the Future of Aviation and NextGen Air Transportation System Integrated Plan.*

Integration of UAS into the NAS will require: review of current policies, regulations, environmental impact, privacy considerations, standards, and procedures; identification of gaps in current UAS technologies and regulations, standards, policies, or procedures; development of new technologies and new or revised regulations, standards, policies, and procedures; and the associated development of guidance material, training, and certification of aircraft systems, propulsion systems, and airmen. The FAA will coordinate these integration activities with other United States Government agencies, as needed, through the Interagency Planning Committee (IPC).

1.1 History of UAS

Historically, unmanned aircraft have been known by many names including: "drones," "remotely piloted vehicles (RPV)," "unmanned aerial vehicles (UAV)," "models," and "radio control (R/C) aircraft." Today, the term UAS is used to emphasize the fact that separate system components are required to support airborne operations without a pilot onboard the aircraft. Early UAS operations received little attention from the FAA and its predecessor agencies due to the infrequency of operations, which were mostly conducted in remote locations or in special use airspace and were not deemed to impact the safety of the NAS. In the past two decades, the number of unmanned aircraft operations has been increasing dramatically, highlighting the need for a structured approach for safe and efficient integration.

1.2 Proposed Civil and Commercial Applications

The use of UAS in commercial applications is expected to expand in a number of areas (see Operational Services and Environment Definition (OSED) for Unmanned Aircraft Systems (UAS), RTCA DO-320, 2010). Some of the currently proposed civil and commercial applications of UAS include:

- Security awareness;
- Disaster response, including search and support to rescuers;
- Communications and broadcast, including news/sporting event coverage;
- Cargo transport;
- Spectral and thermal analysis;
- Critical infrastructure monitoring, including power facilities, ports, and pipelines;
- And commercial photography, aerial mapping and charting, and advertising.

1.3 Definitions

Several terms used in this document are defined below as a common point of reference:

Unmanned Aircraft (UA): A device used or intended to be used for flight in the air that has no onboard pilot. This device excludes missiles, weapons, or exploding warheads, but includes all classes of airplanes, helicopters, airships, and powered-lift aircraft without an onboard pilot. UA do not include traditional balloons (see 14 CFR Part 101), rockets, tethered aircraft and un-powered gliders.

Crewmember [UAS]: In addition to the crewmembers identified in 14 CFR Part 1, a UAS flightcrew member includes pilots, sensor/payload operators, and visual observers (VO), but may include other persons as appropriate or required to ensure safe operation of the aircraft.

Unmanned Aircraft System (UAS): An unmanned aircraft and its associated elements related to safe operations, which may include control stations (ground, ship, or air-based), control links, support equipment, payloads, flight termination systems, and launch/recovery equipment. As shown in Figure 1, it consists of three elements:

- Unmanned Aircraft;
- Control Station;
- And Data Link.

National Airspace System (NAS): The common network of U.S. airspace — air navigation facilities, equipment, and services; airports or landing areas; aeronautical charts, information and services; rules, regulations, and procedures; technical information; and manpower and material. (see Figure 2)

Next Generation Air Transportation System (NextGen): According to the FAA's *Destination 2025,* (2011):

> *"NextGen is a series of inter-linked programs, systems, and policies that implement advanced technologies and capabilities to dramatically change the way the current aviation system is operated. NextGen is satellite-based and relies on a network to share information and digital communications so all users of the system are aware of other users' precise locations."*

Unmanned Aircraft System (UAS)

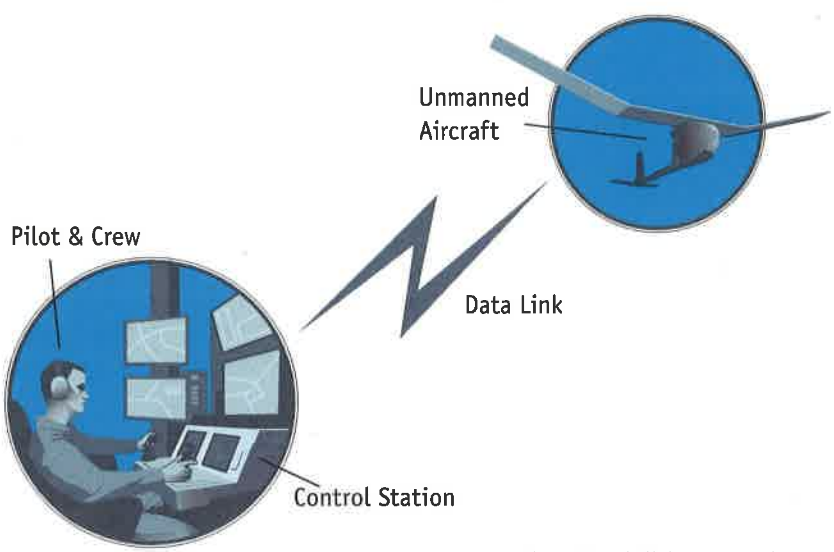


Figure 1: The UAS and Flightcrew Members

1.4 Policy

The FAA is responsible for developing plans and policy for the safe and efficient use of the United States' navigable airspace. This responsibility includes coordinating efforts with national security and privacy policies so that the integration of UAS into the NAS is done in a manner that supports and maintains the United States Government's ability to secure the airspace and addresses privacy concerns. Further, the FAA will harmonize, when appropriate, with the international community for the mutual development of civil aviation in a safe and orderly manner. Components of existing FAA and International Civil Aviation Organization (ICAO) policy are outlined below.

National Airspace System

Figure 2: The NAS

1.4.1 FAA UAS Policy Basis

Established FAA aviation policies support an acceptable level of safety for the NAS. At the core of these policies is the concept that each aircraft is flown by a pilot in accordance with required procedures and practices. This same policy applies to UAS.

Aviation policies and regulations focus on overall safety being addressed through three primary areas: equipment, personnel, and operations and procedures. Each of these areas has standards and minimum levels of safety that must be met, independent of each other. As a matter of regulation, for example, a new civil aircraft must be able to independently obtain an airworthiness certificate, regardless of the airspace class where it might be flown. However, as a result or part of this certification, new procedures may be required for flightcrew members and air traffic control (ATC) in order to maintain the minimum level of safety of the NAS while accommodating the new technology. Under special certifications and authorizations, limited operations may be authorized for equipment unable to meet current standards.

The application of these established aviation policies to UAS is summarized in the following key points excerpted from the FAA Notice of Policy: Unmanned Aircraft Operations in the National Airspace System (72 Fed. Reg. 6689 (Feb. 13, 2007)):

- Regulatory standards need to be developed to enable current technology for unmanned aircraft to comply with Title 14 Code of Federal Regulations;

- In order to ensure safety, the operator is required to establish the UAS airworthiness either from FAA certification, a Department of Defense (DoD) airworthiness statement, or by other approved means;
- Applicants also have to demonstrate that a collision with another aircraft or other airspace user is extremely improbable;
- And the pilot-in-command concept is essential to the safe operation of manned operations. The FAA's UAS guidance applies this pilot-in-command concept to unmanned aircraft and includes minimum qualification and currency requirements.

These policies have enabled the accommodation of UAS into the NAS on a limited basis on the foundation that operations are conducted safely, present an acceptable level of risk to the general public, and do no harm to, or adversely impact, other users. To gain full access to the NAS, UAS need to be able to bridge the gap from existing systems requiring accommodations to future systems that are able to obtain a standard airworthiness certificate. These UAS will also need to be flown by a certified pilot in accordance with existing, revised, or new regulations and required standards, policies, and procedures.

1.4.2 International Civil Aviation Organization (ICAO) Policy

ICAO, a special agency of the United Nations, promotes "the safe and orderly development of international civil aviation throughout the world. It sets standards and regulations necessary for aviation safety, security, efficiency, and regularity, as well as aviation environmental protection."

The goal of ICAO in addressing unmanned aviation is to provide the fundamental international regulatory framework to support routine operation of UAS throughout the world in a safe, harmonized, and seamless manner comparable to that of manned operations. Current ICAO guidance material for UAS is published in ICAO Circular 328, "Unmanned Aircraft Systems (UAS) Circular," which provides basic guidelines for Member States to introduce and integrate UAS into airspace in a consistent manner, to ensure global interoperability and regulatory compatibility, when possible. The document's guiding policy on UAS is:

> *"A number of Civil Aviation Authorities (CAA) have adopted the policy that UAS must meet the equivalent levels of safety as manned aircraft… In general, UAS should be operated in accordance with the rule governing the flight of manned aircraft and meet equipment requirements applicable to the class of airspace within which they intend to operate…To safely integrate UAS in non-segregated airspace, the UAS must act and respond as manned aircraft do. Air Traffic, Airspace and Airport standards should not be significantly changed. The UAS must be able to comply with existing provisions to the greatest extent possible."*

ICAO develops Standards and Recommended Practices (SARP), which are generally followed by national civil aviation authorities of the Member States. The United States is an ICAO Member State, and the FAA plans to harmonize with international efforts and adhere to ICAO SARPs when possible.

1.4.3 Industry Policy Recommendations

RTCA, Inc. is a private, not-for-profit corporation that develops consensus-based recommendations regarding communications, navigation, surveillance, and air traffic management system issues. RTCA functions as a Federal Advisory Committee, and the FAA considers RTCA recommendations when making policy, program, and regulatory decisions. RTCA Special Committee 203 (SC-203) was established in 2004 to help assure the safe, efficient, and compatible operation of UAS with other aircraft operating within the NAS. This Special Committee has developed and documented guiding principles for UAS integration, which are summarized below:

- UAS must operate safely, efficiently, and compatibly with service providers and other users of the NAS so that overall safety is not degraded;
- UAS will have access to the NAS, provided they have appropriate equipage and the ability to meet the requirements for flying in various classes of airspace;
- Routine UAS operations will not require the creation of new special use airspace, or modification of existing special use airspace;
- Except for some special cases, such as small UAS (sUAS) with very limited operational range, all UAS will require design and airworthiness certification to fly civil operations in the NAS;
- UAS pilots will require certification, though some of the requirements may differ from manned aviation;
- UAS will comply with ATC instructions, clearances, and procedures when receiving air traffic services;
- UAS pilots (the pilot-in-command) will always have responsibility for the unmanned aircraft while it is operating;
- And UAS commercial operations will need to apply the operational control concept as appropriate for the type of operation, but with different functions applicable to UAS operations.

Through an FAA-established UAS Aviation Rulemaking Committee (ARC), the FAA continues to collaborate with government and industry stakeholders for recommendations regarding the path toward integration of UAS into the NAS. This effort will harmonize with the work being done by international organizations working toward a universal goal of safe and efficient UAS airspace operations.

1.4.4 Privacy and Civil Liberties Considerations

The FAA's chief mission is to ensure the safety and efficiency of the entire aviation system. This includes manned and unmanned aircraft operations. While the expanded use of UAS presents great opportunities, it also raises questions as to how to accomplish UAS integration in a manner that is consistent with privacy and civil liberties considerations.

As required by the FMRA, the FAA is implementing a UAS test site program to help the FAA gain a better understanding of operational issues relating to UAS. Although the FAA's mission does not include developing or enforcing policies pertaining to privacy or civil liberties, experience with the UAS test sites will present an opportunity to inform the dialogue in the IPC and other interagency forums concerning the use of UAS technologies and the areas of privacy and civil liberties.

As part of the test site program, the FAA will authorize non-federal public entities to establish and operate six test sites in the United States. The FAA recognizes that there are privacy considerations regarding the use of UAS at the test sites. To ensure that these concerns are taken into consideration at the test sites, the FAA plans to require each test site operator to establish a privacy policy that will apply to operations at the test site. The test site's privacy policy must be publicly available and informed by Fair Information Practice Principles. In addition, each site operator must establish a mechanism through which the operator can receive and consider comments on its privacy policy.

The privacy requirements proposed for the UAS test sites are specifically designed for the operation of the test sites and are not intended to predetermine the long-term policy and regulatory framework under which UAS would operate. However, the FAA anticipates that the privacy policies developed by the test site operators will help inform the dialogue among policymakers, privacy advocates, and the industry regarding broader questions concerning the use of UAS technologies in the NAS.

1.4.5 National Security Issues

Integrating public and civil UAS into the NAS carries certain national security implications, including security vetting for certification and training of UAS-related personnel, addressing cyber and communications vulnerabilities, and maintaining/enhancing air defense and air domain awareness capabilities in an increasingly complex and crowded airspace. In some cases, existing security frameworks applied to manned aircraft may be applicable. Other security concerns may require development of new frameworks altogether. The FAA will continue to work with relevant United States Government departments and agencies, and with stakeholders through coordinating bodies such as the IPC and JPDO, to proactively address these areas of concern.

UAS Operations in the NAS

This roadmap focuses on civil UAS access to the NAS. To this end, the FAA and the UAS community are working to address the myriad challenges associated with this effort.

2.1 FAA's Dual Role for UAS Integration

For UAS, as with all aircraft, the FAA acts in a dual role. As the regulator, the FAA ensures aviation safety of persons and property in the air and on the ground. As the service provider, the FAA is responsible for providing safe and efficient air traffic control services in the NAS and the other portions of global airspace delegated to the United States by ICAO.

As part of its regulator role, the Office of Aviation Safety (AVS) efforts are led by the UAS Integration Office. The main focus of the UAS Integration Office is to provide, within the existing AVS structure, subject matter expertise, research, and recommendations to develop policy, regulations, guidance, and procedures for UAS airworthiness and operations in support of safe integration of UAS into the NAS.

As the service provider, the Air Traffic Organization (ATO) efforts are led by the Air Traffic Emerging Technologies Group, which considers operational authorizations for UAS flights that are unable to meet current regulations and procedures. A Certificate of Waiver or Authorization (COA) is issued with limitations and provisions that mitigate the increased risks resulting from the use of uncertified technology. The ATO is responsible for the safe and efficient handling of aircraft and the development of the airspace rules, procedures, and air traffic controller training to support routine operations in the NAS.

2.2 UAS Challenges

A number of issues that impact the integration of UAS into the NAS are being considered across the regulatory and service provider roles of the FAA. To ensure the FAA meets the goals set forth in this roadmap, these offices will be addressing the challenges as outlined in the following subsections.

2.2.1 Policy, Guidance, and Regulatory Product Challenges

To ensure the FAA has the appropriate UAS framework, many policy, guidance, and regulatory products will need to be reviewed and revised to specifically address UAS integration into the NAS. UAS technology and operations will need to mature, and new products may be required in order to meet applicable regulations and standards. Figure 3 depicts policy, guidance, and regulatory product areas requiring research and development. This information is derived from the RTCA notional architecture and is primarily related to airmen and UAS certification.

2

Performance Baseline
UAS Integration

Pilot & Crew

- Policy
- Certification Requirements
- Operational Standards
- Procedures
- Regulations
- Guidance Material
- Training Requirements
- Medical Standards
- Testing Standards

Control Station

- Policy
- Certification Requirements
- Technical Standards
- Airworthiness Standards
- Regulations
- Interoperability Requirements
- Guidance Material
- Continued Airworthiness
- Means of Compliance

Data Link

- Policy
- Certification Requirements
- Technical Standards
- Airworthiness Standards
- Interoperability Requirements
- Guidance Material
- Coordinated Aviation Radiofrequency Spectrum
- Standardized Control Architectures
- Measures of Performance
- Radio/DataLink Security Requirements

Unmanned Aircraft

- Policy
- Certification Requirements
- Technical Standards
- Airworthiness Standards
- Procedures
- Regulations
- Guidance Material
- Measures of Performance
- Continued Airworthiness
- Testing Standards
- Means of Compliance

Figure 3: AVS Products to Regulate UAS Operations

The challenge is to identify and develop the UAS regulatory structure that encompasses areas listed in Figure 3. Other regulatory drivers include:

- Developing minimum standards for Sense and Avoid (SAA), Control and Communications (C2), and separation assurance to meet new or existing operational and regulatory requirements for specified airspace;
- Understanding the privacy, security, and environmental implications of UAS operations and working with relevant departments and agencies to proactively coordinate and align these considerations with the UAS regulatory structure;
- And developing acceptable UAS design standards that consider the aircraft size, performance, mode of control, intended operational environment, and mission criticality.

Although aviation regulations have been developed generically for all aircraft, until recently these efforts were not done with UAS specifically in mind. This presents certain challenges because the underlying assumptions that existed during the previous efforts may not now fully accommodate UAS operations. As an example, current regulations address security requirements for cockpit doors. However, these same regulations lack a legal definition for what a "cockpit" is or where it is located. This presents a challenge for UAS considering that the cockpit or "control station" may be located in an office building, in a vehicle, or outside with no physical boundaries. Applying current cockpit door security regulations to UAS may require new rulemaking, guidance, or a combination of both.

The regulatory process is designed to provide transparency to the public and an opportunity to understand and comment on proposed rules before being issued. Additional checks and balances are in place to ensure that final regulations are not unnecessarily burdensome to the public. Because of these requirements, and lacking any exceptions, an average regulatory effort might span a number of years. These timeframes may be longer for high visibility or complex regulations. FAA experience to date with the development of a Notice of Proposed Rulemaking (NPRM) for small UAS indicates that UAS rulemaking efforts may be more complex, receive greater scrutiny, and require longer development timeframes than the average regulatory effort.

2.2.2 Air Traffic Operational Challenges

Numerous Air Traffic products, policies, and procedures also need to be reviewed and refined or developed through supporting research to permit UAS operations in the NAS. The UAS Integration Office coordinates efforts with the ATO to complete these tasks.

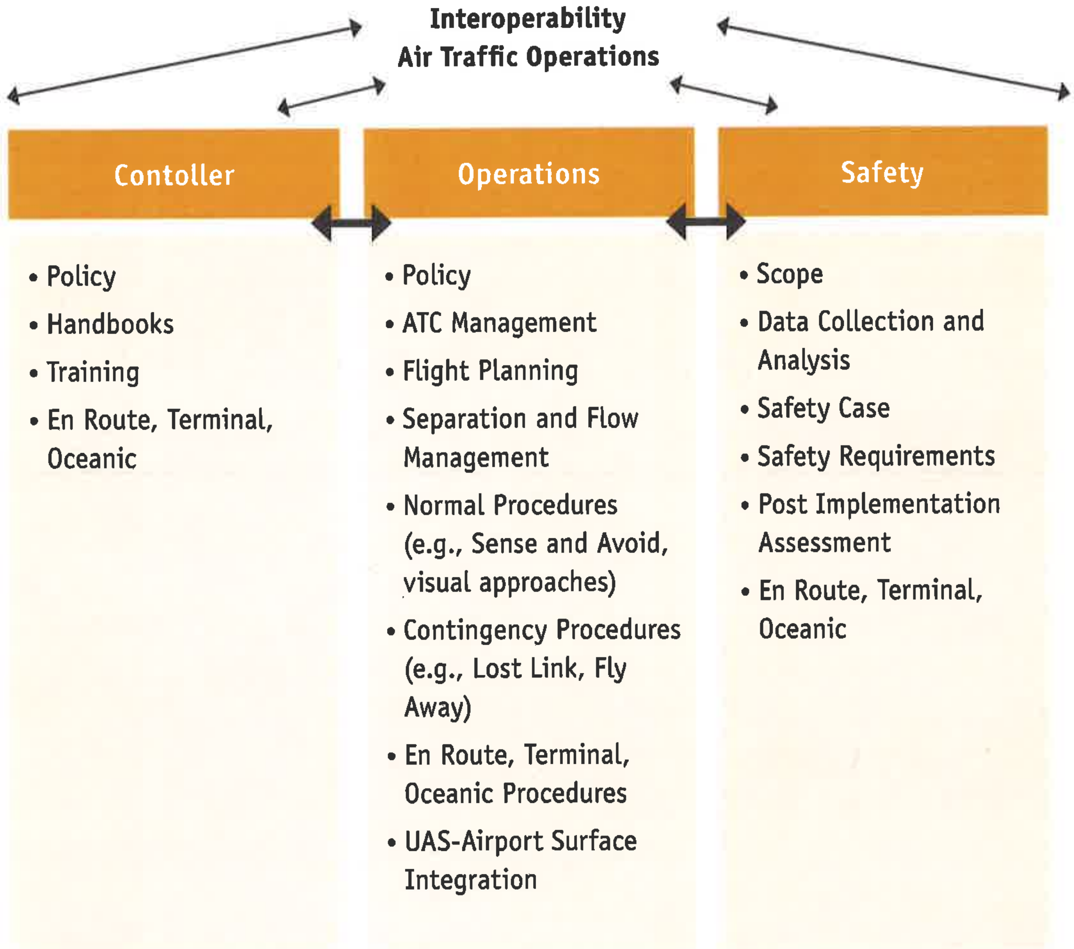


Figure 4: ATO UAS Operational Area

The goal of safely integrating UAS without segregating, delaying, or diverting other aircraft and other users of the system presents significant challenges in the areas outlined in Figure 4 above. For NAS integration, this also includes:

- Identifying policies and requirements for UAS to comply with ATC clearances and instructions commensurate with manned aircraft (specifically addressing the inability of UAS to comply directly with ATC visual clearances or to operate under visual flight rules);
- Establishing procedures and techniques for safe and secure exchange of voice and data communication between UAS pilots, air traffic controllers, and other NAS users;
- Establishing wake vortex and turbulence avoidance criteria needed for UAS with unique characteristics (e.g., size, performance, etc.);
- And reviewing environmental requirements (e.g., the National Environmental Policy Act).

2.2.3 Technological Challenges

The FAA recognizes that current UAS technologies were not developed to comply with existing airworthiness standards. Current civil airworthiness regulations may not consider many of the unique aspects of UAS operations. Materials properties, structural design standards, system reliability standards, and other minimum performance requirements for basic UAS design need to be evaluated against civil airworthiness standards for existing aircraft. Although significant technological advances have been made by the UAS community, critical research is needed to fully understand the impact of UAS operations in the NAS. There has also been little research to support the equipment design necessary for UAS airworthiness certification. In the near- to mid-term, UAS research will need to focus on technology deemed necessary for UAS access to the NAS.

As UAS are introduced, their expected range of performance will need to be evaluated for impact on the NAS. UAS operate with widely varying performance characteristics that do not necessarily align with manned aircraft performance. They vary in size, speed, and other flight capabilities. Similarly, the issue of performance gap between the pilot and the avionics will impact NAS operations. For example, a quantitative time standard for a pilot response to ATC directions (such as "turn left heading 270, maintain FL250") does not exist – there is an acceptable delay for the pilot's verbal response and physical action, but there is no documented required range of acceptable values. Avionics that perform the corresponding function cannot be designed and built without these performance requirements being established.

Existing standards ensure safe operation by pilots actually on board the aircraft. These standards may not translate well to UAS designs where pilots are remotely located off the aircraft. Removing the pilot from the aircraft creates a series of performance considerations between manned and unmanned aircraft that need to be fully researched and understood to determine acceptability and potential impact on safe operations in the NAS. These include the following considerations:

- The UAS pilot is not onboard the aircraft and does not have the same sensory and environmental cues as a manned aircraft pilot;
- The UAS pilot does not have the ability to directly comply with see-and-avoid responsibilities and UAS SAA systems do not meet current operational rules;
- The UAS pilot must depend on a data link for control of the aircraft. This affects the aircraft's response to revised ATC clearances, other ATC instructions, or unplanned contingencies (e.g., maneuvering aircraft);
- UAS cannot comply with certain air traffic control clearances, and alternate means may need to be considered (e.g., use of visual clearances);
- UAS present air traffic controllers with a different range of platform sizes and operational capabilities (such as size, speed, altitude, wake turbulence criteria, and combinations thereof);

Removing the pilot from the aircraft creates a series of performance considerations between manned and unmanned aircraft that need to be fully researched and understood to determine acceptability and potential impact on safe operations in the NAS.

- And some UAS launch and recovery methods differ from manned aircraft and require manual placement and removal from runways, a lead vehicle for taxi operations, or dedicated launch and recovery systems.

Therefore, it is necessary to develop new or revised regulations/ procedures and operational concepts, formulate standards, and promote technological development that will enable manned and unmanned aircraft to operate cohesively in the same airspace. Specific technology challenges include two critical functional areas:

- **"Sense and Avoid" (SAA) capability** must provide for self-separation and ultimately for collision avoidance protection between UAS and other aircraft analogous to the "see and avoid" operation of manned aircraft that meets an acceptable level of safety. SAA technology development is immature. In manned flight, see and avoid, radar, visual sighting, separation standards, proven technologies and procedures, and well-defined pilot behaviors combine to ensure safe operation. Unmanned flight will require new or revised operational rules to regulate the use of SAA systems as an alternate method to comply with "see and avoid" operational rules currently required of manned aircraft. SAA system standards must be developed to assure both self-separation and collision avoidance capability for UAS. Interoperability constraints must also be defined for safe and secure interactions between SAA-enabled UAS and other airborne and ground-based collision avoidance systems. While SAA may be an independent system, it must be designed to be compatible across other modes (e.g., ATC separation services). See Appendix C.3 and C.4 for specific goals and metrics.

Unmanned flight will require new or revised operational rules to regulate the use of SAA systems as an alternate method to comply with "see and avoid" operational rules currently required of manned aircraft.

- **Control and Communications (C2) system performance requirements** are needed and RTCA is developing consensus-based recommendations for the FAA to consider in C2 policy, program, and regulatory decisions. The resulting C2 requirements need to support the minimum performance required to achieve higher-level (UAS level) performance and safety requirements. Third-party communication service providers are common today (e.g., ARINC, Harris, etc.) and the FAA has experience with setting and monitoring performance of third parties. The use of third parties is dependent on the UAS architecture chosen, but these are still being evaluated in terms of feasibility from a performance, cost, and safety perspective. See Appendix C.5 for specific goals and metrics.

2.2.4 Managing the Challenges

To provide the UAS community insight into the FAA process for fostering UAS flight in the NAS, Figure 5 highlights the intended shift in focus over time from Accommodation to Integration, and then to Evolution. This method is consistent with the approach used for new technologies on manned aircraft introduced into the NAS.

Current design standards reflect the focus in the COA process on allowing existing designs, embodying some experimental design philosophies, to fly in the NAS. Progress toward standard airworthiness will also increase as design standards mature, but not before.

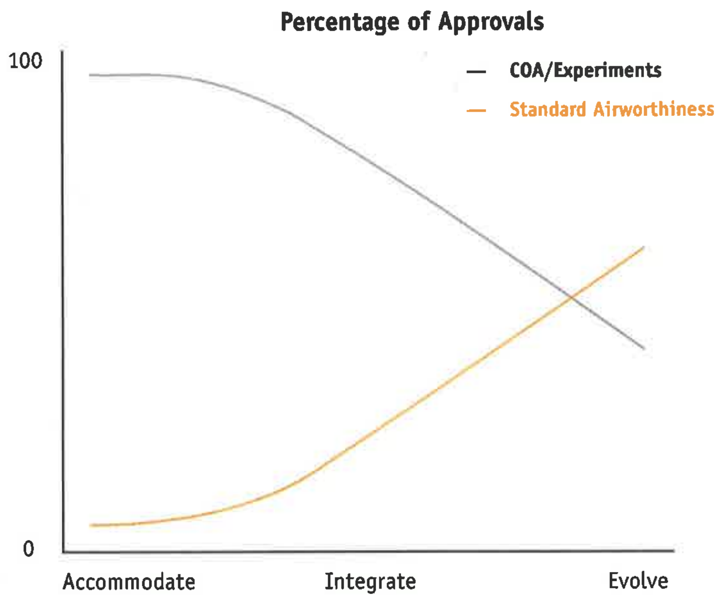


Figure 5: Transition from COA/Experimental to Standard Airworthiness Approvals

Recognizing the challenges and the complex coordination required for integration, the UAS roadmap addresses the efforts needed to move forward incrementally toward the goal of full NAS integration.

Timely progress on products, decisions, research, development, testing, and evaluation will be needed to successfully move from accommodation to integration in the evolving NAS.

The approach to managing the challenges discussed in this section focuses on the following interdependent topics:

- Standards;
- Rules and Regulations;
- Certification of the UAS;
- Procedures and Airspace;
- Training (Pilot, Flightcrew Member, Mechanic, and Controller);
- And Research and Development (R&D) and Technology.

The roadmap discusses the activities and transitions for the above interdependent topic areas from the vantage point of Accommodation, Integration, and Evolution, as summarized below and described in more detail in subsequent sections of this roadmap. These perspectives transcend the near-, mid-, and far-term timeframes and provide additional insight into the task of integrating UAS into the NAS.

Perspective 1: Accommodation. Take current UAS and apply special mitigations and procedures to safely facilitate limited access to the NAS. UAS operations in the NAS are considered on a case-by-case basis. Accommodation will predominate in the near-term, and while it will decline significantly as integration begins and expands in the mid-term, it will continue to be a viable means for NAS access with appropriate restrictions and constraints to mitigate any performance shortfalls. During the near-term, R&D will continue to identify challenges, validate advanced mitigation strategies, and explore opportunities to progress UAS integration into the NAS.

Perspective 2: Integration. Establishing threshold performance requirements for UAS that would increase access to the NAS is a primary objective of integration. During the mid- to far-term, the Agency will establish new or revised regulations, policies, procedures, guidance material, training, and understanding of systems and operations to support routine NAS operations. Integration is targeted to begin in the near- to mid-term with the implementation of the sUAS rule and will expand further over time (mid- and far-term) to consider wider integration of a broader field of UAS.

Perspective 3: Evolution. All required policy, regulations, procedures, guidance material, technologies, and training are in place and routinely updated to support UAS operations in the NAS operational environment as it evolves over time. It is important that the UAS community maintains the understanding that the NAS environment is not static, and that there are many improvements planned for the NAS over the next 13-15 years. To avoid obsolescence, UAS developers will need to maintain a dual focus: integration into today's NAS while maintaining cognizance of how the NAS is evolving.

Perspective 1: Accommodation

3.1 Overview

The FAA's near-term focus will be on safely allowing for the expanded operation of UAS through accommodation. Enhanced procedures and technology, over time, will increase access to the NAS through accommodation made possible by improvements to current mitigations and the introduction of advanced mitigations. The need to maintain this avenue for NAS access will continue. Research and development on current and advanced mitigations is necessary to maintain this avenue for access with appropriate restrictions and constraints to mitigate performance shortfalls and address privacy, security, and environmental concerns. The consideration and planning for integration of UAS into the NAS will continue simultaneously.

There has been a growing interest in a wide variety of civil uses for unmanned aircraft. A number of paths can be used to apply for airworthiness certification of UAS. One method that the UAS civil community is currently using to access the NAS is with a special airworthiness certificate in the experimental category, which requires specific, proven capabilities to enable operations at a constrained level. Each application is reviewed for approval on a case-by-case basis that allows a carefully defined level of access that is limited and dependent on risk mitigations that ensure safety and efficiency of the NAS is not diminished. The use of special airworthiness certificates for UAS is similar to their use for manned aircraft and they are normally issued to UAS applicants for the purposes of research and development, crew training or market surveys per 14 CFR 21.191(a), (c), and (f).

Through August 2012, the FAA had issued 114 special airworthiness certificates (i.e., 113 experimental certificates and one special flight permit) to 22 different models of civil aircraft. Of these 22 different models, 16 are unmanned aircraft and 6 are Optionally Piloted Aircraft (OPA). These experimental certificates have been useful for UAS research and development (R&D), and as R&D efforts subside, the use of experimental certificates may decrease. While the FAA continues to accommodate special access to the NAS, existing airworthiness standards are also an avenue for full-type certification. The FAA is working with the UAS ARC to gain feedback to potential changes to airworthiness standards for UAS, as necessary. In the long-term, UAS that are designed to a standard and built to conform to the design may be integrated into the NAS as fully certificated aircraft.

3

3.2 Standards

If UAS are to operate routinely in the NAS, they must conform to an agreed-upon set of standards. Requirements will vary depending on the nature and complexity of the operation, aircraft or component system limitations, pilot and other crewmember qualifications, and the operating environment.

A technical (or operational) standard is an established norm or requirement about a technical (or operational) system that documents uniform engineering or technical criteria, methods, processes, and practices. A standard may be developed privately or unilaterally, by a corporation, regulatory body, or the military. Standards can also be developed by organizations such as trade unions and associations. These organizations often have more diverse input and usually develop voluntary standards that may be adopted by the FAA as a means of regulatory compliance.

To operate an aircraft safely and efficiently in today's NAS, a means of complying with applicable parts of Title 14 of the Code of Federal Regulations must be developed. Aircraft certification standards govern the design, construction, manufacturing, and continued airworthiness of aircraft used in private and commercial operations. These standards were developed with an underlying assumption that a person would be onboard the aircraft and manipulating the controls. This has led to numerous requirements that make aircraft highly reliable and safe for their intended operations and flightcrew protection.

While UAS share many of the same design considerations as manned aircraft, such as structural integrity and performance, most unmanned aircraft and control stations have not been designed to comply with existing civil airworthiness or operational standards. Beyond the problem of meeting existing aircraft certification standards, other components of the UAS, such as the equipment and software associated with the data link (control and communications) and the launch and recovery mechanisms, are not currently addressed in civil airworthiness or operational standards.

Since 2004, the FAA has developed close working relationships with several standards development organizations. Most of these organizations plan to complete their UAS standards development efforts in the near- to mid-term timeframe. When accepted, these standards development products may provide a means of compliance for rules established in the mid-term. The FAA has also been either the lead or an important participant in cross-agency efforts that influence standards development and has coordinated and harmonized these activities with international efforts such as the ICAO UAS Study Group.

Standardization efforts have already produced a number of useful definitions, guidance documents, and considerations that provide common understanding and add insight and data to UAS integration efforts:

- RTCA/SC-203's Guidance Material (DO-304) and numerous position papers
- RTCA/SC-203's Operational Services and Environment Definition For Unmanned Aircraft Systems (OSED, DO-320), which documents definitions and operating scenarios for different UAS operations in the NAS
- RTCA Air Traffic Management Advisory Committee, Requirements and Planning Work Group Report "Airspace Considerations for UAS Integration in the National Airspace System," March 26, 2008
- SAA Workshop Reports that have documented SAA timelines and definitions

Standards development will continue with the goal of producing Minimum Aviation System Performance Standards (MASPS) by the end of the near-term. RTCA products will be taken under consideration by the FAA in the development of policy and guidance products such as Advisory Circulars. Minimum Operational Performance Standards (MOPS) may be used to define Technical Standard Orders (TSO) in the mid- to long-term timeframe.

Additional coordination and input from the stakeholder community (industry and trade associations, manufacturers, academia, research organizations, and public agencies) is being provided with the recent establishment of the UAS ARC.

Although the need to develop standards cannot be overstated, detailed policy, guidance, technical performance requirements, and operational procedures are also needed to enable manned and unmanned aircraft to fly safely and efficiently in the NAS. See Appendix C for specific goals and metrics.

3.3 Rules and Regulations

Unmanned aircraft operations have significantly increased in number, technical complexity, and sophistication during recent years without specific regulations to address their unique characteristics. For a person wishing to design, manufacture, market, or operate a UAS for a commercial mission and seeking FAA approval for that aircraft, its pilot and the operations, existing rules have not been fully tailored to the unique features of UAS.

The FAA has published a Notice which replaced the previous interim operational guidance material used to support UAS accommodation. Since accommodation is not envisioned to be eliminated entirely, this Notice will need to be updated periodically, even as progress continues simultaneously on development of UAS rules and regulations for integration.

The FAA is also developing an NPRM to allow sUAS to conduct operations. This rulemaking effort includes an associated industry effort to develop consensus standards needed for rule implementation. Assuming the sUAS NPRM effort proceeds to a final rule, associated guidance will also be completed to allow the FAA to approve operations and civil and public UAS operators to apply for and safely implement these sUAS operations. All sUAS rule development and implementation will be in accordance with the FMRA.

During this period, the appropriate regulations are also being reviewed for applicability to UAS operations by the FAA, industry groups, and the

> The emphasis will be on the need for new or revised rules for UAS to operate under instrument flight rules (IFR), including rules to allow UAS operations analogous to manned aircraft using visual capabilities.

UAS ARC. The results of this review will determine any regulatory gaps that need to be addressed in the development of specific UAS guidance and rulemaking. The emphasis will be on the need for new or revised rules for UAS to operate under instrument flight rules (IFR), including rules to allow UAS operations analogous to manned aircraft using visual capabilities. Based on the findings of this review, a determination will be made regarding the need to modify, supplement, or create specific new regulations to support UAS beyond the near-term. UAS rulemaking will follow these steps.

3.4 Airworthiness Certification of the UAS

Airworthiness certification is a process that the FAA uses to ensure that an aircraft design complies with the appropriate safety standards in the applicable airworthiness regulations. FAA type design approval indicates the FAA has evaluated the safety of the unmanned aircraft design and all its systems, which is more rigorous than simply making a determination that the UAS is airworthy.

Airworthiness standards for existing aircraft are codified in Title 14 of the Code of Federal Regulations, with processes described for FAA type certification in FAA Order 8110.4 and airworthiness certification in FAA Order 8130.2. The FAA has the authority and regulations in place to tailor the design standards to specific UAS applications, and plans to use this authority until further experience is obtained in addressing the design issues that are unique to UAS.

Civil UAS are currently accommodated with experimental certificates under FAA Order 8130.34. The FAA and the UAS industry will need to work together to move away from the existing experimental or expendable design philosophy, toward a design philosophy more consistent with reliable and safe civilian operation over populated areas and in areas of manned aircraft operation.

Existing airworthiness standards have been developed from years of operational safety experience with manned aircraft and may be too restrictive for UAS in some areas and inadequate in others. For example, existing structural requirements that ensure safe operation in foreseeable weather conditions that are likely to be encountered represent an example of well-established design requirements that existing UAS designs will most likely need to consider. Structural failures have nearly been eliminated from manned aircraft operations and must be mitigated to a similar level of likelihood in UAS operations.

Detailed consideration of UAS in the certification process will be limited in number until such time as a broad and significant consideration is given to existing standards, regulations, and policy. This will be facilitated by UAS manufacturers making application for type design approval to the FAA. For type design approval, UAS designers must show they meet acceptable safety levels for the basic UAS design, and operators must employ certified systems that enable compliance with standardized air traffic operations and contingency/emergency procedures for UAS.

The FAA believes that the UAS community will be best served by the use of an incremental approach to gaining type-design and airworthiness approval. This incremental approach (see Figure 6) could involve the following steps:

- First, allowing existing UAS designs to operate with strict airworthiness and operational limitations to gain operational experience and determine their reliability in very controlled circumstances, as under the existing COA concept or through regulations specific to sUAS;
- Next, developing design standards tailored to a specific UAS application and proposed operating environment. This step would enable the development of useful unmanned aircraft and system design and operational standards for the UAS to facilitate safe operation, without addressing all potential UAS designs and applications. This would lead to type certificates (TC) and production certificates with appropriate limitations documented in the aircraft flight manual;

- And lastly, defining standards for repeatable and predictable FAA type certification of a UAS designed with the redundancy, reliability, and safety necessary to allow repeated safe access to the NAS, including seamless integration with existing air traffic.

Because the UAS community is well established under its current operational assumptions, it is unlikely the FAA or UAS industry will establish an entire set of design standards from scratch. As additional UAS airworthiness options are considered and UAS airworthiness design and operational standards are developed, type certification may be more efficiently and effectively achieved. The UAS industry will continue to build capabilities into the mid- and long-term timeframes. See Appendix C.1 for specific goals and metrics.

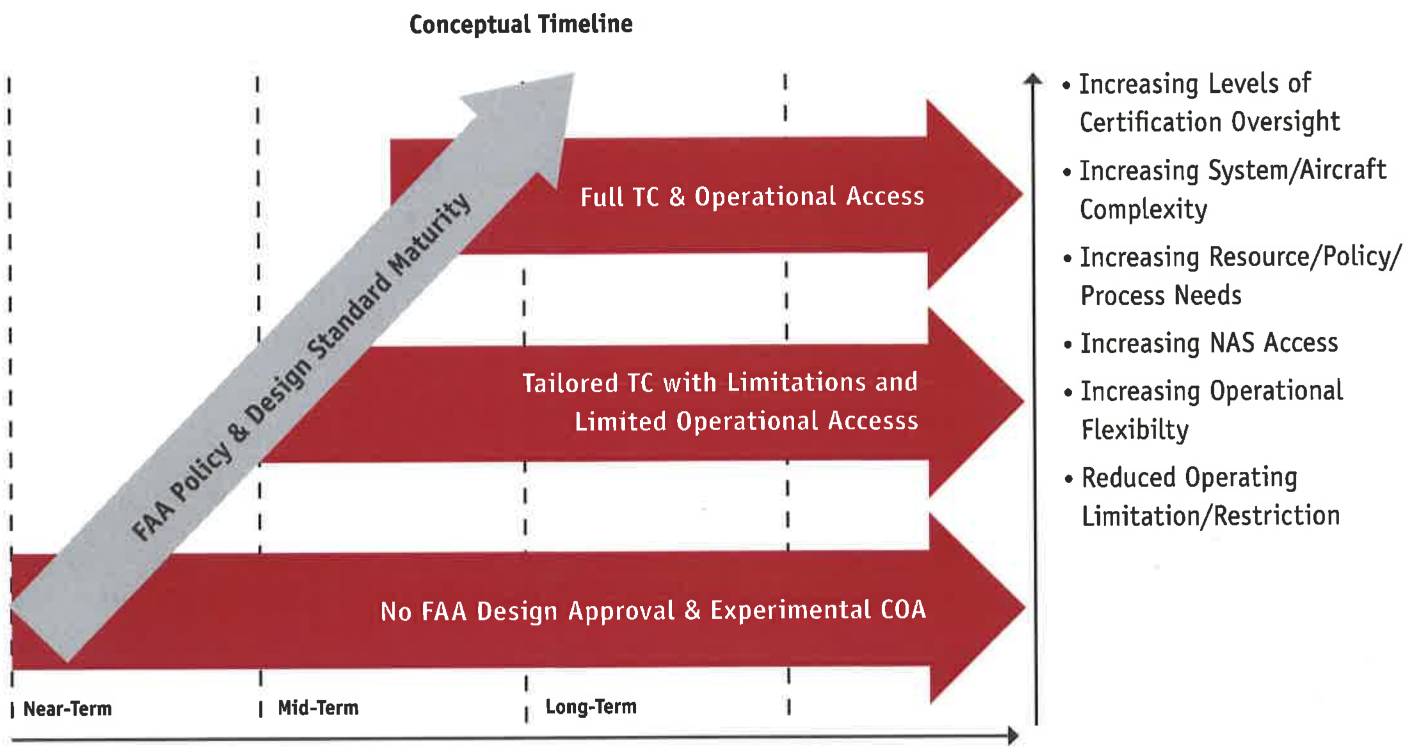


Figure 6: Potential Airworthiness Path for UAS Industry

3.5 Procedures and Airspace

A procedure is a series of actions or operations that have to be executed in the same manner to always obtain the same result under the same circumstances (for example, emergency procedures). The NAS depends on the structure of its airspace and the use of standard procedures to enable safe and efficient operations. ATO directives and other FAA policy and guidance define how UAS are permitted to operate in the NAS today:

- COAs for public access to the NAS – Notice 8900.207 has been released for these operations;
- Experimental Certificates for civil access to the NAS;
- AND AC 91-57 for modeler (recreation) access to the NAS (June 1981) and Section 336 (Special Rule for Model Aircraft) of FMRA.

Experimental certificates and COAs will always be viable methods for accessing the NAS, but typically come with constraints and limitations. Expanded, easier access to the NAS will occur after new or revised operational rules and UAS certification criteria are defined and the FAA develops specific methods for appropriately integrating UAS into NAS operations.

Another requirement is the baselining activity to assess the applicability of existing air traffic control regulations and orders to UAS operations. Any identified gaps will need to be analyzed, and decisions on accommodation or changes to UAS or regulations will be completed. Some sample differences that affect UAS interoperability with the air traffic system are:

- En Route—Current UAS are not able to meet requirements to fly in reduced vertical separation minimum (RVSM) airspace. They do not fly traditional trajectory-based flight paths and require non-traditional handling in emergency situations.
- Terminal—UAS cannot comply with ATC visual separation clearances and cannot execute published instrument approach procedures.
- Facilities—The introduction of UAS at existing airports represents a complex operational challenge. For the near-term, it is expected that UAS will require segregation from mainstream air traffic, possibly accommodated with UAS launch windows, special airports, or off-airport locations where UAS can easily launch and recover. Initial rulemaking for UAS may not address the requirements for UAS at airport facilities, since sUAS are not expected to routinely use airports for takeoff and landing. However, as civil UAS are developed that require airport access, airport integration requirements will need to be developed. These requirements will include environmental impact and/or assessments (when required) concerning noise, emissions, and any unique fuels and other associated concerns. The current Airport Cooperative Research Project (ACRP 03-30) will address the impacts of commercial UAS on airports. The results of the study will be a publication to help airports and communities gain an understanding of UAS, including a description of how various areas of the aviation system, particularly airports, could be affected. The results should be helpful in addressing the airport integration requirement.

ICAO has issued guidance requiring Member States to implement Safety Management System (SMS) programs. These programs are essential to manage risk in the aviation system. The FAA supports this and is a leader in the design and implementation of SMS. Technical challenges abound, including the ability to analyze massive amounts of data to provide useful information for oversight and assessment of risk.

A key input to a Safety Management methodology is the use of safety data. Valuable data collection is underway, but development of a safety-reporting database is currently limited to reporting requirements from existing COAs and experimental certificate holders. Data collection will expand when additional agreements are finalized for sharing public UAS data and new rules and associated safety data reporting requirements are implemented for sUAS. The strategy will use UAS incident, accident, and operational data from public, experimental, and sUAS operations to iteratively support the basis for and define appropriate UAS operating requirements. The availability and quality of this data may directly determine how fast or slow UAS are integrated into the NAS.

3.6 Training (Pilot, Flightcrew Member, Mechanic, and Air Traffic Controller)

UAS training standards will mirror manned aircraft training standards to the maximum extent possible, including appropriate security and vetting requirements, and will account for all roles involved in UAS operation. This may include the pilot, required crew members such as visual observers or launch and recovery specialists, instructors, inspectors, maintenance personnel, and air traffic controllers. See Appendix C.2 and C.8 for specific goals and metrics.

Accident investigation policies, processes, procedures, and training will be developed near-term, and will be provided to Flight Standards District Offices (FSDO) for implementation. Existing manned procedures will be leveraged as much as possible, though differences will need to be highlighted and resolved (e.g., when an unmanned aircraft accident occurs, there may be a need to impound the control station as well as the aircraft).

3.7 Research and Development (R&D) / Technology

Research in the areas of gaps in current technology and new UAS technologies and operations will support and enable the development of airworthiness and operational guidance required to address new and novel aspects of UAS and associated flight operations. The FAA will continue to establish requirements for flight in the NAS so R&D efforts are not duplicative. Additionally, the FAA's research needs are considered within the JPDO NextGen Research Development and Demonstration Roadmap to prevent overlap and provide opportunities for research collaboration.

R&D efforts with industry support the establishment of acceptable performance limits in the NAS and enable the development of performance parameters for today's NAS, while evaluating future concepts, technologies, and procedures for NextGen. The UAS Technical Community Representative Group (TCRG) is sponsoring broad-based UAS research (SAA, C2, and control station studies) aimed at integration with NextGen and validation of concepts. Near-term expected progress is described here:

Sense and Avoid:
Significant research into SAA methods is underway by both government and industry through a variety of approaches and sensor modes. Specifically the FAA is researching:

- Establishment of Sense and Avoid system definitions and performance levels;
- Assessment of Sense and Avoid system multi-sensor use and other technologies;
- And Minimum Sense and Avoid information set required for collision avoidance maneuvering.

Some public agencies and commercial companies are seeking to develop advanced mitigations, such as Ground Based Sense and Avoid (GBSAA) systems, as a strategy for increased access. Concept-of-use demonstrations are underway at several locations to use GBSAA as a mitigation to see-and-avoid requirements for public UAS COA operators in limited operational areas. GBSAA research and the test evaluations will help develop the sensor, link, and algorithm requirements that could allow GBSAA to function as a partial solution set for meeting the SAA requirement and will help build the overall SAA requirements in the long-term. Additionally, as GBSAA technology matures, GBSAA could be used to provide localized UAS NAS integration in addition to being used as an advanced accommodation tool. See Appendix C.3 for specific goals and metrics.

Research is underway on Airborne Sense and Avoid (ABSAA) concepts. Due to complexity, significant progress in ABSAA is not expected until the mid-term. Research goals for the near-term include a flight demonstration of various sensor modes (electro-optic/infrared, radar, Traffic Alert and Collision Avoidance System (TCAS) and Automatic Dependent Surveillance-Broadcast (ADS-B)). Actual fielding of a standardized ABSAA system is a long-term objective. See Appendix C.4 for specific goals and metrics.

Control and Communications:
A primary goal of C2 research is the development of an appropriate C2 link between the unmanned aircraft and the control station to support the required performance of the unmanned aircraft in the NAS and to ensure that the pilot always maintains a threshold level of control of the aircraft. Research will be conducted for UAS control data link communications to determine values for latency, availability, integrity, continuity, and other performance measures.

UAS contingency and emergency scenarios also require research (e.g., how will a UAS in the NAS respond when the command link is lost either through equipment malfunction or malicious jamming, etc.). This research will drive standards that are being established through:

- Development and validation of UAS control link prototype
- Vulnerability analysis of UAS safety critical communications
- Completion of large-scale simulations and flight testing of initial performance requirements

Spectrum and civil radio frequency (RF) identification requires global coordination. The International Telecommunication Union (ITU) through the 2015 World Radiocommunication Conference (WRC-2015) will consider spectrum for UAS beyond-line-of-sight (BLOS) applications. Within the United States, the Federal Communications Commission (FCC) manages and authorizes all non-federal use of the radio frequency spectrum, including state and local government as well as public safety. The National Telecommunications and Information Administration (NTIA) manages and authorizes all federal use of the radio frequency spectrum. UAS spectrum operations within the United States need either the approval of the FCC or NTIA and shall not transmit without being properly authorized. Government agencies and industry need to investigate link security requirements, such as protection against intended and unintended jamming, RF interference, unauthorized link takeover, and spoofing. See Appendix C.5 for specific goals and metrics.

Modeling and Simulation:
The FAA is working with other government agencies and industry to develop a collaborative UAS modeling and simulation environment to explore key challenges to UAS integration. The near-term modeling goals are to:

- Validate current mitigation proposals;
- Establish a baseline of end-to-end UAS performance measures;
- Establish thresholds for safe and efficient introduction of UAS into the NAS;
- And develop NextGen concepts, including 4-dimensional trajectory utilizing UAS technology.

These modeling and simulation efforts will address NAS integration topics for UAS, such as latency in executing ATC clearances, inability to accept ATC visual clearances or comply with visual flight rules, priority and equity of NAS access, lost link, and flyaway scenarios.

Human Factors:
With the pilot controlling the aircraft from beyond the aircraft, several human factors issues emerge related to both the pilot and ATC, and how they will interact to safely operate unmanned aircraft in the NAS. Human factors issues in manned aviation are well known, but there needs to be further analyses regarding integration of UAS into the NAS. In the near-term, data will be collected to permit analysis of how pilots fly UAS, how controllers provide service involving a mix of manned aircraft and UAS, and how pilots and controllers interact with each other, with the goal of developing pilot, ATC, and automation roles and responsibilities concepts. The JPDO, in collaboration with government, academia, and industry researchers, identified several interrelated research challenges:

- Effective human-automation interaction (level; trust; and mode awareness);
- Pilot-centric ground control station design (displays; sensory deficit and remediation; and sterile cockpit);
- Display of traffic/airspace information (separation assurance interface);
- Predictability and contingency management (lost link status; lost ATC communication; and ATC workload);
- Definition of roles and responsibilities (communication flow among crew, ATC, and flight dispatcher);
- System-level issues (NAS-wide human performance requirements);
- And airspace users' and providers' qualification and training (crew/ATC skill set, training, certification, and currency).

Other research in this phase includes activities to support safety case validation and the associated mitigations. This includes case-by-case assessments to determine the likelihood that a system/operation can achieve an acceptable safety level. The research will consider UAS operational and technical risks including:

- Inability to avoid a collision;
- Inability to maintain positive control;
- Inability to meet the operational environment's expected behavior (e.g., self-separate);
- And Inability to safeguard the public.

Summary of "Accommodation" Priorities
Accommodation of UAS in the NAS through evaluation and improvement of safety mitigations
Work with industry and the ARC to review the operational, pilot, and airworthiness regulations
Development of required standards to support technological solutions to identified operational gaps (MOPS)
Safety case validation for UAS operations in NAS—collect/analyze operational and safety data
Robust research, modeling, and simulation for UAS Sense and Avoid, C2, and human factors

Perspective 2: Integration

4.1 Overview

In the mid-term, emphasis will shift significantly from accommodation to integration. For the residual accommodation requirements, it is expected that operational lessons learned and technological advances will lead to more sophisticated mitigations with increased safety margins. Thus, COAs and experimental certificates will remain avenues for accessing the NAS with appropriate restrictions and constraints. Emphasis will shift toward integration of UAS through the implementation of civil standards for unmanned aircraft pilots and new or revised operational rules, together with necessary policy guidance and operational procedures.

Integration efforts will focus on sequentially developing and implementing the UAS system requirements established by the FAA as a result of R&D and test range outputs:

- Finalize the integrated set of FAA rulemaking, policy, operational guidance, procedures, and standards;
- Define continued airworthiness methodologies;
- Complete training and certification standardization;
- Continue the research and technology development and assessment work that underpins the ability of UAS to operate safely and efficiently in the NAS;
- And address the privacy, security, and environmental implications of UAS operations.

To receive civil certification under existing or adapted/expanded regulations, guidance, and standards, research is needed that will assist in defining the certification basis for unique UAS features. While current regulations, guidance, and standards ensure safe operation of aircraft with pilots in the cockpit, these current regulations may not represent the necessary and sufficient basis for the design criteria and operation of UAS.

Integration efforts will provide a foundation for creating and modifying FAA policies and procedures to permit more routine forms of UAS access and bridge the gap to the long-term goal of developing the policy, guidance, and operational procedures required to enable manned and

Integration efforts will focus on sequentially developing and implementing the UAS system requirements established by the FAA as a result of R&D and test range outputs.

4

unmanned aircraft to fly together in an environment that meets or exceeds today's level of safety and efficiency. As new UAS evolve, more specific training will be developed for UAS pilots, crew members, and certified flight instructors. See Appendix C.2 for specific goals and metrics.

UAS operations comingled at airports with manned aircraft is one of the more significant challenges to NAS integration. The UAS must be able to operate within airport parameters and comply with the existing provisions for aircraft. As with airspace operational requirements, the airport standards are not expected to change with the introduction of UAS, and their operation must be harmonized in the provision of air traffic services.

The following general requirements and assumptions will pertain to all UAS operations that are integrated into the NAS (with the exception of sUAS operating exclusively within visual line-of-sight (LOS) of the flight crew):

1. UAS operators comply with existing, adapted, and/or new operating rules or procedures as a prerequisite for NAS integration.
2. Civil UAS operating in the NAS obtain an appropriate airworthiness certificate while public users retain their responsibility to determine airworthiness.
3. All UAS must file and fly an IFR flight plan.
4. All UAS are equipped with ADS-B (Out) and transponder with altitude-encoding capability. This requirement is independent of the FAA's rule-making for ADS-B (Out).
5. UAS meet performance and equipage requirements for the environment in which they are operating and adhere to the relevant procedures.
6. Each UAS has a flight crew appropriate to fulfill the operators' responsibilities, and includes a pilot-in-command (PIC). Each PIC controls only one UA.*
7. Autonomous operations are not permitted.** The PIC has full control, or override authority to assume control at all times during normal UAS operations.
8. Communications spectrum is available to support UAS operations.
9. No new classes or types of airspace are designated or created specifically for UAS operations.
10. FAA policy, guidelines, and automation support air traffic decision-makers on assigning priority for individual flights (or flight segments) and providing equitable access to airspace and air traffic services.

11. Air traffic separation minima in controlled airspace apply to UA.
12. ATC is responsible for separation services as required by airspace class and type of flight plan for both manned and unmanned aircraft.
13. The UAS PIC complies with all ATC instructions and uses standard phraseology per FAA Order (JO) 7110.65 and the Aeronautical Information Manual (AIM).
14. ATC has no direct link to the UA for flight control purposes.

* This restriction does not preclude the possibility of a formation of UA (with multiple pilots) or a "swarm" (one pilot controlling a group of UA) from transiting the NAS to/from restricted airspace, provided the formation or swarm is operating under a COA.

** Autonomous operations refer to any system design that precludes any person from affecting the normal operations of the aircraft.

4.2 Standards

After MASPS are completed, the emphasis of standards activities will be geared toward the development of MOPS, which will contribute to the basis for regulatory changes and the equipment standards for UAS-specific systems and equipment. The development of MOPS may provide requirements the FAA may invoke as TSO to support airworthiness approval on certificated unmanned aircraft and may lead to the development of improved systems, potentially applicable to all civil aircraft. See Appendix C for specific goals and metrics.

4.3 Rules and Regulations

Recognizing that the UAS community might be better served by specific rules, the FAA is initially proposing to amend its regulations to adopt specific rules for the operation of sUAS in the NAS. These changes will address the classification of sUAS, certification of sUAS pilots, registration of sUAS, approval of sUAS operations, and sUAS operational limits.

Operations of sUAS under new regulations may have operational, airspace, and performance constraints, but will provide experience for pilots and additional data to inform subsequent rulemaking, standards, and training development for safe and efficient integration of other UAS in the NAS.

When the final rule is published and in effect, it will reduce the need for sUAS operators to conduct operations under either a COA or the constraints of an experimental certificate. This will allow operators and the FAA to shift the focus of resources to solutions that will better enable UAS integration. See Appendix C.6 for specific goals and metrics.

As integration continues, new or revised operational rules and associated standards and policies will allow compliant UAS to access additional airspace throughout the NAS.

4.4 Airworthiness Certification of the UAS

The FAA will work with the UAS community in defining policy and standards that facilitate agreement on an acceptable UAS certification basis for each applicant. This may involve the development of new policy, guidance, rulemaking, special conditions, and methods of compliance. See Section 3.4 for a more detailed discussion and Appendix C.1 for specific goals and metrics.

4.5 Procedures and Airspace

There will be incremental increases in NAS access based on rigorous safety mitigations of current UAS that were previously developed and built without approved industry or governmental standards. As integration begins, there will be approved airspace and procedures for sUAS, which will provide a basis for developing plans for increased NAS access as UAS are certified. As integration continues, new or revised operational rules and procedures, and associated standards and policies, will allow compliant UAS to access additional airspace throughout the NAS. The ATO will use procedures with these UAS similar to those used for manned aircraft, but may also delegate separation responsibility to UAS for some operations. To support this, ATO goals will be:

- Standardize air traffic operations and contingency/emergency procedures for UAS operators to ensure certified aircraft systems are interoperable with air traffic procedures and airspace requirements;
- Develop airport facility integration plans. This will require research and the development of procedures that address critical issues such as low visibility, taxi spacing, light gun signals, and compatibility with NextGen operations;
- Establish UAS operating requirements with associated ATC procedures for airport conditions;
- And coordinate with the Department of Defense (DoD) and all other appropriate departments and agencies on the development of any new parallel procedures and requirements for air domain awareness and defense.

See Appendix C.8 for specific goals and metrics.

4.6 Training (Pilot, Flightcrew Member, Mechanic, and Air Traffic Controller)

The FAA's role in training is to establish policy, guidance, and standards. Airmen training standards are under development and will be synchronized with the regulatory guidance. Civil operators normally develop a training regimen that allows pilots and flight support to meet regulatory standards. For any UAS operation, training regimens analogous to those that exist for manned aircraft will need to be considered, including relevant areas such as written tests, practical examinations, and currency and proficiency requirements.

Standards for airmen will proceed following the sUAS regulation. The FAA will issue UAS airman certificates and support activities to enable UAS operations to include:

- Development of practical test standards (PTS) and UAS airmen knowledge test question banks;
- Development of a UAS handbook for airmen;
- Training of aviation safety inspectors (ASI) at the FSDO level to provide practical test oversight;
- Identification of designated pilot examiners (DPE) to assist the FSDOs;
- Development of a UAS handbook for pilot and instructors;
- Development of PTS and UAS pilot knowledge test question banks;
- Development of UAS mechanic training and certificate process;
- And development of flight crew security requirements by the relevant United States Government agencies.

Pilot endorsements may be developed for specific UAS makes and models to permit commercial operations. Pilot qualifications by make and model will be built into training and will be expanded based on pilot experience.

Training standards development will be more complex for UAS with unique operating parameters and will continue into the long-term as these UAS are certified.

Regardless of the UAS platform, similar types of training regimens are expected, consisting of a written knowledge test, practical test standards, and a flight evaluation. There will be a requirement for currency and proficiency; qualified ASIs will be fielded to regional offices across the country.

With the introduction of UAS into the NAS, additional training requirements specific to different types of UAS characteristics will probably be required for ATC personnel, including UAS performance, behavior, communications, unique flight profiles, ATC standardized procedures, lost link/fly away profiles, operating limitations, and emergency procedures. Controller training will include differences in interoperability between manned and UAS flights, with a focus on specific handling issues of the aircraft. This training must be administered to ATC facilities throughout the NAS. It is expected that controllers will handle UAS the same as manned aircraft; therefore, no special ATC certification would be required. See Appendix C.2 and C.8 for specific goals and metrics.

4.7 Research and Development (R&D) /Technology

Sense and Avoid:
Research on SAA sensor performance, data communication, and algorithms must provide solutions for safe separation for integration of UAS into the NAS. Research to develop separation algorithms will be accomplished with the JPDO R&D plan goals of:

- Flight demonstration of self-separation and collision avoidance algorithms, with multiple sensors and intruders;
- Assessment of the performance of various self-separation concepts as a function of surveillance data configurations, and evaluation of risk-based self-separation algorithms and policy issues;
- Assessment of the performance of various separation assurance concepts, and flight demonstration of separation assurance algorithms, with criteria-based separation;
- And assessment of UAS performance for delegated spacing applications (e.g., defined interval clearances).

Although research will continue, fully certified UA-based collision avoidance solutions may not be feasible until the long-term and are deemed to be a necessary component for full UAS NAS integration. This will include research on safe and efficient terminal airspace and ground operations, followed by ground demonstrations of autonomous airfield navigation and ATC interaction. See Appendix C.4 and C.8 for specific goals and metrics.

Control and Communications:
Advanced research is required in data link management, spectrum analysis, and frequency management. Efforts will focus on completing development of C2 link assurance and mitigation technologies and methods for incorporating them into the development of certification of the UAS. This will include:

- Identification of satellite communication spectrum from the ITU through its WRC;
- Verification and validation of control communication final performance requirements;
- Establishment of UAS control link national/international standards;
- And development and validation of technologies to mitigate vulnerabilities.

Complete characterization of the capacity, performance, and security impacts of UAS on ATC communication systems will be completed. See Appendix C.5 and C.8 for specific goals and metrics.

Human Factors:
Human factors research will continue in the areas of human-machine interface (both control station displays and ATC displays), automation, and migration of control. Human factors data collected in the near-term and mid-term will be analyzed to determine the safest technologies and best procedures for pilots and ATC controllers to interact with each other and with the aircraft; these results will influence technology and operations research. For separation and collision avoidance capability, the contribution of human decision making versus automation must be identified. See Appendix C.8 for specific goals and metrics.

4.8 Test Ranges

Per the FMRA, the FAA will establish six test ranges. The test ranges will take into consideration climate and geographic diversity, the location of ground infrastructure and research needs. See Appendix C.7 for specific goals and metrics.

The test range program will address and account for:

- Manned-unmanned operations,
- Certification standards and air traffic requirements,
- Coordination and leveraging of National Aeronautics and Space Administration (NASA) and DoD resources,
- Civil and public unmanned aircraft systems,
- And coordination with NextGen.

The test ranges will help provide a verification mechanism for safe operations before unmanned aircraft are integrated into the NAS.

The FAA anticipates test range operator privacy practices, as discussed in their privacy policies, will help inform the dialogue among policymakers, privacy advocates, and the industry regarding broader questions concerning the use of UAS technologies. Transparency of privacy policies associated with UAS test range operations will engage all stakeholders in discussions about which privacy issues are raised by UAS operations and how law, public policy, and the industry practices should respond to those issues in the long run.

Summary of "Integration" Priorities
New operational rules and associated standards, policies, and procedures established for small UAS
New operational rules and associated standards, policies, and procedures established for other UAS
C2 link standards defined for integrity, latency, and continuity
FAA acceptance of MASPS to enable development of detailed MOPS
Published FAA policy and operational guidance to define acceptable methods to comply with operational rules in accordance with an acceptable UAS certification basis for each applicant
Published FAA flightcrew training and certification standards

Perspective 3: Evolution

5.1 Overview

Overlaying the integration of UAS is the need to remain aware of the changing characteristics and requirements of the evolving NAS. The long-term focus for UAS operations is the refinement and updating of regulation, policy, and standards. The end-state is to implement streamlined processes for the continued integration of UAS into the NAS.

These efforts will include:

- Policy, operational guidance, and standards for civil aircraft airworthiness and NAS operations and with consideration for privacy and security concerns and frameworks;
- Continued airworthiness methodologies;
- Training and certification standardization;
- And certification of key technologies to enable continued operations of UAS in the NAS.

5.2 Standards

Unique UAS certification requirements will have been determined. MASPS, MOPS, and TSOs will support the regulations and certification of key systems for each UAS. Additionally, all standards will be evaluated and modified, as needed. See Appendix C.1 for specific goals and metrics.

5.3 Rules and Regulations

Lessons learned from previous rulemaking efforts may be applicable to the development of new UAS regulations. The process should become more efficient as UAS experience is gained and data analysis proves safety cases more quickly. UAS rulemaking activities will be more likely to involve revisions to existing rules, as needed, rather than the creation of new rules.

5.4 Airworthiness Certification of the UAS

Certification of UAS will evolve as future technologies evolve and will be consistent with all other aircraft airworthiness and operational approval processes, adding more capability to the UAS through data analyses and trending, which will identify areas for change and improvement in operations, human factors, communication links, and maintenance. See Section 3.4 for a more detailed discussion and Appendix C.1 for specific goals and metrics.

5

5.5 Procedures and Airspace

Certified pilots and UAS will be permitted access into the NAS under seamless operating procedures. The need to accommodate special NAS access will be dramatically reduced, and will be limited to research and development or test operations.

UAS operations will continue to evolve based on NextGen requirements. See Appendix C.8 for specific goals and metrics.

5.6 Training (Pilot, Flightcrew Member, Mechanic, and Air Traffic Controller)

As new UAS evolve, more specific training will be developed for UAS pilots, crew members, and certified flight instructors based on lessons learned and data collection. See Appendix C.2 and C.8 for specific goals and metrics.

5.7 Research and Development (R&D) / Technology

Identified limitations and gaps will be closed via research and development of required technologies that meet standards established by the FAA. Planned activities include:

- Sense and Avoid research that focuses on algorithm development and compatibility with current and future manned aircraft collision avoidance systems such as TCAS II/ACAS X and surveillance systems (e.g., ADS-B), as well as compatibility with ATC separation management procedures and tools;
- Research on UAS system safety and levels of automation for the improvement of UAS into the future;
- Examination of potential concepts for the widespread integration of UAS into the future NextGen environment;
- AND research on new tools and techniques to support avionics and control software development and certification, to ensure their safety and reliability.

Organized studies will continue to investigate the evolution of UAS operations into the NextGen environment. Detailed research on SAA flight operations, using certified sensor systems, could allow aircraft to maintain safe distances from other aircraft during flight conditions that would not be appropriate for visual flight in a manned aircraft. This capability would rely heavily on network-enabled information, precision navigation, and cooperative surveillance, and would require the development and integration of NextGen-representative technologies for traffic, weather, and terrain avoidance. This conceptual model will be enlarged with sensors that expand the ability to maintain separation from other aircraft past the current visual spectrum and flight conditions restrictions. See Appendix C.8 for specific goals and metrics.

Summary of "Evolution" Priorities
Seamless operations of certified UAS and crew members in the evolving NAS
Published FAA TSOs based on system level MOPS
Certified Sense and Avoid algorithms for collision avoidance and self-separation that are interoperable with evolving NextGen ATC systems and manned collision avoidance systems

Conclusions

6.1 Summary

The safe integration of unmanned aircraft into the NAS is a significant challenge. The FAA is dedicated to developing the technical and regulatory standards, policy guidance, and operational procedures on which successful UAS integration depends.

The application of financial and human resources by academia and industry to support critical FAA initiatives will shorten the time required to develop technical and regulatory standards. Together, all stakeholders can overcome the challenge of integrating UAS into the NAS and leverage UAS and associated technologies for the greater benefit of society.

6.2 Outlook

Based on FAA policy and the challenges that need to be addressed, this roadmap has focused on the activities required to achieve integration of UAS into the evolving NAS. Throughout the process, the key messages below reflect the basis for the FAA's consideration of requirements to integrate civil UAS into the NAS:

1) **Government-industry collaboration is paramount to success and must focus on process, quality, and timely results.**
   The FAA expects to gain experience in applying the existing airworthiness regulations during the type certification process with early UAS adopters. We also expect input from industry and the ARC. Taking into account industry and ARC inputs, and future experience with UAS type certification projects, the FAA will review and revise as necessary the existing airworthiness regulations to ensure UAS safety.

2) **The FAA must remain committed to the development of technical and regulatory standards, policy guidance, and operations procedures on which successful UAS integration depends.**
   With this roadmap, the FAA has outlined initiatives that must be accomplished. Because unmanned aircraft are considered aircraft that are flown by pilots, existing regulations and procedures are largely applicable. However, the complete integration of UAS at airports and in the various airspace classes may necessitate the development of new or revised regulations and supplemental procedures. These will be developed and implemented in coordination with relevant agencies to address related security and privacy implications.

3) **Global standards encourage harmonization and yield cost-effective development.**
   The FAA is not bound by international policies and standards. However, harmonizing efforts with the international aviation community will allow for more seamless operations of UAS across national boundaries. Synchronizing

6

efforts within the aviation community will also permit better use of limited human and fiscal resources, thereby reducing the time required to produce regulatory guidance, policy, and standards.

4) **The FAA is focused on increased access for UAS without impacting the safety or efficiency of the NAS, while managing environmental impacts.**
The FAA has placed a high priority on the development of rules for small UAS that will increase access to the NAS and provide an initial opportunity for commercial operations. In the long-term, the principal objective of the aviation regulatory framework is to achieve and maintain the highest possible uniform level of safety while maintaining or increasing the efficiency and the environmental performance of the NAS. In the case of UAS, this means ensuring the safety of all airspace users as well as the safety of persons and property on the ground.

5) **Progress must be made on the development of technology to enable NAS access.**
Because of many distinct differences between UAS and manned aircraft, there are required technologies that must be matured to enable the safe and seamless integration of UAS in the NAS. Research will be focused in the areas of sense and avoid, control and communications, and human factors.

Appendix A: Acronyms

ABSAA	Airborne Sense and Avoid
ACAS X	Airborne Collision Avoidance System X
ADS-B	Automatic Dependent Surveillance-Broadcast
AIM	Aeronautical Information Manual
AMA	Academy of Model Aeronautics
ARC	Aviation Rulemaking Committee
ASI	Aviation Safety Inspector
ASTM	American Society for Testing and Materials
ATC	Air Traffic Control
ATO	Air Traffic Organization
AVS	Office of Aviation Safety
BLOS	Beyond-Line-of-Sight
C2	Control and Communications
COA	Certificate of Waiver or Authorization
DAA	Detect and Avoid
DHS	Department of Homeland Security
DoD	Department of Defense
DOJ	Department of Justice
DPE	Designated Pilot Examiner
FAA	Federal Aviation Administration
FCC	Federal Communications Commission
FMRA	FAA Modernization and Reform Act of 2012
FSDO	Flight Standards District Office
GBSAA	Ground Based Sense and Avoid
GSE	Ground Support Equipment
IFR	Instrument Flight Rules
ICAO	International Civil Aviation Organization
IPC	Interagency Planning Committee
ITU	International Telecommunication Union
JPDO	Joint Planning and Development Office
LOS	Line-of-Sight
MASPS	Minimum Aviation System Performance Standard
MOPS	Minimum Operational Performance Standard
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
NextGen	Next Generation Air Transportation System
NIJ	National Institute of Justice
NOAA	National Oceanic and Atmospheric Administration

A

NPRM	Notice of Proposed Rulemaking
NTIA	National Telecommunications and Information Administration
OPA	Optionally Piloted Aircraft
OSED	Operational Services and Environmental Definition
PIC	Pilot-in-Command
PTS	Practical Test Standards
R/C	Radio Control
R&D	Research and Development
RF	Radio Frequency
RPV	Remotely Piloted Vehicle
RVSM	Reduced Vertical Separation Minimum
SAA	Sense and Avoid
SARP	Standards and Recommended Practices
SMS	Safety Management System
S&T	Science and Technology
sUAS	Small Unmanned Aircraft Systems
TC	Type Certificate
TCAS	Traffic Alert and Collision Avoidance System
TCRG	Technical Community Representative Group
TSO	Technical Standard Order
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicle
VO	Visual Observer
WRC	World Radiocommunication Conference
14 CFR	Title 14 of the Code of Federal Regulations

Appendix B: Glossary

The following definitions were obtained from several sources, including:

1. Title 14 of the Code of Federal Regulations, Part 1.1
2. FAA Pilot/Controller Glossary (P/CG)
3. RTCA DO-320: Operational Services and Environmental Definition for Unmanned Aircraft Systems
4. Notice 8900.207, "Unmanned Aircraft Systems (UAS) Operational Approval," January 22, 2013
5. FAA Modernization and Reform Act of 2012
6. "Sense and Avoid (SAA) for Unmanned Aircraft Systems (UAS)" – Second Caucus Workshop Report 2013
7. FAA Order 8130.34B – Airworthiness Certification of Unmanned Aircraft Systems and Optionally Piloted Aircraft

Note: Applicable sources are shown at the end of each definition in parentheses (e.g. (1), (2), etc.). Terms without a specific source definition are defined in this Roadmap.

Terminology	Definition
Air Traffic Control	A service operated by appropriate authority to promote the safe, orderly, and expeditious flow of air traffic. (1)
Aircraft	A device that is used or intended to be used for flight in the air. (1)
Airspace	Any portion of the atmosphere sustaining aircraft flight and which has defined boundaries and specified dimensions. Airspace may be classified as to the specific types of flight allowed, rules of operation, and restrictions in accordance with International Civil Aviation Organization standards or State regulation. (3)
Airworthiness Certification	A process that the FAA uses to ensure that an aircraft design complies with the appropriate safety standards in the applicable airworthiness regulations.
Certificate of Waiver or Authorization	An FAA grant of approval for a specific flight operation. The authorization to operate a UAS in the National Airspace System as a public aircraft outside of Restricted, Warning, or Prohibited areas approved for aviation activities. (4)

B

Terminology	Definition
Civil Aircraft	Aircraft other than public aircraft. (4)
Collision Avoidance	The Sense and Avoid system function where the UAS takes appropriate action to prevent an intruder from penetrating the collision volume. Action is expected to be initiated within a relatively short time horizon before closest point of approach. The collision avoidance function engages when all other modes of separation fail. (6)
Communication Link	The voice or data relay of instructions or information between the UAS pilot and the air traffic controller and other NAS users. (3)
Control Station	The equipment used to maintain control, communicate with, guide, or otherwise pilot an unmanned aircraft. (3)
Crewmember [UAS]	In addition to the crewmembers identified in 14 CFR Part 1, a UAS flightcrew member includes pilots, sensor/payload operators, and visual observers, but may include other persons as appropriate or required to ensure safe operation of the aircraft. (4)
Data Link	A ground-to-air communications system which transmits information via digital coded pulses. (3)
Detect and Avoid	Term used instead of Sense and Avoid in the Terms of Reference for RTCA Special Committee 228. This new term has not been defined by RTCA and may be considered to have the same definition as Sense and Avoid when used in this document.
International Civil Aviation Organization	A specialized agency of the United Nations whose objective is to develop the principles and techniques of international air navigation and to foster planning and development of international civil air transport. (2)
Manned Aircraft	Aircraft piloted by a human onboard. (3)
Model Aircraft	An unmanned aircraft that is capable of sustained flight in the atmosphere; flown within visual line-of-sight of the person operating the aircraft and flown for hobby or recreational purposes. (5)

Terminology	Definition
National Airspace System	The common network of U.S. airspace; air navigation facilities, equipment and services, airports or landing areas; aeronautical charts, information and services; rules, regulations and procedures, technical information, and manpower and material. Included are system components shared jointly with the military. (2)
Optionally Piloted Aircraft	An aircraft that is integrated with UAS technology and still retains the capability of being flown by an onboard pilot using conventional control methods. (7)
Pathfinder	An initial UAS airworthiness certification program that will aid the FAA in the establishment of certification requirements.
Pilot-in-Command	Pilot-in-command means the person who: 1) has final authority and responsibility for the operation and safety of the flight; 2) has been designated as pilot-in-command before or during the flight; and 3) holds the appropriate category, class, and type rating, if appropriate, for the conduct of the flight. (1)
Public Aircraft	An aircraft operated by a governmental entity (including federal, state, or local governments, and the U.S. Department of Defense and its military branches) for certain purposes as described in 49 U.S.C. §§ 40102(a)(41) and 40125. Public aircraft status is determined on an operation by operation basis. See 14 CFR Part 1, § 1.1 for a complete definition of a public aircraft. (4)
RTCA	RTCA, Inc. is a private, not-for-profit corporation that develops consensus-based recommendations regarding communications, navigation, surveillance, and air traffic management system issues. RTCA functions as a Federal Advisory Committee. Its recommendations are used by the FAA as the basis for policy, program, and regulatory decisions and by the private sector as the basis for development, investment and other business decisions. (www.rtca.org)
See and Avoid	When weather conditions permit, pilots operating instrument flight rules or visual flight rules are required to observe and maneuver to avoid another aircraft. Right-of-way rules are contained in 14 CFR Part 91. (2)
Self-Separation	Sense and Avoid system function where the UAS maneuvers within a sufficient timeframe to remain well clear of other airborne traffic. (6)
Sense and Avoid	The capability of a UAS to remain well clear from and avoid collisions with other airborne traffic. Sense and Avoid provides the functions of self-separation and collision avoidance to establish an analogous capability to "see and avoid" required by manned aircraft. (6)
Small Unmanned Aircraft	An unmanned aircraft weighing less than 55 pounds. (5)

Terminology	Definition
Special Airworthiness Certificate – Experimental Category (UAS)	Airworthiness certification for experimental UAS and optionally piloted aircraft.
Test Range	A defined geographic area where research and development are conducted in accordance with Sections 332 and 334 of the FMRA. Test ranges are also known as test sites in related documents such as the FAA's Screening Information Request. (5)
Unmanned Aircraft	1) A device used or intended to be used for flight in the air that has no onboard pilot. This devise excludes missiles, weapons, or exploding warheads, but includes all classes of airplanes, helicopters, airships, and powered-lift aircraft without an onboard pilot. UA do not include traditional balloons (see 14 CFR Part 101), rockets, tethered aircraft and un-powered gliders. (4) 2) An aircraft that is operated without the possibility of direct human intervention from within or on the aircraft. (5)
Unmanned Aircraft System	An unmanned aircraft and its associated elements related to safe operations, which may include control stations (ground, ship, or air-based), control links, support equipment, payloads, flight termination systems, and launch/recovery equipment. (4) An unmanned aircraft and associated elements (including communications links and the components that control the unmanned aircraft) that are required for the pilot-in-command to operate safely and efficiently in the national airspace system. (5)
Visual Line-of-Sight	Unaided (corrective lenses and/or sunglasses exempted) visual contact between a pilot-in-command or a visual observer and a UAS sufficient to maintain safe operational control of the aircraft, know its location, and be able to scan the airspace in which it is operating to see and avoid other air traffic or objects aloft or on the ground. (4)

Appendix C: Goals, Metrics, and Target Dates

This appendix contains FAA-developed goals, metrics, and target dates (date ranges) and incorporates many related Unmanned Aircraft Systems (UAS) Aviation Rulemaking Committee (ARC) recommendations. The target dates in this appendix are generally limited to a five-year planning horizon. The FAA will continue its effective dialogue with the UAS ARC as it makes changes to the existing set of goals, metrics, and target dates in yearly updates to this roadmap. These annual updates will track and report progress, as recommended by the Government Accountability Office.

The following material identifies the key goals and related activities to be accomplished in accommodating, integrating, and evolving UAS operations in the National Airspace System (NAS). The goals are, for the most part, intended to be addressed concurrently. For each goal, a set of metrics (i.e., well-defined milestones with target completion dates) is defined. The metrics help establish and maintain common government and industry expectations, and enable objective assessments of the progress made toward the accomplishment of each goal. The goals and metrics reflect the incremental approach to UAS certification and integration described in this roadmap.

The goals and metrics in and of themselves do not constitute a UAS integration roadmap implementation plan; however, they do establish a set of strategic objectives that can guide the definition of activities, schedules, and resource requirements in such a plan. Many of the goals and metrics are not under the FAA's direct control and are dependent upon industry efforts such as participation in civil UAS standards development activities and execution of initial certification (a.k.a. "Pathfinder") programs to aid the establishment of certification requirements. Goals and metrics addressing FMRA requirements are identified and the FMRA Subtitle B (Unmanned Aircraft Systems) is included as a reference in Appendix D.

Target dates for near-term metrics (i.e., those with dates prior to October 2015) are identified by the calendar quarter and year targeted for metric completion (e.g., "3rd Quarter of 2014" means targeted for completion by the end of September 2014). Mid-term metrics may only have a target year or year range specified. In this case, "2016" means the metric's completion target is the end of calendar year 2016. Far-term metrics are outside the five-year horizon of this roadmap and have no target dates. Target dates shown as "from 201x to 201y" indicate related activity is expected throughout this time period. Unless the target dates are required by law (e.g., FMRA), they are exactly that – targets. They are not commitments, either by the FAA, other government organizations, or industry. The target dates consider ongoing and planned government and industry activities and schedules; however, they are not always constrained by these activities and schedules. Some of the target dates are aggressive and will require additional industry or government resources if they are to be met.

C

Although this roadmap is focused on the integration of civil UAS in the NAS, some of the recommended goals and metrics address public UAS integration activities – primarily those of the Department of Defense (DoD). Public entities may have their own certification processes, but the requirements typically build upon those established by the FAA for civil aviation. The DoD's significant activities to develop public UAS that meet airspace and regulatory requirements can and should be leveraged in the FAA's establishment of civil UAS certification requirements.

C.1 Certification Requirements (Airworthiness)

Note: The term "Operator" is used here as defined by the FAA for passenger/cargo carrying and other "for hire and compensation" operations. Not all UAS operations conducted for hire and compensation will require an Operator Certificate. One outcome of this effort will be to establish which UAS operations will or will not require an Operator Certificate.

Goal 1: FAA initial certification process established for one or more civil applicants by 2014.

A. One or more Pathfinder certification projects were defined through government-industry plans (e.g., Project Specific Certification Plans (PSCP)) in the 2nd Quarter of 2013.

- Explanation. Three UAS manufacturers have already applied for type certification and two of these applications were released from delayed sequencing to proceed with restricted category airworthiness certification. Restricted category type certifications for these two applicants have now been completed. Completion of these type certification projects under appropriate, existing certification regulations, will act as a catalyst to establish the process to be used for similar UAS type certification projects. Note: Some UAS type certifications may be in the restricted category with operating restrictions to maintain an equivalent level of safety for the public, but the goal is to certify the respective UAS to meet all integration requirements, if practical.

B. One or more Pathfinder standard airworthiness certification projects complete initial certification planning by 2014.

- Explanation. If the FAA and one or more industry partners complete initial certification planning as recommended in The FAA and Industry Guide to Product Certification, the groundwork will be in place for an efficient certification project that will help establish the process for similar UAS certification projects. One manufacturer has made application and the project will proceed per FAA sequencing processes.

Goal 2: FAA's initial issue papers for one or more standard airworthiness certification projects are available by 2014.

A. One or more Pathfinder certification projects underway by the 4th Quarter of 2013.

- Explanation. One manufacturer has made application for a standard airworthiness certificate and the project will proceed per FAA sequencing processes.

B. FAA's initial certification issues defined for the certification basis or new and novel systems (e.g., UAS control station, airframe, control system, propulsion system, ground support equipment (GSE), etc.) by the 4th Quarter of 2013.

- Explanation. The certification basis and any unique requirements for new and novel systems must be established. Requirements can be identified and refined as a result of Pathfinder efforts or publication by standards organizations (e.g., RTCA, Inc., ASTM International).

Goal 3: FAA's unique certification requirements identified through issue papers that have matured for one or more standard airworthiness certification projects by 2015.

A. FAA's unique certification requirements for new and novel systems (e.g., UAS control station, airframe, control system, propulsion system, GSE, etc.) published by 2015.

- Explanation. Lessons learned from certification of Pathfinder systems, publication of consensus standards, and additional operational experience gained as a result of small UAS (sUAS) rule publication will provide additional requirement information for future applicants.

B. One or more Pathfinder standard airworthiness certification projects completed by 2017 if all associated activities are completed per the nominal certification process.

- Explanation. It is expected that type certifications will be granted only when all requirements have been met under existing rules and requirements and this target date is a best-case scenario.

C. Other certification programs completed by 2017–2020, based on timely applications and system commonality/complexity.

- Explanation. Lessons learned from certification activities of Pathfinder systems, publication of consensus standards, and operations under the sUAS rule will provide data and experience to support other certification efforts.

Goal 4: FAA certification requirements updated and systems certified as necessary.

A. Certification requirements updated as necessary.

B. UAS certified as necessary.

C.2 Certification Requirements (Pilot/Crew)

Goal 1: FAA certification requirements for pilots and crew members for sUAS classes (including medical requirements, training standards, etc.) published as part of a sUAS rule by 2014 in accordance with the FMRA. Note: These requirements include coordination with other government agencies on security/vetting requirements.

Goal 2: Necessary changes to record keeping systems established as part of a sUAS rule and in accordance with the FMRA.

- Explanation. Once the final requirements are established, some changes to existing record keeping systems will be necessary.

Goal 3: FAA certification requirements for pilots and crew members for UAS classes other than those addressed under the sUAS rule (including medical requirements, training standards, etc.) published by 2014–2017.

C.3 Ground Based Sense and Avoid (GBSAA)

Goal 1: FAA draft Advisory Circular on GBSAA systems and requirements released by 2015.

A. FAA approvals for use of GBSAA at one or more DoD GBSAA test sites granted by the 3rd Quarter of 2015, subject to timely application and completion of Certificate of Waiver or Authorization (COA) or other approval processes.

- Explanation. Use U.S. Army and U.S. Air Force developed solutions at DoD UAS test sites. (Note: These are existing DoD GBSAA test sites, not the new test ranges discussed in Section 4.8 and Appendix C.7.)

B. FAA approvals for use of GBSAA for educational and other public applications granted by 2016–2018, subject to timely application and completion of COA or other approval processes.

- Explanation. As above, but expanded beyond the DoD to include public use at other locations equipped with suitable GBSAA systems.

Goal 2: GBSAA operations fully approved by the FAA for routine use by all aviation, including both public and civil entities (if needed).

A. FAA approvals for use of GBSAA for limited civil applications granted.

- Explanation. As with FAA operational approvals for use of GBSAA at all DoD GBSAA test sites and operational approvals for use of GBSAA for educational and other public applications, expanded approvals are expected to be granted for limited civil use at select locations. These approvals will incorporate relevant data from UAS test site operations with GBSAA.

B. FAA's initial GBSAA certification standards for civil operations established.

- Explanation. Assimilate prior deployment experience for DoD, public, and limited civil use, and develop Minimum Aviation System Performance Standards (MASPS) for GBSAA. These approvals will incorporate relevant data from UAS test site operations with GBSAA.

C. FAA approvals for use of GBSAA for civil applications granted.

D. FAA's final GBSAA certification standards for civil operations established.

E. GBSAA certification standards updated as necessary.

C.4 Airborne Sense and Avoid (ABSAA)

Goal 1: Initial FAA certification of ABSAA that facilitates UAS operations without the requirement for a visual observer by 2016–2020.

A. Initial industry proposal for Sense and Avoid (SAA) implementation, integration, and operation in a Pathfinder program provided by the 2nd Quarter of 2014. (See Appendix C.1 for the Pathfinder program goals and metrics.)

- Explanation. This industry proposal will address: a) general UAS operations requirements, b) UAS sense-and-avoid requirements for all proposed operations, including proposed launch and recovery sites, c) proposed UAS ABSAA equipage, and d) planned installation and integration of the proposed ABSAA system(s). ("System" includes both hardware and software.)

B. FAA Stage 2 issue paper on UAS SAA implementation in one or more Pathfinder programs completed by the 2nd Quarter of 2015, subject to applicant provision of sufficient information in certification application and ongoing processes.

- Explanation. An FAA Stage 2 issue paper will provide the "FAA Position" indicating the FAA's concerns, opinions, and actions the applicant is required to accomplish to resolve the issue. This position gives the applicant direction that will enable compliance to the requirements without dictating design

Goal 2: Installation and certification of ABSAA developed to meet industry standards for use by the DoD and other public and civil entities that provide the SAA functions required in the NAS for Classes A, E, and G airspace, and operations approved without the requirement for a visual observer or a COA. Note: the RTCA Program Management Committee established a new Special Committee 228 and working group for Detect and Avoid (DAA). SAA and DAA may be used interchangeably until SC-228 provides a unique definition for DAA. Special Committee 228's Terms of Reference acknowledge that the requirements for UAS DAA in some airspace will require rulemaking.

A. RTCA Operational and Functional Requirements and Safety Objectives (OFRSO) for UAS, Volume 1 was released in the 2nd Quarter of 2013.

- Explanation. The OFRSO "provides recommendations for UAS system level operational and functional requirements and safety objectives for UAS flown in the United States National Airspace System (NAS) under the rules and guidelines for civil aviation." This document provides a framework to support the development of future UAS performance standards and "will prove useful to designers, manufacturers, installers, service providers and users in the development of future standards."

B. RTCA preliminary Phase 1 Detect and Avoid (DAA) Minimum Operational Performance Standards (MOPS) developed to establish performance standards that can be verified and validated for UAS DAA equipment in specified airspace by the 3rd Quarter of 2015.

- Explanation. Emphasis for this initial phase will be standards development on civil UAS equipped to operate into Class A airspace under IFR. A second phase of MOPS development may include DAA equipment to support extended UAS operations in Class D, E and perhaps G airspace. This work effort includes recommendations for a verification and validation test program to be completed before the release of the DAA MOPS. Note: RTCA has sunset Special Committee 203 and Special Committee 228; has a new Detect and Avoid working group developing these DAA MOPS.

C. RTCA Phase 1 DAA MOPS released by the 3rd Quarter of 2016.

- Explanation. This document includes the avionics onboard the UAS and required elements of ground control systems and is based on the results of verification and validation activities on the preliminary Phase 1 DAA MOPS.

D. FAA DAA Technical Standard Order (TSO) issued by the 1st Quarter of 2017.

- Explanation. This document includes the avionics onboard the UAS and required elements of ground control systems.

E. FAA DAA TSO-required equipment used operationally.

Goal 3: DoD or other public entity certification of initial ABSAA systems that enable the DoD and other public entities to safely operate ABSAA-equipped UAS in all NAS airspace classes without the need for a COA. Note: RTCA Special Committee 228's Terms of Reference acknowledge that the requirements for UAS DAA in some airspace will require rulemaking.

A. Initial proposal for ABSAA implementation, integration, and operation in one or more programs released by 2016.

- Explanation. This proposal will address the requirements for ABSAA system(s), including the SAA avionics onboard the unmanned aircraft and required elements of ground control systems. "System" includes both hardware and software.

B. FAA issue paper(s) on UAS SAA implementation in one or more programs for UAS operations in one or more airspace classes released.

- Explanation. The FAA issue paper(s) will document the special considerations for certification of UAS airborne systems that include SAA functions. They also will document special considerations for operating UAS that employ these ABSAA systems and special considerations (including avionics equipage requirements) for manned aircraft operating in the same airspace.

Goal 4: Installation and certification of ABSAA systems for use by the DoD and other public and civil entities that provide the SAA functions that facilitate integrated operation of manned and unmanned aircraft in all NAS airspace classes.

A. RTCA OFRSO for UAS, Volume 1 was released in the 2nd Quarter of 2013.

- Explanation. The OFRSO "provides recommendations for UAS system level operational and functional requirements and safety objectives for UAS flown in the NAS under the rules and guidelines for civil aviation." This document provides a framework to support the development of future UAS performance standards.

B. RTCA Phase 1 DAA MOPS released by the 3rd Quarter of 2016.

- Explanation. This document includes the SAA avionics onboard the aircraft and required elements of ground control systems for IFR flight in Class D, E, and G airspace as noted in the Terms of Reference.

C. RTCA DAA MOPS released for other classes of airspace.

- Explanation. The second phase of DAA MOPS may specify DAA equipment to support extended UAS operations in Class D, E, G, and other airspace as noted in the Terms of Reference.

D. FAA initial DAA TSO released by the 1st Quarter of 2017.

- Explanation. This document will include the avionics onboard the aircraft and required elements of ground control systems as invoked from requirements specified in the Phase 1 DAA MOPS.

E. FAA DAA TSO-required equipment used operationally.

- Explanation. UAS will receive operational approval to use DAA equipment through standard operational approval processes that may include exemptions to Part 91 and/or rulemaking activities as defined by FMRA.

F. RTCA UAS OFRSO and DAA MOPS updated as necessary.

G. FFAA DAA TSO(s) updated as necessary.

C.5 Control and Communications (C2)

Note: For purposes of this section, line-of-sight (LOS) means radio LOS, not visual LOS.

Goal 1: International agreements, industry standards, and FAA regulations and guidance material established by 2015 for civil UAS Control and Communications (C2) capabilities such that C2 subsystems can be certified by the FAA for use in FAA-approved UAS operations.

Note: C2 includes communications internal to the UAS for pilots to operate unmanned aircraft from ground control stations.

A. International agreement was reached in February 2012 at the International Telecommunication Union's (ITU) World Radiocommunication Conference (WRC) on spectrum identified for radio LOS UAS C2 links (or in ITU terminology, Control and Non-Payload Communications links).

- Explanation. Internationally harmonized radio spectrum is needed to help ensure protection from unintentional radio frequency interference, to help ensure adequate spectral bandwidth is available, and to facilitate operation of UAS across international borders. While spectrum is also needed for beyond-line-of-sight (BLOS) C2 links, the initial focus was on radio line-of-sight for civil UAS because demand for LOS links is expected to be greater.

B. RTCA OFRSO for UAS, Volume 1 was released in the 2nd Quarter of 2013.

- Explanation. The OFRSO "provides recommendations for UAS system level operational and functional requirements and safety objectives for UAS flown in the NAS under the rules and guidelines for civil aviation." This document provides a framework to support the development of future UAS performance standards.

C. RTCA's initial MOPS for all the UAS subsystems involved in providing or enabling C2 Data Link using L-Band and C-Band Terrestrial data links are available to be verified and validated by the 3rd Quarter of 2015.

- Explanation. These preliminary MOPS and associated recommendations for a verification and validation test program are needed for the FAA and industry to mature the final Terrestrial data link standards before the release of the final MOPS. RTCA is expected to define MOPS that include L-Band and C-Band frequencies identified at WRC 2012. The resulting MOPS form the basis upon which the FAA can certify systems and services used in providing C2 capabilities for civil UAS.

D. RTCA final Phase 1 C2 Terrestrial Data Link MOPS released by the 3rd Quarter of 2016.

- Explanation. These performance standards in both L-Band and C-Band spectrum are based on the results of the verification and validation test program activities. RTCA is expected to define MOPS that include L-Band and C-Band frequencies identified at WRC 2012.

E. FAA's initial regulations and guidance material (such as TSOs and Advisory Circulars) to enable the production, sale, installation, and maintenance of FAA-certified systems and services used in providing radio LOS C2 capabilities for civil UAS published by 2016–2017.

- Explanation. For the commercial marketplace to offer FAA-certified systems and services for use in providing C2 capabilities for civil UAS, the FAA must establish the necessary regulations and guidance material. These are expected to be based on and largely incorporate the consensus industry standards defined in the RTCA MOPS.

F. Initial FAA-certified Terrestrial C2 Data Link subsystems intended for civil UAS operations are available commercially.

- Explanation. FAA-certified Terrestrial C2 Data Link subsystems for civil UAS are needed for operators and manufacturers to incorporate in their UAS, and for operators to obtain FAA approval for their UAS operations.

Goal 2: Beyond-Line-of-Sight C2 links and capabilities are addressed in international agreements, industry standards, and FAA regulations and guidance material.

A. International agreement reached at the ITU's WRC 15 on radio spectrum identified for BLOS UAS C2 links by 2015.

- Explanation. Internationally harmonized radio spectrum is needed for UAS C2 links to help ensure their protection from unintentional radio frequency interference, to help ensure adequate spectral bandwidth is available for meeting the projected C2 link capacity demands, and to facilitate operation of UAS across international borders. In the far-term, an increasing number of civil UAS operations are expected to require BLOS C2 links.

B. RTCA's second phase MOPS for all the UAS subsystems involved in providing or enabling radio BLOS C2 capabilities for civil UAS published. These elements will include the necessary portion of avionics onboard the unmanned aircraft, the voice and data links, and the necessary portion of ground control systems.

- Explanation. This second phase of MOPS will be needed to provide standards for the use of SATCOM in multiple bands as a C2 Data Link to support UAS. This development will be based on the results of the ITU's WRC 15 as well as lessons learned from industry application of the initial MOPS during product development and FAA certification activities.

C. FAA's final regulations and guidance material to enable the production, installation, and maintenance of FAA-certified systems and services used in providing radio BLOS C2 capabilities for civil UAS published.

- Explanation. A revised set of FAA regulations and guidance material will be needed to address BLOS C2 Data Link systems. These regulations and guidance material will apply lessons learned from application of the initial set.

D. Initial FAA-certified BLOS C2 subsystems intended for civil UAS operations are available commercially.

- Explanation. FAA-certified BLOS C2 subsystems for civil UAS are needed for operators and manufacturers to incorporate in their UAS, and for operators to obtain FAA approval for their UAS operations.

Goal 3: Adequate spectrum is available for both radio LOS and BLOS C2 links to meet the current and projected demand generated by civil UAS operations in the NAS.

A. International spectrum identified for LOS and BLOS UAS C2 links reviewed for possible modification at a future WRC by 2020.

C.6 Small UAS (sUAS) and Other Rules

Goal 1: sUAS rule adopted to allow for both civil and public operations.

A. Agreements (Memorandums of Understanding (MOU), Memorandums of Agreement (MOA), COA, etc.) among the FAA and the DoD, the Department of Homeland Security (DHS), the National Aeronautics and Space Administration (NASA), the National Oceanic and Atmospheric Administration (NOAA), the Department of Justice (DOJ) and other public entities finalized and signed in conjunction with the release of the sUAS Notice of Proposed Rulemaking (NPRM). (The sUAS NPRM is expected to be released in early 2014).

- Explanation. The sUAS proposed rule has undergone a risk assessment by the FAA through its Safety Management System (SMS) process. Adopting or applying the provisions of the proposed rule for public operations is necessary and will accelerate NAS integration of sUAS. It will also reduce the number of COAs the FAA will need to process and free up FAA resources to address other time-critical UAS in the NAS integration issues.

B. sUAS follow-on night operations experiments and study accepted by the FAA for review by the 3rd Quarter of 2014.

- Explanation. NASA completed an initial study at New Mexico State University in 2012. The FAA reviewed the report on this initial study and provided questions and other inputs for inclusion in NASA's planned follow-on study. The FAA will review the report of these focused experiments and may consider DoD and other night operational data.

C. If night operations are deemed as safe as or safer by the FAA, increased night operations for public entities are allowed by the 3rd Quarter of 2015.

- Explanation. Public entities are requesting night operations as a means to fully exploit the capability of sUAS.

D. D. Drafts of all required consensus standards necessary for the implementation of 14 CFR Part 107 available to the public in conjunction with the release of the sUAS NPRM (currently expected to be released in 2013).

- Explanation. More than three years of consensus standard development have occurred. When completed, these standards will provide meaningful guidance to manufacturers and end users for the design, construction, and operation of sUAS. The timely release of the standards will permit industry an opportunity to fully prepare for publication of a final rule, and provide useful guidance to public entities desiring UAS deployment prior to final rule release.

Goal 2: sUAS rule adoption for public and civil operations.

A. 14 CFR Part 107 published, consensus-based standards accepted by the FAA, and the FAA able to issue permits to operate in accordance with requirements of the FMRA.

- Explanation. In order for operations to be conducted under 14 CFR Part 107, the FAA will issue a Notice of Applicability of referenced consensus-based standards and will be able to issue permits to operate.

B. Update sUAS rules, guidance, and/or consensus-based standards after sufficient data have been gathered and analyzed.

- Explanation. Assuming a final rule implementation, the FAA will gain experience with sUAS operating under 14 CFR Part 107. Advancements in technology and analysis of operational and safety data will provide the catalyst for refinement and improvement of Part 107 guidance and/or standards.

C. Update sUAS rules, guidance, and/or consensus-based standards as necessary.

- Explanation. As more operational and safety data is accumulated it will provide a catalyst for refinement and improvement of 14 CFR Part 107 guidance and/or standards as necessary.

Goal 3: sUAS rule supports ATC interoperability to ensure safe and efficient NAS operations.

A. Train air traffic control workforce within six months after sUAS rule enactment.

B. Ensure consistency between sUAS rule proposed operational expectations and proposed changes to ATC Handbook and the Aeronautical Information Manual (AIM).

C. sUAS operations are aligned with ATC Handbook and AIM when the sUAS rule is published and effective.

D. Employ existing strategies to conduct UAS integration safety analysis within SMS Manual guidance to ongoing safety analyses supporting ATC interoperability.

- Explanation. The FAA will enhance ATC interoperability under sUAS rule operations with safety analyses, as required.

Goal 4: Other Rulemaking per the FMRA.

A. Notice of Proposed Rulemaking published to implement the recommendations of the plan required by FMRA by the 3rd Quarter of 2014.

- Explanation. Section 332, subsection (a)(1) of the FMRA specifies plan requirements and subsection (b) requires publication of an NPRM.

B. Final rule published to implement the recommendations of the plan required by the FMRA by the 4th Quarter of 2015.

- Explanation. Section 332, subsection (a)(1) of the FMRA specifies plan requirements and subsection (b) requires publication of a final rule not later than 16 months after publication of the associated NPRM.

C. C. Update to the Administration's most recent policy statement on unmanned aircraft systems contained in Docket No. FAA-2006-25714 required by the FMRA by the 3rd Quarter of 2014.

- Explanation. Section 332, subsection (b) requires publication of this update.

C.7 Test Ranges

Goal 1: FAA program to integrate UAS into the NAS at six test ranges established in accordance with the FMRA.

- Explanation. To establish this program, selection criteria and procedures were developed and communicated to prospective site operators. Test areas criteria consider geographic and climate diversity, the location of ground infrastructure, and research needs. FAA dialogue with prospective site operators clarified criteria and procedures by gathering prospective site operator questions and documenting answers for use by all.

Goal 2: Test ranges selected by FAA in accordance with the FMRA.

- Explanation. The FAA received applications from prospective site operators in the 1st Quarter of 2013 and is evaluating the applications per the established selection criteria and procedures. Any test range selected should provide the FAA, NASA, DoD, industry and academia with the opportunity for UAS prototype development and deployment.

Goal 3: Selected test ranges operational in accordance with the FMRA

- Explanation. The FMRA states that "the test range shall be operational no later than 180 days after the date on which a project is established."

Goal 4: Test range program operational until February 2017.

- Explanation. The FMRA requires the test range program to be terminated by February 2017.

Goal 5: Report findings and conclusions concerning projects in accordance with the FMRA.

- Explanation. The FMRA states that "Not later than 90 days after the date of the termination of the program...the Administrator shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Transportation and Infrastructure and the Committee on Science, Space, and Technology of the House of Representatives a report setting forth the Administrator's findings and conclusions concerning the projects."

C.8 Air Traffic Interoperability

Goal 1: Safety and Interoperability—The overall level of safety in the NAS is preserved through NAS integration, which requires adherence to rigorous airworthiness standards and airspace regulations. While they apply equally to manned aircraft, they also recognize the distinguishing characteristics of UAS.

A. Conduct research that validates the required functional and performance capabilities for safe operation of UAS within the various airspaces of the NAS from 2012 to 2017.

B. Air Traffic interoperability requirements will be allocated to appropriate Air Traffic program and UAS integration efforts from 2012 to 2017.

C. Employ existing strategies to conduct UAS integration safety analysis within SMS Manual guidance to ongoing safety analyses supporting ATC interoperability.

D. Conduct research on Sense and Avoid algorithms for collision avoidance and self-separation that are interoperable with evolving Next Generation Air Transportation System (NextGen) ATC systems and manned collision avoidance systems.

E. Analyze human factors data to determine the safest technologies and best procedures for air traffic controllers to provide services to UAS pilots.

F. Track safety and operational data to use as a basis for policy decisions from 2012 to 2017.

Goal 2: Procedures and Training

A. Develop ATC training requirements specific to different types of UAS characteristics, including UAS performance, behavior, communications, unique flight profiles, ATC standardized procedures, lost link/ fly away profiles, operating limitations, and emergency procedures. Initial training produced in 2009, first revision to be available in 3rd Quarter of 2013. Subsequent training development will occur through 2020.

B. B. Administer UAS training to ATC facilities throughout the NAS from 2013 to 2020.

C.9. Miscellaneous

Goal 1: Develop more detailed plans for safely integrating UAS operations in the NAS by 2015.

A. UAS ARC reviewed FAA and industry plans, including the 2006 Airspace Integration Plan, in 2012.

- Explanation. The 2006 Airspace Integration Plan modified the airspace integration plan developed under the government-industry Access 5 program to more directly address the eight major challenges with UAS integration in the NAS. The UAS ARC will review the 2006 plan and update recommendations consistent with current thinking, including goals and metrics documented in this roadmap.

B. UAS ARC made recommendations for changes to FAA and industry programs and provided them to the FAA in the 2nd Quarter of 2013.

- Explanation. The UAS ARC completed its review of FAA and related industry plans and sent the FAA recommendations for additional planning elements and details. These recommendations include proposed changes to existing and planned programs.

C. Updated FAA UAS Integration Roadmap published annually in accordance with the FMRA.

Goal 2: Identify air traffic management system changes required to be implemented in NextGen.

A. UAS are addressed in the FAA's 2012 *NextGen Implementation Plan* by the 4th Quarter of 2013.

- Explanation. This requires explicitly addressing the operation of UAS in the NAS and the evolution of enabling system capabilities in the various NextGen Segment Implementation Plans (NSIP). Although no significant changes to the current NAS and future NextGen are expected for the integration of UAS operations in unrestricted airspace, some system and procedure changes may be necessary. Any changes need to be incorporated in the *NextGen Implementation Plan,* so that appropriate adjustments to program baselines can be made.

B. UAS are addressed in FAA's NextGen Enterprise Architecture by the 4th Quarter of 2013.

- Explanation. This requires explicitly addressing the integration of UAS operations in the NAS, including the necessary operational concepts and system capabilities. The NextGen Enterprise Architecture identifies whatever is needed to integrate UAS operations in unrestricted airspace. The CY 2012 update to the NextGen Enterprise Architecture depicted FMRA milestones in the aircraft roadmap component.

Goal 3: Review and revise and/or develop new UAS operational scenarios to mature UAS operational concept elements, update operational requirements, and validate key concept elements for UAS integration into the NAS.

A. FAA initiates an effort to review existing UAS operational scenarios/concept elements and revise them and/or develop new scenarios, if needed, for use in UAS operational concept development per established air traffic system engineering practices by the 1st Quarter of 2014.

- Explanation. A rich set of operational scenarios and mature concept elements is needed to develop a complete set of operational requirements, from which system functional and performance requirements can be derived. Off-nominal operations may also be defined for conceivable contingency situations.

B. FAA uses vetted operational scenarios and other concept maturation products to update UAS operator and NAS operational requirements by the 3rd Quarter of 2014.

- Explanation. This process uses vetted scenarios and other mature concept elements to update and document the set of UAS operator and NAS operational requirements associated with integrating UAS operations into the NAS per established air traffic system engineering analyses and related processes.

C. FAA uses vetted operational scenarios, updated UAS operator and NAS requirements and other mature concept elements to validate key concept elements and requirements associated with integrating UAS operations into the NAS.

- Explanation. Air traffic system engineering processes continue to validate concept elements and requirements based on priority need for their validation. Concept element validation priorities will determine resource allocations and schedule for validation of respective concept elements.

Goal 4: Develop UAS integration in the Arctic Region in accordance with the FMRA

A. A. FAA evaluates key operational concepts for potential inclusion into appropriate operational policy and procedures documents (e.g., FAA Order 8900.1 (Flight Standards Information Management System), state Aeronautical Information Publication (AIP) supplements, Notices to Airmen (NOTAM), etc.) by the 2nd Quarter of 2015.

B. FAA and Arctic UAS operators examine the costs (e.g., aircraft certification, mandatory equipage requirements, etc.) and benefits (i.e., value of main business cases for use) by the 3rd Quarter of 2015.

C. FAA begins Air Traffic Organization (ATO) process to establish UAS Arctic Areas, including airspace designation and DoD notice, by the 3rd Quarter of 2015.

D. FAA completes safety studies in accordance with Section 335 of the FMRA by the 3rd Quarter of 2015. (Note: The first safety risk management (SRM) panel for initial projects convened in 2013 and has drafted the associated SRM document.)

E. FAA develops UAS restricted category special airworthiness certificate standards by the 3rd Quarter of 2015.

F. FAA reviews planning and approval documents (e.g., COA template, FAA Destination 2025, FAA Flight Plan 2012, other FAA/International Civil Aviation Organization (ICAO) documents) and evaluates or adapts their use for Arctic Area operations by 2015.

G. Begin international UAS scientific experiments (Marginal Ice Zone Observations and Processes Experiment (MIZOPEX)) with NASA, NOAA, and the University of Alaska), commercial UAS photography missions, or other expanded use/demonstration of UAS in accordance with the Arctic Plan by the 3rd Quarter of 2013.

Goal 5: Develop implementation of Common Strategy for DOJ and associated law enforcement, fire, and first responder agency use of sUAS in the NAS in accordance with the FMRA.

Note: Progress on original metrics is documented below along with metrics to be completed.

A. FAA began collaboration with the DHS Science and Technology (S&T) Directorate during the 4th Quarter of 2012 to support FAA testing and evaluation program of sUAS for law enforcement and first responders, with high-level suitability criteria.

B. FAA formally accepted and signed the MOU with the DOJ National Institute of Justice (NIJ) in the 1st Quarter of 2013.

C. FAA established a working group to examine validity of legacy pilot-in-command (PIC) and observer medical qualifications currently stipulated in COA guidelines in the 2nd Quarter of 2013.

D. FAA established a liaison with DOJ NIJ and U.S. Fire Administration on the development of common strategies for the deployment of sUAS technologies in support of fire enforcement agencies in the 2nd Quarter of 2013.

E. FAA established a working group to examine validity and alternatives to PIC certification requirements established in the 2nd Quarter of 2013.

F. FAA established a collaborative working group with DOJ NIJ and federal law enforcement agencies to examine, plan, and develop a nationwide COA process/approval for the Federal Bureau of Investigation, Bureau of Alcohol, Tobacco, Firearms and Explosives, the National Park Service, and other federal law enforcement and emergency management agencies with country-wide jurisdictions in the 2nd Quarter of 2013.

G. FAA incorporates key operational concepts of strategy into a revised law enforcement/first responder-specific COA template by the 4th Quarter of 2013.

H. FAA establishes a collaborative working group with DOJ NIJ and appropriate law enforcement agencies and trade associations to examine, plan, and develop a COA approval process for law enforcement and first responder mutual aid operations by the 4th Quarter of 2013.

I. FAA to establish working group with DOJ NIJ and the DHS S&T on the development of a technical bulletin on the Common Strategy for distribution to law enforcement/first responders across the nation by the 4th Quarter of 2013.

J. FAA commences collaboration and coordination with DOJ NIJ and DHS S&T to support the co-hosting of a DOJ/FAA/DHS-focused sUAS conference to be convened in the 4th Quarter of 2013.

K. FAA establishes a collaborative working group with DOJ NIJ, DHS and appropriate law enforcement associations to examine, plan, and develop guidelines for any law enforcement agency contemplating the use of unmanned aircraft by the 4th Quarter of 2013.

L. FAA establishes working group with DOJ NIJ on the development of a process for the collection of Unmanned Aircraft Aviation Operations Report data from law enforcement agencies by the 4th Quarter of 2013.

M. FAA completes the development of law enforcement and first responder sUAS competency evaluation procedures, safety risk analysis plan (SRAP), and evaluation checklist completed by the 4th Quarter of 2013.

N. FAA assists three different-sized law enforcement agencies in first implementation of the Common Strategy – target date coordinated with the agencies and confident timeline for the agencies – 4th Quarter of 2013.

- Explanation: FAA assistance is planned for one small agency (i.e., less than 100 sworn officers), one medium agency (i.e., 100 to 300 sworn officers), and one large law enforcement agency (i.e., greater than 300 sworn officers).

O. FAA establishes working group to examine sUAS aircraft recommended guidelines for law enforcement agencies contemplating the use of unmanned aircraft by the 4th Quarter of 2013.

P. FAA will complete COA online modifications to enable Common Strategy implementation by law enforcement agencies by the 4th Quarter of 2014.

Q. FAA reviews planning and approval documents (e.g., unique law enforcement agency COA template, FAA Flight Plan 2012, other FAA/ICAO documents) and modifies or adapts their use for law enforcement agency and first responder sUAS operations by 2015.

Goal 6: In accordance with the FMRA, develop policies to ensure "the Administrator of the FAA may not promulgate any rule or regulation regarding a model aircraft, or an aircraft being developed as a model aircraft."

A. Publish FAA order to establish criteria the agency will use to determine which model aircraft organizations can be considered community-based organizations.

B. Publish update to Federal Register that compares content of AC 91-57 and the FMRA, provides examples of careless and reckless operations, and makes distinction between modeling and commercial operations.

Goal 7: Requirements for the operation of "public unmanned aircraft systems" in the NAS in accordance with the FMRA.

A. Develop and implement operational and certification requirements for the operation of "public unmanned aircraft systems" in the NAS by the 4th Quarter of 2015.

Appendix D: FAA Modernization and Reform Act of 2012 Reference Text

Appendix D: FAA Modernization and Reform Act of 2012 Reference Text

Subtitle B—Unmanned Aircraft Systems

SEC. 331. DEFINITIONS.

In this subtitle, the following definitions apply:

(1) ARCTIC.—The term "Arctic" means the United States zone of the Chukchi Sea, Beaufort Sea, and Bering Sea north of the Aleutian chain.

(2) CERTIFICATE OF WAIVER; CERTIFICATE OF AUTHORIZATION.—The terms "certificate of waiver" and "certificate of authorization" mean a Federal Aviation Administration grant of approval for a specific flight operation.

(3) PERMANENT AREAS.—The term "permanent areas" means areas on land or water that provide for launch, recovery, and operation of small unmanned aircraft.

(4) PUBLIC UNMANNED AIRCRAFT SYSTEM.—The term "public unmanned aircraft system" means an unmanned aircraft system that meets the qualifications and conditions required for operation of a public aircraft (as defined in section 40102 of title 49, United States Code).

(5) SENSE AND AVOID CAPABILITY.—The term "sense and avoid capability" means the capability of an unmanned aircraft to remain a safe distance from and to avoid collisions with other airborne aircraft.

(6) SMALL UNMANNED AIRCRAFT.—The term "small unmanned aircraft" means an unmanned aircraft weighing less than 55 pounds.

(7) TEST RANGE.—The term "test range" means a defined geographic area where research and development are conducted.

(8) UNMANNED AIRCRAFT.—The term "unmanned aircraft" means an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft.

(9) UNMANNED AIRCRAFT SYSTEM.—The term "unmanned aircraft system" means an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the pilot in command to operate safely and efficiently in the national airspace system.

SEC. 332. INTEGRATION OF CIVIL UNMANNED AIRCRAFT SYSTEMS INTO NATIONAL AIRSPACE SYSTEM.

(a) REQUIRED PLANNING FOR INTEGRATION.—

(1) COMPREHENSIVE PLAN.—Not later than 270 days after the date of enactment of this Act, the Secretary of Transportation, in consultation with representatives of the aviation industry, Federal agencies that employ unmanned aircraft systems technology in the national airspace system, and the unmanned aircraft systems industry, shall develop a comprehensive plan to safely accelerate the integration of civil unmanned aircraft systems into the national airspace system.

(2) CONTENTS OF PLAN.—The plan required under paragraph (1) shall contain, at a minimum, recommendations or projections on—

(A) the rulemaking to be conducted under subsection (b), with specific recommendations on how the rulemaking will—

(i) define the acceptable standards for operation and certification of civil unmanned aircraft systems;

(ii) ensure that any civil unmanned aircraft system includes a sense and avoid capability; and

(iii) establish standards and requirements for the operator and pilot of a civil unmanned aircraft system, including standards and requirements for registration and licensing;

(B) the best methods to enhance the technologies and subsystems necessary to achieve the safe and routine operation of civil unmanned aircraft systems in the national airspace system;

(C) a phased-in approach to the integration of civil unmanned aircraft systems into the national airspace system;

(D) a timeline for the phased-in approach described under subparagraph (C);

(E) creation of a safe

(F) airspace designation for cooperative manned and unmanned flight operations in the national airspace system;

(G) establishment of a process to develop certification, flight standards, and air traffic requirements for civil unmanned aircraft systems at test ranges where such systems are subject to testing;

(H) the best methods to ensure the safe operation of civil unmanned aircraft systems and public unmanned aircraft systems simultaneously in the national airspace system; and

(I) incorporation of the plan into the annual NextGen Implementation Plan document (or any successor document) of the Federal Aviation Administration.

(3) DEADLINE.—The plan required under paragraph (1) shall provide for the safe integration of civil unmanned aircraft systems into the national airspace system as soon as practicable, but not later than September 30, 2015.

(4) REPORT TO CONGRESS.—Not later than 1 year after the date of enactment of this Act, the Secretary shall submit to Congress a copy of the plan required under paragraph (1).

(5) ROADMAP.—Not later than 1 year after the date of enactment of this Act, the Secretary shall approve and make available in print and on the Administration's Internet Web site a 5-year roadmap for the introduction of civil unmanned aircraft systems into the national airspace system, as coordinated by the Unmanned Aircraft Program Office of the Administration. The Secretary shall update the roadmap annually.

(b) RULEMAKING.—Not later than 18 months after the date on which the plan required under subsection (a)(1) is submitted to Congress under subsection (a)(4), the Secretary shall publish in the Federal Register—

(1) a final rule on small unmanned aircraft systems that will allow for civil operation of such systems in the national airspace system, to the extent the systems do not meet the requirements for expedited operational authorization under section 333 of this Act;

(2) a notice of proposed rulemaking to implement the recommendations of the plan required under subsection (a)(1), with the final rule to be published not later than 16 months after the date of publication of the notice; and

(3) an update to the Administration's most recent policy statement on unmanned aircraft systems, contained in Docket No. FAA-2006-25714.

(c) PILOT PROJECTS.—

(1) ESTABLISHMENT.—Not later than 180 days after the date of enactment of this Act, the Administrator shall establish a program to integrate unmanned aircraft systems into the national airspace system at 6 test ranges. The program shall terminate 5 years after the date of enactment of this Act.

(2) PROGRAM REQUIREMENTS.—In establishing the program under paragraph (1), the Administrator shall—

(A) safely designate airspace for integrated manned and unmanned flight operations in the national airspace system;

(B) develop certification standards and air traffic requirements for unmanned flight operations at test ranges;

(C) coordinate with and leverage the resources of the National Aeronautics and Space Administration and the Department of Defense;

(D) address both civil and public unmanned aircraft systems;

(E) ensure that the program is coordinated with the Next Generation Air Transportation System; and (F) provide for verification of the safety of unmanned aircraft systems and related navigation procedures before integration into the national airspace system.

(3) TEST RANGE LOCATIONS.—In determining the location of the 6 test ranges of the program under paragraph (1), the Administrator shall—

(A) take into consideration geographic and climatic diversity;

(B) take into consideration the location of ground infrastructure and research needs; and

(C) consult with the National Aeronautics and Space Administration and the Department of Defense.

(4) TEST RANGE OPERATION.—A project at a test range shall be operational not later than 180 days after the date on which the project is established.

(5) REPORT TO CONGRESS.—

(A) IN GENERAL.—Not later than 90 days after the date of the termination of the program under paragraph (1), the Administrator shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Transportation and Infrastructure and the Committee on Science, Space, and Technology of the House of Representatives a report setting forth the Administrator's findings and conclusions concerning the projects.

(B) ADDITIONAL CONTENTS.—The report under sub-paragraph (A) shall include a description and assessment of the progress being made in establishing special use air-space to fill the immediate need of the Department of Defense—

(i) to develop detection techniques for small unmanned aircraft systems; and

(ii) to validate the sense and avoid capability and operation of unmanned aircraft systems.

(d) EXPANDING USE OF UNMANNED AIRCRAFT SYSTEMS IN ARCTIC.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Secretary shall develop a plan and initiate a process to work with relevant Federal agencies and national and international communities to designate permanent areas in the Arctic where small unmanned aircraft may operate 24 hours per day for research and commercial purposes. The plan for operations in these permanent areas shall include the development of processes to facilitate the safe operation of unmanned aircraft beyond line of sight. Such areas shall enable over-water flights from the surface to at least 2,000 feet in altitude, with ingress and egress routes from selected coastal launch sites.

(2) AGREEMENTS.—To implement the plan under paragraph (1), the Secretary may enter into an agreement with relevant national and international communities.

(3) AIRCRAFT APPROVAL.—Not later than 1 year after the entry into force of an agreement necessary to effectuate the purposes of this subsection, the Secretary shall work with relevant national and international communities to establish and implement a process, or may apply an applicable process already established, for approving the use of unmanned aircraft in the designated permanent areas in the Arctic without regard to whether an unmanned aircraft is used as a public aircraft, a civil aircraft, or a model aircraft.

SEC. 333. SPECIAL RULES FOR CERTAIN UNMANNED AIRCRAFT SYSTEMS.

(a) IN GENERAL.—Notwithstanding any other requirement of this subtitle, and not later than 180 days after the date of enactment of this Act, the Secretary of Transportation shall determine if certain unmanned aircraft systems may operate safely in the national airspace system before completion of the plan and rulemaking required by section 332 of this Act or the guidance required by section 334 of this Act.

(b) ASSESSMENT OF UNMANNED AIRCRAFT SYSTEMS.—In making the determination under subsection (a), the Secretary shall determine, at a minimum—

(1) which types of unmanned aircraft systems, if any, as a result of their size, weight, speed, operational capability, proximity to airports and populated areas, and operation within visual line of sight do not create a hazard to users of the national airspace system or the public or pose a threat to national security; and

(2) whether a certificate of waiver, certificate of authorization, or airworthiness certification under section 44704 of title 49, United States Code, is required for the operation of unmanned aircraft systems identified under paragraph (1).

(c) REQUIREMENTS FOR SAFE OPERATION.—If the Secretary determines under this section that certain unmanned aircraft systems may operate safely in the national airspace system, the Secretary shall establish requirements for the safe operation of such aircraft systems in the national airspace system.

SEC. 334. PUBLIC UNMANNED AIRCRAFT SYSTEMS.

(a) GUIDANCE.—Not later than 270 days after the date of enactment of this Act, the Secretary of Transportation shall issue guidance regarding the operation of public unmanned aircraft systems to—

(1) expedite the issuance of a certificate of authorization process;

(2) provide for a collaborative process with public agencies to allow for an incremental expansion of access to the national airspace system as technology matures and the necessary safety analysis and data become available, and until standards are completed and technology issues are resolved;

(3) facilitate the capability of public agencies to develop and use test ranges, subject to operating restrictions required by the Federal Aviation Administration, to test and operate unmanned aircraft systems; and

(4) provide guidance on a public entity's responsibility when operating an unmanned aircraft without a civil air-worthiness certificate issued by the Administration.

(b) STANDARDS FOR OPERATION AND CERTIFICATION.—Not later than December 31, 2015, the Administrator shall develop and implement operational and certification requirements for the operation of public unmanned aircraft systems in the national airspace system.

(c) AGREEMENTS WITH GOVERNMENT AGENCIES.—

(1) IN GENERAL.—Not later than 90 days after the date of enactment of this Act, the Secretary shall enter into agreements with appropriate government agencies to simplify the process for issuing certificates of waiver or authorization with respect to applications seeking authorization to operate public unmanned aircraft systems in the national airspace system.

(2) CONTENTS.—The agreements shall—

(A) with respect to an application described in paragraph (1)—

(i) provide for an expedited review of the application;

(ii) require a decision by the Administrator on approval or disapproval within 60 business days of the date of submission of the application; and

(iii) allow for an expedited appeal if the application is disapproved;

(B) allow for a one-time approval of similar operations carried out during a fixed period of time; and

(C) allow a government public safety agency to operate unmanned aircraft weighing 4.4 pounds or less, if operated—

(i) within the line of sight of the operator;

(ii) less than 400 feet above the ground;

(iii) during daylight conditions;

(iv) within Class G airspace; and

(v) outside of 5 statute miles from any airport, heliport, seaplane base, spaceport, or other location with aviation activities.

SEC. 335. SAFETY STUDIES.

The Administrator of the Federal Aviation Administration shall carry out all safety studies necessary to support the integration of unmanned aircraft systems into the national airspace system.

SEC. 336. SPECIAL RULE FOR MODEL AIRCRAFT.

(a) IN GENERAL.—Notwithstanding any other provision of law relating to the incorporation of unmanned aircraft systems into Federal Aviation Administration plans and policies, including this subtitle, the Administrator of the Federal Aviation Administration may not promulgate any rule or regulation regarding a model aircraft, or an aircraft being developed as a model aircraft, if—

(1) the aircraft is flown strictly for hobby or recreational use;

(2) the aircraft is operated in accordance with a community-based set of safety guidelines and within the programming of a nationwide community-based organization;

(3) the aircraft is 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) the aircraft is 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, the operator of the aircraft provides the airport operator and the airport air traffic control tower (when an air traffic facility is located at the airport) with prior notice of the operation (model aircraft operators flying from a permanent location within 5 miles of an airport should establish a mutually-agreed upon operating procedure with the airport operator and the airport air traffic control tower (when an air traffic facility is located at the airport)).

(b) STATUTORY CONSTRUCTION.—Nothing in this section shall be construed to limit the authority of the Administrator to pursue enforcement action against persons operating model aircraft who endanger the safety of the national airspace system.

(c) MODEL AIRCRAFT DEFINED.—In this section, the term "model aircraft" means 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.

U.S. Department of Transportation
Federal Aviation Administration

800 Independence Avenue, SW
Washington, DC 20591

2012-AJG-502 Produced by FAA Communications

Section 8

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE
AVIATION COMMITTEE

Recommended Guidelines for the use of Unmanned Aircraft

August 2012

BACKGROUND:

Rapid advances in technology have led to the development and increased use of unmanned aircraft. That technology is now making its way into the hands of law enforcement officers nationwide.

We also live in a culture that is extremely sensitive to the idea of preventing unnecessary government intrusion into any facet of our lives. Personal rights are cherished and legally protected by the Constitution. Despite their proven effectiveness, concerns about privacy threaten to overshadow the benefits this technology promises to bring to public safety. From enhanced officer safety by exposing unseen dangers, to finding those most vulnerable who may have wandered away from their caregivers, the potential benefits are irrefutable. However, privacy concerns are an issue that must be dealt with effectively if a law enforcement agency expects the public to support the use of UA by their police.

The Aviation Committee has been involved in the development of unmanned aircraft policy and regulations for several years. The Committee recommends the following guidelines for use by any law enforcement agency contemplating the use of unmanned aircraft.

DEFINITIONS:

1. **Model Aircraft** - A remote controlled aircraft used by hobbyists, which is manufactured and operated for the purposes of sport, recreation and/or competition.
2. **Unmanned Aircraft (UA)** – An aircraft that is intended to navigate in the air without an on-board pilot. Also called Remote Piloted Aircraft and "drones."
3. **UA Flight Crewmember** - A pilot, visual observer, payload operator or other person assigned duties for a UA for the purpose of flight.
4. **Unmanned Aircraft Pilot** - A person exercising control over an unmanned aircraft during flight.

COMMUNITY ENGAGEMENT:

1. Law enforcement agencies desiring to use UA should first determine how they will use this technology, including the costs and benefits to be gained.
2. The agency should then engage their community early in the planning process, including their governing body and civil liberties advocates.
3. The agency should assure the community that it values the protections provided citizens by the U.S. Constitution. Further, the agency will operate the aircraft in full compliance with the mandates of the Constitution, federal, state and local law governing search and seizure.
4. The community should be provided an opportunity to review and comment on agency procedures as they are being drafted. Where appropriate, recommendations should be considered for adoption in the policy.
5. As with the community, the news media should be brought into the process early in its development.

SYSTEM REQUIREMENTS:

1. The UA should have the ability to capture flight time by individual flight and cumulative over a period of time. The ability to reset the flight time counter should be restricted to a supervisor or administrator.
2. The aircraft itself should be painted in a high visibility paint scheme. This will facilitate line of sight control by the aircraft pilot and allow persons on the ground to monitor the location of the aircraft. This recommendation recognizes that in some cases where officer safety is a concern, such as high risk warrant service, high visibility may not be optimal. However, most situations of this type are conducted covertly and at night. Further, given the ability to observe a large area from an aerial vantage point, it may not be necessary to fly the aircraft directly over the target location.
3. Equipping the aircraft with weapons of any type is strongly discouraged. Given the current state of the technology, the ability to effectively deploy weapons from a small UA is doubtful. Further, public acceptance of airborne use of force is likewise doubtful and could result in unnecessary community resistance to the program.
4. The use of model aircraft, modified with cameras, or other sensors, is discouraged due to concerns over reliability and safety.

OPERATIONAL PROCEDURES:

1. UA operations require a Certificate of Authorization (COA) from the Federal Aviation Administration (FAA). A law enforcement agency contemplating the use of UA should contact the FAA early in the planning process to determine the requirements for obtaining a COA.
2. UA will only be operated by personnel, both pilots and crew members, who have been trained and certified in the operation of the system. All agency personnel with UA responsibilities, including command officers, will be provided training in the policies and procedures governing their use.
3. All flights will be approved by a supervisor and must be for a legitimate public safety mission, training, or demonstration purposes.
4. All flights will be documented on a form designed for that purpose and all flight time shall be accounted for on the form. The reason for the flight and name of the supervisor approving will also be documented.
5. An authorized supervisor/administrator will audit flight documentation at regular intervals. The results of the audit will be documented. Any changes to the flight time counter will be documented.
6. Unauthorized use of a UA will result in strict accountability.
7. Except for those instances where officer safety could be jeopardized, the agency should consider using a "Reverse 911" telephone system to alert those living and working in the vicinity of aircraft operations (if such a system is available). If such a system is not available, the use of patrol car public address systems should be considered. This will not only provide a level of safety should the aircraft make an uncontrolled landing, but citizens may also be able to assist with the incident.
8. Where there are specific and articulable grounds to believe that the UA will collect evidence of criminal wrongdoing and if the UA will intrude upon reasonable expectations of privacy, the agency will secure a search warrant prior to conducting the flight.

IMAGE RETENTION:

1. Unless required as evidence of a crime, as part of an on-going investigation, for training, or required by law, images captured by a UA should not be retained by the agency.
2. Unless exempt by law, retained images should be open for public inspection.

Section 9

Protecting Privacy From Aerial Surveillance:

Recommendations for Government Use of Drone Aircraft

DECEMBER 2011

ACLU
AMERICAN CIVIL LIBERTIES UNION

Protecting Privacy From Aerial Surveillance:

Recommendations for Government Use of Drone Aircraft

Report by Jay Stanley and Catherine Crump

DECEMBER 2011

AMERICAN CIVIL LIBERTIES UNION

American Civil Liberties Union
125 Broad Street, 18th Floor
New York, NY 10004
www.aclu.org

Protecting Privacy From Aerial Surveillance:

Recommendations for Government Use of Drone Aircraft

DECEMBER 2011

American Civil Liberties Union
125 Broad Street, 18th Floor
New York, NY 10004
www.aclu.org

Report by Jay Stanley and Catherine Crump

Contents

Introduction..1
The Technology..2
Drone capabilities—today and in the future..4
Current status of domestic deployment..6
Pressure on the FAA to loosen the rules..8
UAVs and privacy..10
The Fourth Amendment restricts the use of drones..13
Recommendations..15

Introduction

Unmanned aircraft carrying cameras raise the prospect of a significant new avenue for the surveillance of American life. Many Americans have heard of these aircraft, commonly called drones, because of their use overseas in places like Afghanistan and Yemen.[1] But drones are coming to America. Their deployment has so far been held up by the Federal Aviation Administration (FAA) over safety concerns, but that agency is under strong industry and Congressional pressure to pave the way for domestic deployment. Meanwhile, the technology is quickly becoming cheaper and more powerful, interest in deploying drones among police departments is increasing, and our privacy laws are not strong enough to ensure that the new technology will be used responsibly and consistently with democratic values.

In short, all the pieces appear to be lining up for the eventual introduction of routine aerial surveillance in American life—a development that would profoundly change the character of public life in the United States.

We need a system of rules to ensure that we can enjoy the benefits of this technology without bringing us a large step closer to a "surveillance society" in which our every move is monitored, tracked, recorded, and scrutinized by the authorities. In this paper, we outline a set of protections that we believe would protect Americans' privacy in the coming world of drones.

Aerial surveillance from manned aircraft has been with us for decades. One of the first aircraft the Wright brothers built was a surveillance aircraft, and it was sold to the U.S. Army. Many common uses of drone aircraft—search and rescue, fighting wildfires, dangerous tactical police operations—are beneficial. In the 1980s the Supreme Court ruled that the Fourth Amendment does not categorically prohibit the government from carrying out warrantless aerial surveillance of private property.

Manned aircraft are expensive to purchase, operate and maintain, and this expense has always imposed a natural limit on the government's aerial surveillance capability. This natural limit is eroding.

But manned aircraft are expensive to purchase, operate and maintain, and this expense has always imposed a natural limit on the government's aerial surveillance capability. Now that surveillance can be carried out by unmanned aircraft, this natural limit is eroding. The prospect of cheap, small, portable flying video surveillance machines threatens to eradicate existing practical limits on aerial monitoring and allow for pervasive surveillance, police fishing expeditions, and abusive use of these tools in a way that could eventually eliminate the privacy Americans have traditionally enjoyed in their movements and activities.

1 The ACLU has filed a Freedom of Information Act (FOIA) lawsuit against the U.S. Department of Defense and the Central Intelligence Agency asking for information on when, where and against whom drone strikes can be authorized, the number and rate of civilian casualties and other basic information essential for assessing the wisdom and legality of using armed drones to conduct targeted killings. See ACLU, "Predator Drone FOIA" web page, at http://www.aclu.org/national-security/predator-drone-foia. The focus of this report is on a different subject: their domestic use for surveillance.

Just as the FAA regulates drones to ensure that they are safe, so, too, should drones be regulated so they are not used in ways that infringe on privacy. The FAA's primary purpose is protecting the physical safety of the national airspace, but its mandate also extends to "protecting individuals . . . on the ground," and the courts have suggested that this mandate is a broad one.[2] Therefore, the FAA's obligation to protect individuals on the ground should include protecting the privacy that Americans have traditionally enjoyed and rightly expect. If the agency refuses to do so, or is found by the courts to have limited powers in that area, then Congress should step in to directly enact any additional protections that are needed to preserve that privacy.

The technology

There are hundreds of different types of Unmanned Aerial Vehicles (UAVs), as drones are formally known.[3] They can be as large as commercial aircraft or as small as hummingbirds, and include human remotely guided aircraft as well as autonomous, self-guided vehicles. They include:

- **Large fixed-wing aircraft.** The largest UAVs currently in use, such as the Israeli-made Eitan, are about the size of a Boeing 737 jetliner. The Eitan's wingspan is 86 feet, and it can stay aloft for 20 hours and reach an altitude of 40,000 feet.[4] The Predator B drone, which has been used extensively on overseas battlefields as well as on the U.S.-Mexico border, has a wingspan of 66 feet, and it can stay aloft for over 30 hours and reach an altitude of 50,000 feet.[5] In Pakistan and Afghanistan, the U.S. military and CIA deploy Predators and Reapers armed with surveillance capability as well as missiles capable of destroying a moving vehicle from thousands of feet in the air.[6]

- **Small fixed-wing aircraft.** Smaller fixed-wing aircraft are the current favorite for domestic deployment. The Houston police department, for example, recently tested the ScanEagle, made by Boeing subsidiary Insitu.[7] The ScanEagle is 4 ½ feet long with a wingspan of 10 feet, and it can climb to 19,500 feet and stay aloft for more than 24 hours.[8]

---

2 49 U.S.C. § 40103(b)(2)(B) (2006); City of Burbank v. Lockheed Air Terminal, Inc., 411 U.S. 624, 626-27 (1973) ("[T]he Administrator of the Federal Aviation Administration (FAA) has been given broad authority to regulate the use of the navigable airspace, 'in order to insure the safety of aircraft and the efficient utilization of such airspace . . .' and 'for the protection of persons and property on the ground.'").

3 See Wikipedia, "List of unmanned aerial vehicles," at http://en.wikipedia.org/wiki/List_of_unmanned_aerial_vehicles.

4 "Israel unveils world's largest UAV," *Homeland Security Newswire*, Feb. 23, 2010, online at http://homelandsecuritynewswire.com/israel-unveils-worlds-largest-uav.

5 See General Atomics web page on Predator B at http://www.ga-asi.com/products/aircraft/predator_b.php; R.P.G. Collinson, *Introduction to Avionic Systems* (2011), p. 495.

6 Yochi J. Dreazen, "From Pakistan, With Love: The technology used to monitor the skies over Waziristan is coming to your hometown," *National Journal*, March 13, 2011, online at http://www.nationaljournal.com/magazine/drones-may-be-coming-to-your-hometown-20110313.

7 Stephen Dean, "Police line up to use drones on patrol after Houston secret test," *Houston Examiner*, Jan. 11, 2010, online at http://www.examiner.com/page-one-in-houston/police-line-up-to-use-drones-on-patrol-after-houston-secret-test.

8 Insitu, ScanEagle brochure, online at http://www.insitu.com/documents/Insitu%20Website/Marketing%20Collateral/ScanEagle%20Folder%20Insert.pdf

- **Backpack craft.** Another class of craft is designed to be carried and operated by a single person. The hand-launched AeroVironment Raven, for example, weighs 4 pounds, has a wingspan of 4.5 feet and a length of 3 feet, can fly up to 14,000 feet and stay aloft for up to 110 minutes. Similar-sized products include a three-foot helicopter called the Draganflyer X6, a one-foot-long, one-pound fixed-wing craft called the AeroVironment Wasp, and a fan-propelled craft called the Honeywell T-Hawk that can "hover and stare." Individual hobbyists have also built a number of drones in this size range.[9]

- **Hummingbirds.** A tiny drone called the Nano Hummingbird was developed for the Pentagon's Defense Advanced Research Projects Agency (DARPA) by AeroVironment. Intended for stealth surveillance, it can fly up to 11 miles per hour and can hover, fly sideways, backwards and forwards, for about 8 minutes. It has a wingspan of 6.5 inches and weighs only 19 grams—less than a single AA battery.[10]

- **Blimps.** By mid-2012, the Air Force aims to fly a massive, 370-foot long blimp over Afghanistan.[11] Some blimps are envisioned as high-altitude craft, up to 300 feet in diameter, that would compete with satellites, while others would be low-altitude craft that would allow the police to monitor the streets. Supporters say they are more cost-effective than other craft due to their ability to stay aloft for extended periods.[12]

- **Satellites.** While not precisely drones, space satellites raise many of the same issues. In 2007 the Department of Homeland Security approved a plan to allow U.S. law enforcement to turn the nation's powerful spy satellites inward for use domestically.[13] The program, which was run by the blandly named "National Applications Office," provoked continuing objections from members of Congress as well as privacy and civil liberties groups,[14] which raised numerous questions about the program's unclear legal basis, its inadequate privacy controls and the worrisome implications of using military assets for domestic law enforce-

---

9 AeroVironment brochure, online at http://www.avinc.com/downloads/Raven_Domestic_1210.pdf; AeroVironment web page on the Wasp at http://www.avinc.com/uas/small_uas/wasp/; Carrie Kahn, "It's A Bird! It's A Plane! It's A Drone!" National Public Radio, March 14, 2011, online at http://www.npr.org/2011/03/14/134533552/its-a-bird-its-a-plane-its-a-drone; "Drones on the home front," *Washington Post*, Jan. 23, 2011, online at http://www.washingtonpost.com/wp-srv/special/nation/drone-gallery/.

10 W.J. Hennigan, "It's a bird! It's a spy! It's both," *Los Angeles Times*, Feb. 17, 2011, online at http://articles.latimes.com/2011/feb/17/business/la-fi-hummingbird-drone-20110217.

11 Noah Shachtman, "Look: Giant Spy Blimp Dwarfs 18-Wheeler," *Wired.com*, Oct. 7, 2011, online at http://www.wired.com/dangerroom/2011/10/giant-blimp-dwarfs-truck.

12 On high-altitude blimps see Elliott Minor, "Interest Growing in 'Security' Blimps," Associated Press, April 27, 2004, available online at http://www.rustysforum.com/cgi-bin/domains/com/rustysforum/frc_bb/ultimatebb.cgi?ubb=next_topic&f=1&t=000807&go=older; on low-altitude blimps see e.g. James Nelson, "Utah city may use blimp as anti-crime spy in the sky," Reuters, Jan. 16, 2011, online at http://www.reuters.com/article/2011/01/16/us-crime-blimp-utah-idUSTRE70F1DJ20110116.

13 See Joby Warrick, "Domestic Use of Spy Satellites To Widen," *Washington Post*, Aug. 16, 2007, online at http://www.washingtonpost.com/wp-dyn/content/article/2007/08/15/AR2007081502430.html; Siobhan Gorman, "Satellite-Surveillance Program to Begin Despite Privacy Concerns," *Wall Street Journal*, Oct. 1, 2008, online at http://online.wsj.com/article/SB122282336428992785.html.

14 Congressional testimony on this issue by the ACLU, which helped prod Congress on the issue, is available online at http://www.aclu.org/privacy/gen/31835prs20070906.html

ment. Amid continuing debate, DHS decided in 2009 to end the program.[15] It is unclear what the precise capabilities and limits of the nation's spy satellite system are in terms of the resolution of the images they take, their ability to target specific geographic areas, and the degree to which they utilize thermal and other forms of imaging that reveal details not visible to the naked eye. It is known that their telescopes can peer at the surface of the earth in great detail.

Drone capabilities—today and in the future

The aircraft themselves are steadily improving and, as with so many technologies, that is likely to continue. They are becoming smaller. The military and law enforcement are keenly interested in developing small drones, which have the advantages of being versatile, cheap to buy and maintain, and in some cases so small and quiet that they will escape notice.[16] They are also becoming cheaper. The amazing continual decreases in the prices of electronics that have become normal in our time all but guarantee that the surveillance technologies attached to UAVs will become less expensive and yet more powerful—and with mass production, the aircraft that carry those electronics will become inexpensive enough for a police department to fill the skies over a town with them.

Drones are also becoming smarter. Artificial intelligence advances will likely help drones carry out spying missions. Korean researchers, for example, are working to teach robots how to hide from and sneak up upon a subject.[17] They also will have better staying power, with a greater ability to stay aloft for longer periods of time. Mechanisms for increasing time aloft could include solar power, or the use of blimps or gliders.[18]

Although the primary uses of drones so far have been military, even on overseas battlefields their main use is surveillance. The larger drones can be fitted with weapons or other heavy payloads, but all of them can carry cameras and other imaging technologies that have developed amazing capabilities in recent years and are likely to become even more capable in the near future.

---

15 Spencer S. Hsu, "DHS to Cut Police Access to Spy-Satellite Data," *Washington Post*, June 24, 2009, online at http://www.washingtonpost.com/wp-dyn/content/article/2009/06/23/AR2009062302060.htm; DHS, "Secretary Napolitano Announces Decision to End National Applications Office Program," DHS press release, June 23, 2009, online at http://www.dhs.gov/ynews/releases/pr_1245785980174.shtm.

16 W.J. Hennigan, "It's a bird! It's a spy! It's both," *Los Angeles Times*, Feb. 17, 2011, online at http://articles.latimes.com/2011/feb/17/business/la-fi-hummingbird-drone-20110217.

17 M. Ryan Calo, "Robots and Privacy," April 2010, online at http://ssrn.com/abstract=1599189.

18 "Gliders Emerge As Surveillance UAVs," *Aviation Week*, June 8, 2010, online at http://www.aviationweek.com/aw/generic/story_generic.jsp?topicName=ila_2010&id=news/awx/2010/06/08/awx_06_08_2010_p0-232627.xml; James Nelson, "Utah city may use blimp as anti-crime spy in the sky," Reuters, Jan. 16, 2011, online at http://www.reuters.com/article/2011/01/16/us-crime-blimp-utah-idUSTRE70F1DJ20110116; Ned Smith, "Solar-powered UAV can stay aloft 5 years," *TechNewsDaily*, Sept. 22, 2010, online at http://www.msnbc.msn.com/id/39313306/ns/technology_and_science-tech_and_gadgets/t/solar-powered-uav-can-stay-aloft-years.

Except for possibly the very lightest craft, drones can carry the full range of advanced surveillance technologies that have been developed—and are likely to be developed—including:

The military is developing radar technologies that can see through ceilings and walls and allow the tracking of human targets even when they are inside buildings.

- **High-power zoom lenses.** UAVs can carry increasingly powerful lenses that allow significant zooming, increasing the chance that individuals will come under scrutiny from faraway aircraft without knowing it. And the density of photo sensors is growing at an exponential pace (in line with Moore's law), allowing for higher and higher resolution photos to be taken for the same price camera.[19]

- **Night vision.** Infrared and ultraviolet imaging enable night vision by capturing light outside the spectrum visible to the human eye. Infrared imaging (also known as thermal imaging) shows heat emitted by an object, and so is especially suited for identifying humans and animals in the dark.[20] Ultraviolet (UV) imaging can detect some materials not visible in natural or infrared light, and can also be used to enhance detail; for instance, it can be used to image surface textures not apparent in visible light.[21] Moving forward, thermal imaging is likely to improve—for example becoming more sensitive and available at higher resolutions.

- **See-through imaging.** The military is developing radar technologies that can see through ceilings and walls and allow the tracking of human targets even when they are inside buildings.[22] A technology called Synthetic Aperture Radar, for example, can see through cloudy and dusty conditions and through foliage, and has the potential to penetrate the earth and walls.[23]

- **Video analytics.** This field seeks to apply artificial intelligence techniques not just to collect but also to "watch" video. The technology has been improving rapidly, and can recognize and respond to specific people, events, and objects.[24] One of the most significant uses would be to continually track individuals or vehicles as they move about, using face recognition or other

---

19 Nathan Myhrvold, "Moore's Law Corollary: Pixel Power," *New York Times*, June 7, 2006, online at http://www.nytimes.com/2006/06/07/technology/circuits/07essay.html. Moore's law is the observation that the number of transistors that can be placed on an integrated circuit—and therefore broadly speaking the power of computers—doubles approximately every two years. It has held true for over 50 years.

20 NASA Science Mission Directorate, "Infrared Energy," Mission: Science, 2010, online at http://missionscience.nasa.gov/ems/07_infraredwaves.html.

21 Austin Richards, "Digital Reflected-Ultraviolet Imaging," *Advanced Imaging*, Apr. 2006, online at http://www.uvcorder.com/pdf/AD10406%20Component%2018-20.pdf.

22 See e.g., William Saletan, "Nowhere To Hide," *Slate.com*, Sept. 17, 2008, online at http://www.slate.com/articles/health_and_science/human_nature/2008/09/nowhere_to_hide.html; Greg Miller and Julian E. Barnes, "Special drones pursue militias," *Los Angeles Times*, Sept. 12, 2008, online at http://articles.latimes.com/2008/sep/12/world/fg-pakistan12.

23 "Ground Moving Target Indicator (GMTI) Radar Discrimination of Combatants versus Animals in Severe Clutter," DARPA, undated document (topic number SB082-019), online at http://www.dodsbir.net/sitis/archives_display_topic.asp?Bookmark=32303. Sandia National Laboratories, "Synthetic Aperture Radar Applications," undated, online at http://www.sandia.gov/radar/sarapps.html; Alicia Tejada, "MIT Develops New Radar Technology: Military Could See Through Walls," ABC News, Oct. 20, 2011, online at http://abcnews.go.com/Technology/radar-technology-mit-walls/story?id=14773871.

24 Vigilant Video, online at http://www.vigilantvideo.com (last visited Aug. 12, 2011).

bodily characteristics.[25] It might also be used to identify particular movement patterns as "suspicious," or to identify and flag changes in routines, buildings or grounds.[26] Computers performing these tasks have a distinct advantage over human observers, because as one observer summed it up, "machines do not blink or forget. They are tireless assistants."[27]

- **Distributed video.** A large number of cheap, autonomous UAVs working in concert like a swarm of insects could provide surveillance capabilities impossible with just a few vehicles.[28] The Air Force is testing a system called "Gorgon Stare," which uses multiple video cameras that "will be looking at a whole city, so there will be no way for the adversary to know what we're looking at, and we can see everything," as an Air Force officer enthused to the *Washington Post*. The Air Force is seeking to put the system on a craft that can stay airborne for up to two weeks—and the Department of Homeland Security is exploring the technology for possible domestic applications.[29]

"Gorgon Stare will be looking at a whole city, so there will be no way for the adversary to know what we're looking at, and we can see everything."

—AIR FORCE MAJ. GEN. JAMES O. POSS

Current status of domestic deployment

So far the federal government has restricted law enforcement's use of drones out of concern for the safety of the airspace. But those restrictions may soon be loosened, and law enforcement has a strong interest in deploying drones as a cheap way to conduct surveillance that is now prohibitively expensive.[30] Already, limited deployments of UAVs have been made, including:

- Along the border. Since 2005, the Customs and Border Protection agency (CBP) has operated UAVs along the border. It currently operates seven Predator B drones, which are controlled remotely by pilots sitting in Arizona, North Dakota, and Florida, and hopes to expand that number to 24 by 2016, with 11 of those assigned to the southwest border and the rest

---

25 Noah Shachtman, "Army Tracking Plan: Drones That Never Forget a Face," *Wired.com*, Sept. 28, 2011, online at http://www.wired.com/dangerroom/2011/09/drones-never-forget-a-face/.

26 On change detection, see Sandia National Laboratories, "Synthetic Aperture Radar Applications," undated, online at http://www.sandia.gov/radar/sarapps.html.

27 Steve Lohr, "Computers That See You and Keep Watch Over You," *New York Times*, Jan. 1, 2011, online at http://www.nytimes.com/2011/01/02/science/02see.html.

28 Darren Quick, "Boeing demonstrates swarm technology," *Gizmag.com*, Aug. 22, 2011, online at http://www.gizmag.com/uav-swarm-technology/19581/.

29 Ellen Nakashima and Craig Whitlock, "With Air Force's Gorgon Drone 'we can see everything', *Washington Post*, Jan. 2, 2011, online at http://www.washingtonpost.com/wp-dyn/content/article/2011/01/01/AR2011010102690.html.

30 Yochi J. Dreazen, "From Pakistan, With Love: The technology used to monitor the skies over Waziristan is coming to your hometown," *National Journal*, March 10, 2011, online at http://www.nationaljournal.com/magazine/drones-may-be-coming-to-your-hometown-20110313.

elsewhere.[31] As of September 1, 2010, CBP drones patrol the entire length of the southern border.[32] Starting in February, the Department of Defense moved beyond the border, sending drones deep into Mexico in an effort to gather information about major drug traffickers as part of the Mexican drug war.[33]

- The Los Angeles Times reported in December 2011 that CBP has been making its Predator drones available for domestic law enforcement operations by local police departments, and federal agencies such as the FBI and the Drug Enforcement Administration have used Predators inside the United States as well. This expanded use of the Predators was carried out with no public knowledge or debate.[34]

- The police department in rural Mesa County, Colorado won FAA permission in early 2011 to operate its Draganflyer drones anywhere in the county, the first time a police department had won permission to operate in such a broad area.[35]

- The Miami police have also won permission to test drones, which they have been doing for more than 18 months with two 18-pound Honeywell aircraft, one of which they obtained with a grant from the federal government and the other of which Honeywell is loaning them. But they may only fly them over the everglades and no higher than 400 feet.[36]

After a police spokesperson allowed that drones might ultimately be used to issue traffic tickets, support for the program reportedly collapsed.

- Police in Houston, Texas attempted to carry out secret tests of a drone in 2007, which were discovered and filmed by local television reporters. After a police spokesperson allowed that drones might ultimately be used to issue traffic tickets, support for the program reportedly collapsed.[37]

---

31 "UAS Overview," U.S. Customs and Border Protection, Aug. 31, 2010, online at http://www.cbp.gov/xp/cgov/border_security/air_marine/uas_program/uasoverview.xml; Leslie Berestein, "Drones' Aim: Smugglers," *San Diego Union-Tribune*, Dec. 4, 2009, online at http://www.signonsandiego.com/news/2009/dec/04/drones-aim-smugglers/; General Accountability Office, "Observations on the Costs and Benefits of an Increased Department of Defense Role in Helping to Secure the Southwest Land Border," GAO-11-856R, Sept. 12, 2011, online at http://www.gao.gov/products/GAO-11-856R.

32 "U.S. Drones to Watch Entire Mexico Border from September 1," Reuters, Aug. 30, 2010, online at http://www.reuters.com/article/2010/08/30/us-usa-immigration-security-idUSTRE67T5DK20100830.

33 Ginger Thompson and Mark Mazzetti, "U.S. Drones Fight Mexican Drug Trade," *New York Times*, Mar. 15, 2011, online at http://www.nytimes.com/2011/03/16/world/americas/16drug.html.

34 Brian Bennett, "Police employ Predator drone spy planes on home front," *Los Angeles Times*, Dec. 10, 2011, online at http://www.latimes.com/news/nationworld/nation/la-na-drone-arrest-20111211,0,72624,full.story.

35 The FAA requires the operator to keep the craft within line of sight, and below 400 feet, however. John Dzenitis, "Cop Drone Stirs Big Brother Debate," KREX News Channel 5, Feb. 10, 2011, online at http://www.krextv.com/news/around-the-region/Cop-Drone-Stirs-Big-Brother-Debate-115796764.html; Shawn Zeller, "Unmanned Planes Take Off," *Congressional Quarterly Weekly—Vantage Point*, April 11, 2011, p. 785.

36 Yochi J. Dreazen, "From Pakistan, With Love: The technology used to monitor the skies over Waziristan is coming to your hometown," *National Journal*, March 10, 2011, online at http://www.nationaljournal.com/magazine/drones-may-be-coming-to-your-hometown-20110313.

37 Stephen Dean, "Local 2 Investigates Police Secrecy Behind Unmanned Aircraft Test," KPRC Local 2 News Houston, Nov. 21, 2007, online at http://www.click2houston.com/investigates/14659066/detail.html; Peter Finn, "Domestic use of aerial drones by law enforcement likely to prompt privacy debate," *Washington Post*, Jan. 23, 2011, online at http://www.washingtonpost.com/wp-dyn/content/article/2011/01/22/AR2011012204111.html.

- Police in Arlington, Texas received a drone to help with security during the Super Bowl in February 2011 and FAA permission to deploy it for "training and evaluation" purposes in unpopulated areas.[38]
- The Texas Department of Public Safety has also been using unmanned surveillance aircraft for specific police operations. In one operation, they used a bird-sized "Wasp" aircraft for aerial surveillance as part of an operation in which a search warrant was executed on private property and a suspect arrested.[39]
- In 2011 the city of Ogden, Utah sought FAA permission to deploy an autonomous unmanned blimp for surveillance and crime prevention.[40]
- Hawaii has taken steps toward federal approval to fly drones for surveillance over its harbors, a plan that was reportedly "under review" by the state governor.[41]
- National Guard units around the country also operate drones to train for their use overseas. Brigades in 30 states have or are receiving AAI Shadow UAVs, which have a 14-foot wingspan and can fly 15,000 feet high.[42] The New York Air National Guard, meanwhile, deploys the much larger (66-foot wingspan) Reaper drone. The military is barred by law from engaging in domestic law enforcement, but Guard soldiers do practice their aerial tracking skills by following random civilian vehicles driving near the Adirondacks.[43]

Pressure on the FAA to loosen the rules

Despite strong interest in deploying drones from law enforcement, so far the domestic use of drones has been held back by the Federal Aviation Administration (FAA), which is responsible for the safety of the nation's airspace and has been proceeding very cautiously.[44] Any entity wishing to

---

38 "Arlington, Texas hopes to keep aerial drone," *Homeland Security Newswire*, May 17, 2011, online at http://www.homelandsecuritynewswire.com/arlington-texas-hopes-keep-aerial-drone.

39 Peter Finn, "Domestic use of aerial drones by law enforcement likely to prompt privacy debate," *Washington Post*, Jan. 23, 2011, online at http://www.washingtonpost.com/wp-dyn/content/article/2011/01/22/AR2011012204111.html.

40 James Nelson, "Utah city may use blimp as anti-crime spy in the sky," Reuters, Jan. 16, 2011, online at http://www.reuters.com/article/2011/01/16/us-crime-blimp-utah-idUSTRE70F1DJ20110116; Tim Gurrister, "Ogden blimp may be patrolling by Christmas," *Standard-Examiner* [Ogden, Utah], August 31, 2011, online at http://www.standard.net/stories/2011/08/29/ogden-blimp-may-be-patrolling-christmas.

41 Jim Dooley, "State Surveillance Drones 'Under Review,'" *Hawaii Reporter*, Feb. 1, 2011, online at http://www.hawaiireporter.com/state-surveillance-drones-under-review/123.

42 William Cole, "Hawaii Guard gets flock of Shadow UAVs," *Honolulu Star Advertiser*, May 25, 2011, online at http://www.staradvertiser.com/news/hawaiinews/20110525_hawaii_guard_gets_flock_of_shadow_UAVs.html.

43 Dave Tobin, "Unmanned drones, controlled by Air National Guard from Hancock Airfield, will fly over the Adirondacks," *Post-Standard* [Syracuse, NY], Feb. 6, 2011, online at http://www.syracuse.com/news/index.ssf/2011/02/unmanned_drones_controlled_by.html.

44 The FAA's rules for "Unmanned Aircraft Operations in the National Airspace System," effective March 28, 2011, are online at http://www.faa.gov/documentLibrary/media/Notice/N7210.766.pdf.

operate a UAV must obtain permission from the agency,[45] and the FAA has only permitted a small number of domestic law enforcement agencies to do so—and attaches strict conditions to their flights.[46]

Aerospace companies are looking beyond Iraq, Pakistan and Afghanistan and see a potentially lucrative domestic market for their technology.

However, the FAA is coming under increasing pressure from industry and its allies in Congress, as well as law enforcement agencies, to open the skies to UAVs. Aerospace companies are looking beyond Iraq, Pakistan and Afghanistan and see a potentially lucrative domestic market for their technology, and supporters argue that the United States must loosen restrictions on the technology so that the nation can be a leader in the industry.[47] Manufacturers have formed a trade association, the Association for Unmanned Vehicle Systems International.[48] Pressure is also coming from states; for example Oklahoma, hoping to help retain and attract aerospace businesses, is pushing to create an 80-mile corridor where drones could fly without specific FAA permission.[49]

Proposed legislation would require the FAA to grant permits more quickly and allow broader use of the technology by 2015.[50] Meanwhile, amid the mounting pressure, the FAA is planning to create a more permissive approval system for commercial UAV operations, which have been severely restricted until now.[51]

The FAA's caution is understandable—the prospect of unmanned flying robots being introduced into the national air space obviously raises very serious safety issues. Groups representing pilots and aircraft operators have expressed concern about UAVs, and have argued that they should not

---

45 In 2006 the Los Angeles County Sheriff was slapped down by the FAA after they tested a surveillance drone without agency permission. Lynn Doan and Ashraf Khalil, "FAA Grounds L.A. Sheriff's Drone Air Force," *Los Angeles Times*, June 22, 2006, online at http://articles.latimes.com/2006/jun/22/local/me-drone22. The agency also told police in Gaston County, N.C. that a 15-pound drone they were testing could not be flown without permission. Yochi J. Dreazen, "From Pakistan, With Love: The technology used to monitor the skies over Waziristan is coming to your hometown," *National Journal*, March 10, 2011, online at http://www.nationaljournal.com/magazine/drones-may-be-coming-to-your-hometown-20110313.

46 Peter Finn, "Domestic use of aerial drones by law enforcement likely to prompt privacy debate," *Washington Post*, Jan. 23, 2011, online at http://www.washingtonpost.com/wp-dyn/content/article/2011/01/22/AR2011012204111.html. The FAA sometimes also grants the military swaths of restricted airspace where UAVs can be freely flown. For the private sector, getting permission to fly a UAV is much harder; they are only granted for research and development, demonstrations, and crew training. Although rules permit their operation by hobbyists, commercial uses of UAVs are not permitted. Government entities wishing to fly drones (from law enforcement at all levels to state universities to the Department of Defense) must obtain a certificate from the FAA (a "Certificate of Waiver or Authorization," or COA). The permit available to non-government parties is called the "Special Airworthiness Certificate—Experimental Category." The FAA's regulations, "Unmanned Aircraft Operations in the National Airspace System," effective March 28, 2011, are online at http://www.faa.gov/documentLibrary/media/Notice/N7210.766.pdf.

47 Yochi J. Dreazen, "From Pakistan, With Love: The technology used to monitor the skies over Waziristan is coming to your hometown," *National Journal*, March 10, 2011, online at http://www.nationaljournal.com/magazine/drones-may-be-coming-to-your-hometown-20110313.

48 *See* Association for Unmanned Vehicle Systems International website, http://www.auvsi.org/Home.

49 Neal Ungerleider, "Oklahoma Wants To Reserve Airspace For Drones," Talking Points Memo Idea Lab, July 26, 2011, online at http://idealab.talkingpointsmemo.com/2011/07/oklahoma-blocks-off-airspace-for-drones.php.

50 Shawn Zeller, "Unmanned Planes Take Off," *Congressional Quarterly Weekly—Vantage Point*, April 11, 2011, p. 785.

51 U.S. Dep't of Transp., Report on DOT Significant Rulemakings: FAA, Aug. 2011, online at http://regs.dot.gov/rulemakings/201108/FAA.htm#11.

be permitted to operate in the National Air Space unless they have the same ability as all other aircraft to fly under visual flight rules, and can be certified to the same level as manned aircraft.[52] A number of domestic UAV accidents have been reported; in 2006, for example, a Predator B drone operated by Customs and Border Protection (CBP) crashed along the U.S.-Mexico border.[53] In 2009 North Little Rock's unmanned helicopter crashed due to a "software failure."[54] In 2010, a Mexican drone crashed into the back yard of an El Paso home.[55] And that same year, a military drone experiencing what the Navy called a "software problem" flew off course and entered restricted Washington, DC airspace.[56] According to government data, UAVs experience an accident rate over 7 times higher than general aviation, and 353 times higher than in commercial aviation.[57]

According to government data, UAVs experience an accident rate over 7 times higher than general aviation, and 353 times higher than in commercial aviation.

Just as the FAA is carefully evaluating the safety implications of drones, so too should we be evaluating the privacy implications of this new technology. We need clear privacy rules so that we can enjoy the benefits drones have to offer in many contexts, without having to worry that they are being used to trample our privacy.

UAVs and privacy

With the federal government likely to permit more widespread use of drones, and the technology likely to become ever more powerful, the question becomes: what role will drones play in American life? Based on current trends—technology development, law enforcement interest, political and

52 Statement of Andrew V. Cebula, Aircraft Owners and Pilots Association, before the House Committee on Transportation and Infrastructure, Aviation Subcommittee, on Unmanned Aerial Vehicles in the National Airspace System, March 29, 2006, online at http://www.aopa.org/whatsnew/newsitems/2006/060329uav-testimony.html.

53 Geoff Carrigan, Dave Long, M.L. Cummings, John Duffner, "Human Factors Analysis of Predator B Crash," MIT Humans and Automation Lab (2008), online at http://web.mit.edu/aeroastro/labs/halab/papers/Carrigan_AUVSI.pdf.

54 "North Little Rock Police Department UAV Crashes During Training," Aero News Network, June 24, 2009, online at http://www.aero-news.net/index.cfm?do=main.textpost&id=d356535f-4aab-4037-aa50-ccf9cf2c65de. Documents obtained by the ACLU of Arkansas connected with North Little Rock's acquisition of UAVs include discussion of various failure modes for the craft, including "Lost link," "Lost communications," "computer hardware or software failure," "GPS failure," "engine failure," and "fly away." Letter on "Public aircraft," North Little Rock [Arkansas] Police Department, Jan. 30, 2008, online at https://www.aclu.org/technology-and-liberty/letter-drone-failure-modes.

55 Diana Washington Valdez and Daniel Borunda, "Mexican drone crashes in backyard of El Paso home," *El Paso Times*, Dec. 17, 2010, online at http://www.elpasotimes.com/ci_16875462.

56 Peter Finn, "Domestic use of aerial drones by law enforcement likely to prompt privacy debate," *Washington Post*, Jan. 23, 2011, online at http://www.washingtonpost.com/wp-dyn/content/article/2011/01/22/AR2011012204111.html.

57 Statement of Nancy Kalinowski, Vice President for System Operations Services, FAA, before the House of Representatives Committee on Homeland Security, Subcommittee on Border, Maritime, and Global Counterterrorism on the Role of Unmanned Aerial Systems on Border Security, July 15, 2010, online at http://www.faa.gov/news/testimony/news_story.cfm?newsId=11599. Statement of Henry Krakowski, Chief Operating Officer, Air Traffic Organization, FAA, before the Senate Committee on Commerce, Science, & Transportation, Subcommittee on Aviation Operations, Safety, & Security, Sept. 13, 2010, online at http://www.faa.gov/news/testimony/news_story.cfm?newsId=11841.

industry pressure, and the lack of legal safeguards—it is clear that drones pose a looming threat to Americans' privacy. The reasons for concern reach across a number of different dimensions:

Based on current trends—technology development, law enforcement interest, political and industry pressure, and the lack of legal safeguards—it is clear that drones pose a looming threat to Americans' privacy.

- **Mission creep.** Even where UAVs are being envisioned for search and rescue, fighting wildfires, and in dangerous tactical police operations, they are likely to be quickly embraced by law enforcement around the nation for other, more controversial purposes. The police in Ogden, Utah think that floating a surveillance blimp above their city "will be a deterrent to crime when it is out and about."[58] In Houston, police suggested that drones could possibly be used for writing traffic tickets.[59] The potential result is that they become commonplace in American life.[60]

- **Tracking.** The Justice Department currently claims the authority to monitor Americans' comings and goings using GPS tracking devices—without a warrant. Fleets of UAVs, interconnected and augmented with analytics software, could enable the mass tracking of vehicles and pedestrians around a wide area.

- **New uses.** The use of drones could also be expanded from surveillance to actual intervention in law enforcement situations on the ground. Airborne technologies could be developed that could, for example, be used to control or dispel protesters (perhaps by deploying tear gas or other technologies), stop a fleeing vehicle, or even deploy weapons.[61]

In addition, drones raise many of the same issues that pervasive video surveillance brings in any context. For example:

- **Chilling effects.** What would be the effect on our public spaces, and our society as a whole, if everyone felt the keen eye of the government on their backs whenever they ventured outdoors? Psychologists have repeatedly found that people who are being observed tend to behave differently, and make different decisions, than when they are not being watched. This effect is so great that a recent study found that "merely hanging up posters of staring human eyes is enough to significantly change people's behavior."[62]

---

58 James Nelson, "Utah city may use blimp as anti-crime spy in the sky," Reuters, Jan. 16, 2011, online at http://www.reuters.com/article/2011/01/16/us-crime-blimp-utah-idUSTRE70F1DJ20110116.

59 Stephen Dean, "Police line up to use drones on patrol after Houston secret test," Houston Examiner, Jan. 11, 2010, online at http://www.examiner.com/page-one-in-houston/police-line-up-to-use-drones-on-patrol-after-houston-secret-test.

60 Joseph Nevins, "Robocop: Drones at Home," Boston Review, January/February 2011, online at http://www.bostonreview.net/BR36.1/nevins.php.

61 Stephen Dean, "New Police Drone Near Houston Could Carry Weapons," KPRC Houston, Nov. 10, 2011, online at http://www.click2houston.com/news/New-Police-Drone-Near-Houston-Could-Carry-Weapons/-/1735978/4717922/-/59xnnez/-/index.html.

62 Sander van der Linden, "How the Illusion of Being Observed Can Make You a Better Person," Scientific American, May 3, 2011, online at http://www.scientificamerican.com/article.cfm?id=how-the-illusion-of-being-observed-can-make-you-better-person; M. Ryan Calo, "People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship," 114 Penn St. L. Rev. 809, online at http://www.pennstatelawreview.org/articles/114/114%20Penn%20St.%20L.%20Rev.%20809.pdf.

- **Voyeurism.** Video surveillance is susceptible to individual abuse, including voyeurism. In 2004, a couple making love on a dark nighttime rooftop balcony, where they had every reason to expect they enjoyed privacy, were filmed for nearly four minutes by a New York police helicopter using night vision. This is the kind of abuse that could become commonplace if drone technology enters widespread use. (Rather than apologize, NYPD officials flatly denied that this filming constituted an abuse, telling a television reporter, "this is what police in helicopters are supposed to do, check out people to make sure no one is ... doing anything illegal").[63]

- **Discriminatory targeting.** The individuals operating surveillance systems bring to the job all their existing prejudices and biases. In Great Britain, camera operators have been found to focus disproportionately on people of color. According to a sociological study of how the systems were operated, "Black people were between one-and-a-half and two-and-a-half times more likely to be surveilled than one would expect from their presence in the population."[64]

- **Institutional abuse.** In addition to abuse by the inevitable "bad apples" within law enforcement, there is also the danger of institutional abuse. Sometimes, bad policies are set at the top, and an entire law enforcement agency is turned toward abusive ends. That is especially prone to happen in periods of social turmoil and intense political conflict. During the labor, civil rights, and anti-Vietnam war movements of the 20th century, the FBI and other security agencies engaged in systematic illegal behavior against those challenging the status quo. And once again today we are seeing an upsurge in spying against peaceful political protesters across America.[65]

- **Automated enforcement.** Drones are part of a trend toward automated law enforcement, in which cameras and other technologies are used to mete out justice with little or no human intervention. This trend raises a variety of concerns, such as the fact that computers lack the judgment to fairly evaluate the circumstances surrounding a supposed violation, and may be susceptible to bugs and other software errors, or simply are not programmed to fairly and properly encapsulate the state of the law as passed by legislatures.[66]

Drones are part of a trend toward automated law enforcement, in which cameras and other technologies are used to mete out justice with little or no human intervention.

One point that is often made with regards to new surveillance technologies is that, while they may increase government surveillance of individuals, they can also increase individuals' ability to

63 "Did NYPD Cameras Invade A Couple's Privacy?" WCBS-TV report, Feb. 24, 2005, video no longer available online; Jim Dwyer, "Police Video Caught a Couple's Intimate Moment on a Manhattan Rooftop," *New York Times*, Dec. 22, 2005, online at http://www.nytimes.com/2005/12/22/nyregion/22rooftop.html.

64 Clive Norris and Gary Armstrong, "The Unforgiving Eye: CCTV Surveillance in Public Spaces," Centre for Criminology and Criminal Justice at Hull University, 1997.

65 See ACLU "Spyfiles" web site at www.aclu.org/spyfiles.

66 Danielle Keats Citron, "Technological Due Process," 85 Washington University Law Review 1249 (2008), online at http://lawreview.wustl.edu/inprint/85/6/Citron.pdf.

record the activities of officials, which can serve as a check on their power.[67] Too often, however, the authorities seek to increase their surveillance over individuals (for example, by installing surveillance cameras throughout public spaces) while restricting individuals' ability to use that same technology as a check against their power (for example, by attempting to prevent individuals from videotaping police[68]). Already, security experts have started expressing concern that unmanned aircraft could be used for terrorism[69]—which naturally raises the question: will individuals be able to make use of the new technology for their own purposes, or will government seek a monopoly over the new technology by citing fears of its use for terrorism?

The Fourth Amendment restricts the use of drones

With drone technology holding so much potential to increase routine surveillance in American life, one key question is the extent to which our laws will protect us. The courts should impose limits on the use of drones for surveillance, prohibiting them from becoming pervasive.

The courts should impose limits on the use of drones for surveillance, prohibiting them from becoming pervasive.

The Supreme Court has never taken a position on whether the Fourth Amendment places limits on government use of UAV surveillance. However, it allowed some warrantless aerial surveillance from *manned* aircraft.

- In the 1986 decision **California v. Ciraolo**, the Supreme Court focused on whether an individual has a privacy interest in being free from aerial surveillance of his backyard. The police had received a tip that Dante Ciraolo was growing marijuana in his backyard, but high fences prevented them from viewing his backyard from the street. The police borrowed a plane, flew it over the backyard and easily spotted marijuana plants growing there. Ciraolo argued that his Fourth Amendment rights were violated because the government did not get a warrant. The Court rejected this argument, explaining that there was no intrusion into his privacy because "[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers observed."[70]
- In **Dow Chemical Co. v. United States,** also decided in 1986, the Supreme Court addressed whether the Environmental Protection Agency violated Dow's Fourth Amendment rights when it employed a commercial aerial photographer to use a precision aerial mapping camera to take photographs of a chemical plant. The Court found no violation, in part because

67 See David Brin, *The Transparent Society* (New York: Basic Books, 1998).

68 See Jay Stanley, "You Have Every Right to Photograph That Cop," ACLU, online at http://www.aclu.org/free-speech/you-have-every-right-photograph-cop.

69 Agence France Press, "Flying Robot Attacks 'Unstoppable' Say Experts," Agence France Press, May 11, 2006, available online at http://www.rense.com/general71/sspm.htm.

70 476 U.S. 207 (1986).

the camera the EPA used was a "conventional, albeit precise, commercial camera commonly used in mapmaking," and "the photographs here are not so revealing of intimate details as to raise constitutional concerns." However, the Court suggested that the use of more sophisticated, intrusive surveillance might justify a different result. It wrote, "surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant."[71]

- In **Florida v. Riley**, decided in 1989, the police had received a tip that Michael Riley was growing marijuana in a greenhouse on the property surrounding his home. The interior of the greenhouse was not visible from the ground outside the property, and the greenhouse had a ceiling, though two panels in the ceiling were missing. A police officer flew over the greenhouse and spotted marijuana through the openings in the roof. While no reasoning commanded a majority of the Court, four justices concluded that its decision in *Ciraolo* applied because Riley had left part of the greenhouse open to public view, and so the search was constitutional.[72]

Because of their potential for pervasive use in ordinary law enforcement operations and capacity for revealing far more than the naked eye, drones pose a more serious threat to privacy than do manned flights. There are good reasons to believe that they may implicate Fourth Amendment rights in ways that manned flights do not.

Government use of UAVs equipped with technology that dramatically improves on human vision or captures something humans cannot see (such thermal or x-ray images) should be scrutinized especially closely by the courts. This follows from the Supreme Court's statement in Dow Chemical that using sophisticated technology not generally available to the public may be considered a search under the Fourth Amendment. It is also suggested by the 2001 case Kyllo v. United States, in which the court rejected the use of thermal imaging devices to peer into a suspect's home without a warrant.[73]

Further, the Supreme Court has suggested that the pervasive or continuous use of a surveillance technology may heighten Fourth Amendment concerns. In United States v. Knotts, the Supreme Court addressed whether attaching primitive "beeper" tracking technology to a car violated the driver's Fourth Amendment rights.[74] Although it concluded that the use of the beeper in that case did not violate the Fourth Amendment, it held that if "such dragnet type law enforcement practices" as "twenty-four hour surveillance of any citizen of this country" ever arose, it would determine if different constitutional principles would be applicable. Citing to this language in Knotts, the federal appeals court in Washington D.C. recently ruled that attaching a GPS device to a person's car and tracking his movements for 28 days fell into this category of dragnet-type

---

71 *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986).

72 *Florida v. Riley*, 488 U.S. 445 (1989).

73 533 U.S. 27 (2001).

74 *United States v. Knotts*, 460 U.S. 276, 283-84 (1983).

surveillance and held that the government's warrantless tracking violated the Fourth Amendment.[75] That case is now up on review before the Supreme Court. Because drones allow for surveillance at least as pervasive and continuous as GPS tracking, the courts should recognize that the Fourth Amendment places restrictions on their use.

With drones as in so many areas, the technology is moving far more rapidly than our jurisprudence, and it is important that the courts keep the Constitution relevant in the world of high technology in which we are increasingly going to be living.

Recommendations

UAVs are potentially extremely powerful surveillance tools, and that power, like all government power, needs to be subject to checks and balances. Like any tool, UAVs have the potential to be used for good or ill. If we can set some good privacy ground rules, our society can enjoy the benefits of this technology without having to worry about its darker potentials. We impose regulations on what law enforcement can do all the time, for example allowing law enforcement to take a thermal image of someone's home only when they get a warrant. We need to impose rules, limits and regulations on UAVs as well in order to preserve the privacy Americans have always expected and enjoyed.

UAVs are potentially extremely powerful surveillance tools, and that power, like all government power, needs to be subject to checks and balances.

The ACLU recommends at a minimum the following core measures be enacted to ensure that this happens:

- **Usage restrictions.** UAVs should be subject to strict regulation to ensure that their use does not eviscerate the privacy that Americans have traditionally enjoyed and rightly expect. Innocent Americans should not have to worry that their activities will be scrutinized by drones. To this end, the use of drones should be prohibited for indiscriminate mass surveillance, for example, or for spying based on First Amendment-protected activities. In general, drones should not be deployed except:
  - o where there are specific and articulable grounds to believe that the drone will collect evidence relating to a specific instance of criminal wrongdoing or, if the drone will intrude upon reasonable expectations of privacy, where the government has obtained a warrant based on probable cause; or
  - o where there is a geographically confined, time-limited emergency situation in which particular individuals' lives are at risk, such as a fire, hostage crisis, or person lost in the wilderness; or

75 *United States v. Maynard*, 615 F.3d 544, 556 (2010).

- for reasonable non-law enforcement purposes by non-law enforcement agencies, where privacy will not be substantially affected, such as geological inspections or environmental surveys, and where the surveillance will not be used for secondary law enforcement purposes.

- **Image retention restrictions.** Images of identifiable individuals captured by aerial surveillance technologies should not be retained or shared unless there is reasonable suspicion that the images contain evidence of criminal activity or are relevant to an ongoing investigation or pending criminal trial.
- **Public notice.** The policies and procedures for the use of aerial surveillance technologies should be explicit and written, and should made public. While it is legitimate for the police to keep the details of particular investigations confidential, policy decisions regarding overall deployment policies—including the privacy tradeoffs they may entail—are a public matter that should be openly discussed.
- **Democratic control.** Deployment and policy decisions surrounding UAVs should be democratically decided based on open information—not made on the fly by police departments simply by virtue of federal grants or other autonomous purchasing decisions or departmental policy fiats.
- **Auditing and effectiveness tracking.** Investments in UAVs should not be made without a clear, systematic examination of the costs and benefits involved. And if aerial surveillance technology is deployed, independent audits should be put in place to track the use of UAVs by government, so that citizens and other watchdogs can tell generally how and how often they are being used, whether the original rationale for their deployment is holding up, whether they represent a worthwhile public expenditure, and whether they are being used for improper or expanded purposes.

Section 10

COMMONWEALTH of VIRGINIA

Department of Criminal Justice Services

Garth L. Wheeler
Director

1100 Bank Street
Richmond, Virginia 23219
(804) 786-4000
TDD (804) 786-8732

November 1, 2013

To: The Honorable Robert F. McDonnell
Members of the General Assembly

From: Garth Wheeler, Director

Subject: Protocols for the Use of Unmanned Aircraft Systems by Law-Enforcement Agencies

It is my pleasure to provide you with the Protocols for the Use of Unmanned Aircraft Systems by Law-Enforcement Agencies developed pursuant to House Bill 2012 (2013). During the 2013 General Assembly Session, House Bill 2012 created a moratorium on the use of unmanned aircraft systems by law-enforcement agencies until July 1, 2015, with certain exceptions. The legislation also required the Department of Criminal Justice Services, in consultation with the Office of the Attorney General and other agencies, to develop model protocols for the use of unmanned aircraft systems by law-enforcement agencies. The results of the Department's work are included in the attached report.

If you have any questions about the protocols, please contact Teresa Gooch, Division Director, Division of Law Enforcement and Security Services (804-786-8730).

REPORT OF THE
DEPARTMENT OF CRIMINAL JUSTICE SERVICES

Protocols for the Use of Unmanned Aircraft Systems (UAS) by Law-Enforcement Agencies

TO THE GOVERNOR AND
THE GENERAL ASSEMBLY OF VIRGINIA

HOUSE DOCUMENT NO. 12

COMMONWEALTH OF VIRGINIA
RICHMOND
2013

Unmanned Aircraft Systems
(UAS)
Protocols for use by Law Enforcement Agencies

October 7, 2013

Virginia Department of Criminal Justice Services
www.dcjs.virginia.gov

In the 2013 session of the General Assembly, House Bill 2012 placed a moratorium on the use of unmanned aircraft systems by state and local law enforcement and regulatory entities until July 1, 2015, except in defined emergency situations or in training exercises related to such situations.

The moratorium does not apply to certain Virginia National Guard functions or to research and development conducted by institutions of higher education or other research organizations.

The bill requires the Department of Criminal Justice Services, in consultation with the Office of the Attorney General and other agencies, to develop protocols for the use of drones by law enforcement agencies and report its findings to the Governor and the General Assembly by November 1, 2013.

In April 2013, a workgroup of public safety and legal professionals was assembled to accomplish the Department of Criminal Justice Services requirement of this bill.

The Department of Criminal Justice Services would like to thank the following individuals for their professional contributions to this policy:

Colonel Steven Sellers, Albemarle County Police Department
Sheriff Brian Roberts, Brunswick County Sheriff's Office
Chief Doug Middleton, Henrico County Department of Police
Ms. Shannon Dion, Office of the Attorney General
Sheriff Steve Dye, Russell County Sheriff's Office
SSA Marc Haalman, Virginia Department of Alcoholic Beverage Control
Officer Greg Hall, Virginia Department of Game and Inland Fisheries
Mr. David Summers, Virginia Department of Conservation and Recreation
Lt. Colonel James Caruso, Virginia Department of Military Affairs
Capt. Kirk Marlowe, Virginia Department of State Police
1st Sgt. Angelo Woodhouse, Virginia State Police

Virginia Department of Criminal Justice Services staff:

Teresa Gooch, Director, Division of Law Enforcement
Sam Hoffman, Standards, Policy and Homeland Security Manager
Gary M. Dillon, Manager, Virginia Accreditation Center

Definitions

Model Aircraft – Remote controlled aircrafts used by hobbyists, which are built, produced, manufactured and operated for the purposes of sport, recreation and/or competition. Model aircraft use is not regulated at the federal level and many UAS hobbyist belong to the Academy of Model Aeronautics, a professional association representing the interests of the hobby.

Unmanned Aircraft System (UAS) – The preferred industry definition of aircraft designed to navigate in the air without an on-board pilot. The authorization to use UAS is regulated by the Federal Aviation Administration (FAA). For the purposes of this policy guideline, UASs are non-weaponized.

UAS Flight Crew Member – A pilot, observer, payload operator or other person(s) assigned duties for a UAS flight mission or training exercise.

UAS Pilot – A person exercising control over a UAS during flight.

VTOL – Vertical take-off and landing

Potential Law Enforcement Applications

Accident Investigation
Missing Persons
Search and Rescue
Drug Investigations
Disaster Management
Crowd Control
Explosive Ordnance Disposal
Hostage and Barricade Situations
CBRNE Incident *(chemical, biological, radiological, nuclear, and explosives)*
Forensic Scenes
Support for Arrest Warrants
VIP Security Support
Perimeter Security
Low Cost Aerial Imagery
Enhance Situational Awareness

Protocols Based upon Legislation

Under current Virginia legislation, UASs cannot be used by law enforcement agencies for anything other than specified types of search and rescue or training. This legislation places a moratorium on their use, with exceptions, until July 1, 2015.

Protocols for the use of UASs currently must mirror those situations specified in that legislation, as listed below:

- Amber Alert
- Senior Alert
- Blue Alert
- Search or Rescue (To alleviate an immediate danger to a person)
- Training exercises related to these uses

Benefits to Officer and Community Safety

Unmanned Aerial Systems (UAS) do not require a qualified pilot on board to operate the UAS or the attached equipment such as cameras, FLIR (forward looking infrared), etc. UAS operators and system operators remain safely on the ground reducing their exposure to threats.

UASs are able to enter environments, which may be hazardous to pilots of manned aircraft. These threats may be natural or manmade. They include hazardous waste, fire, smoke, threatening weather, and ground fire from perpetrators.

UASs provide superior situational awareness while minimizing the danger to which operators are exposed.

UASs and trained operators minimize response time to most emergency situations. UASs can be launched from a safe location within close proximity to the scene.

UASs designed for law enforcement come in two categories, vertical takeoff and landing (VTOL), and fixed wing. This allows for their use in different environments that may restrict the size of the launch area. VTOL may be launched and landed in a very limited space.

UAS operators should be in direct contact with incident command, enhancing communication between command and air assets.

Community safety is enhanced by the rapid response of air assets to an emergency. Many UASs designed for law enforcement use can be launched within five minutes. In most cases manned aircrafts must take off and land at an airports under the direction of air traffic controllers, which can adversely delay response time.

UASs designed for law enforcement use are small enough to be stored in containers, which are the approximate size of a small backpack, or in small cases that can be carried in patrol vehicles, thereby minimizing response time.

Agencies wishing to utilize UASs must obtain a Certificate of Authorization (COA) from the Federal Aviation Administration (FAA) to ensure compliance with federal requirements thus ensuring UASs are operated in accordance strict federal guidelines.

Cost Benefit

The cost benefit of utilizing a UAS designed for public safety as compared to manned aircraft is substantial. It should be noted that UASs are not designed to take the place of manned aircraft. The use of UASs would supplement the aerial capabilities of a law enforcement agency to provide enhanced service to the public.

The Metro Aviation Unit, a joint effort by the City of Richmond, Chesterfield County, and Henrico County, operates four fixed wing aircraft (two Cessna 172s and two Cessna 182s). The average hourly cost to operate each of these aircraft is $150. The cost of purchasing a manned aircraft similar to those being utilized by the Metro Aviation Unit is in excess of $800,000. These figures do not include personnel costs.

According to the Association for Unmanned Vehicle Systems International (AUVSI), the average hourly cost of operating a UAS designed for public safety use ranges from $30 to $50. The costs of UASs designed for law enforcement ranges from a few hundred dollars to over $40,000. These figures do not include personnel costs.

Training

The FAA has developed the rules for the public's operation of UASs. They can be found in FAA Memorandum "Interim Operational Approval Guidance 08-01 Unmanned Aircraft Systems Operations in the U. S. National Airspace".

Agency model policy and operational procedures

Community Engagement

Law enforcement agencies interested in integrating UAS technology in their operations should actively engage their communities in an effort to educate the public. Due to extensive media coverage of military drone use, there is widespread fear of similar deployment tactics on Virginia soil. Additionally, civil liberties organizations have concerns about violations of 4^{th} Amendment rights.

1. Law enforcement agencies desiring to use UAS technology should first determine how they will utilize this technology, including the costs, benefits and risks.
2. Law enforcement agencies should then engage the community early in the planning process, including their governing body and civil liberties advocates.
3. It's imperative that the use of UAS technology be as transparent as possible to ensure the community that the law enforcement agency is in full compliance with the US Constitution, federal, state and local law governing search and seizure.
4. Law enforcement agencies should provide an opportunity for the community to review and comment on agency procedures for the use of UAS.
5. Transparency is the key to successful community support. For that reason, it is recommended that agencies work with the local media to help facilitate community education and dialogue.

System Requirements

1. Agencies deploying UAS technology shall maintain a flight log, which captures flight time, duration, date, supervisory authorization and reason for flight. UAS vehicles equipped with digital logs/counters are an acceptable alternative.
2. It is strongly encouraged that UAS vehicles should be painted in a high visibility paint or display high visibility markings, if the construction of the UAS permits. This will facilitate line-of-sight control by the pilot and allow for easier ground monitoring. In situations where covert operations are authorized (high risk search/arrest warrant), high visibility markings may not be optimal.
3. Equipping law enforcement UAS with weapons of any kind is strictly prohibited.
4. Law enforcement UAS technology shall be equipped with "auto return" technology, which automatically returns the vehicle to the launch location if radio connectivity is lost. For this reason, the use of "home built" aircraft or RC model aircraft is strongly discouraged.

Operational Procedures

1. All law enforcement UAS vehicles require a Certificate of Authorization (COA) from the Federal Aviation Administration (FAA). 0A law enforcement agency interested in deploying UAS technology should contact the FAA early in the planning process to determine the requirements of a COA.
2. UAS vehicles will only be operated by personnel, both pilots and crewmembers, who have been trained and certified in the operation of the system. All law enforcement agency personnel with UAS responsibilities, including supervisors and commanders, must complete training in the policies and procedures governing their use.

3. All flights will be approved by a supervisor and must be for a legitimate public safety mission, training or for demonstration purposes. Supervisory authorization shall be documented in the flight log.
4. A Virginia standardized flight log shall be used.
5. An authorized supervisor/commander will conduct a quarterly audit of flight logs. Unless as restricted by the Virginia FOIA, all flight logs and quarterly audits will be made available to the public upon request. Public agencies are encouraged to publish flight log information on their webpages.
6. Agencies must develop a disciplinary policy, which addresses unauthorized use of UAS technology.
7. Unless community or officer safety is compromised, agencies are encouraged to publically notify neighborhoods prior to using an UAS vehicle. The use of Reverse 911 telephone calls is a good example of a notification procedure.
8. When the primary mission is to collect evidence of a criminal incident AND the UAS vehicle will intrude upon the reasonable expectation of privacy, the law enforcement agency should consult with their Commonwealth's Attorney about obtaining a search warrant in advance of deployment.

Legal Considerations

Federal Legislation Governing the Use of UASs

The FAA Modernization and Reform Act of 2012 (49 U.S.C. § 40101, et seq.) is the only legislation passed by the United States Congress on the topic of unmanned aircraft systems. The act sets out requirements for new laws and regulations concerning unmanned aircrafts. The requirements are to ensure public safety and uniformity throughout national airspace and that civil unmanned aircraft systems include a sense and avoid capability. The act defines different types of unmanned aircraft and aircraft systems including:

1. **Unmanned aircraft** – an aircraft operated without the possibility of direct human intervention from within or on the aircraft.

2. **Small unmanned aircraft** – an unmanned aircraft weighing less than 55 pounds.

3. **Unmanned aircraft system** – an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) required for the pilot in command to operate safely and efficiently in the national airspace system.

4. **Public unmanned aircraft system** – an unmanned aircraft system meeting the qualifications and conditions required for operation of a public aircraft.

Law enforcement agencies should be aware that laws and regulations related to the use of UAS are evolving and what may be true today is not necessarily true tomorrow. For example, the FAA is expected to release proposed rules later this year establishing policies, procedures and standards for small UAS which law enforcement may use. Additionally, there are several bills under consideration by the U.S. Congress, including: Preserving American Privacy Act of 2013, Preserving Freedom from Unwarranted Surveillance Act of 2013, Drone Aircraft Privacy and Transparency Act of 2013, and Safeguarding Privacy and the Fostering Aerospace Innovation Act of 2013. Enactment of these bills will impact law enforcement agencies' use of UASs and agencies should diligently monitor the law for future changes.

Federal Communications Commission Considerations

The Federal Communications Commission (FCC) regulates the use of radio frequencies, which UASs depend upon for operation. Frequencies allow the ground operator to control the device and collect surveillance data but are subject to interference. Some UAS systems available at retail stores include FCC approved frequencies that are shared by many users, which means reliability and security of the system may be at risk. For example, a UAS operating on a shared frequency may not maintain adequate connectivity between the device and the ground operator, thereby increasing the risk of losing control of the device. If control is lost, the device may crash into the ground or other property. Shared frequencies are also not secure, meaning a sophisticated user could intercept the frequency and access data sent from the UAS to the ground operator. Both scenarios involve liability issues for agencies which should be thoroughly considered before utilization of a UAS.

On the other hand, some UAS manufacturers have safeguards in place to decrease the risk of frequency interference. Some systems use encrypted communications and technology to prevent detection and unauthorized access. "Pairing" a UAS and ground control station creates a unique line of communication, which prevents outside linkage to the system. Other safeguards include key recognition, monitoring for interference and lost link modes.

If an agency wants a more secure frequency with which to control their UAS, it should petition the FCC for a designated spectrum for law enforcement. Doing so does not guarantee protection from interference, as the device itself must have built in safeguards to protect against interference and consequence mitigation in the event there is a communication breech. In summary, law enforcement agencies should thoroughly research various types of UAS systems to determine which model offers the best security measures for its intended use. Agencies are encouraged to contact the Virginia State Police Communications Division for additional guidance.

Freedom of Information Act

The Virginia Freedom of Information Act (FOIA) "ensures the people of the Commonwealth ready access to public records in the custody of a public body or its officers and employees, and free entry to meetings of public bodies wherein the business of the people is being conducted." All public records are presumed open unless a public body properly invokes an exemption and does not disclose the records. Va. Code §§ 2.2-3700-3714. Law enforcement agencies should consider the applicability of statutory exemptions for their public records regarding UASs. For example, an agency may elect to withhold records contained in criminal investigative files which include photographs taken by an UAS or specific tactical plans utilizing UAS technology. See Va. Code 2.2-3705.2 and 2.2-3706. Other exemptions may apply depending on the situation and agencies are advised to consult with their legal counsel in drafting responses to FOIA requests.

Agencies with specific FOIA questions are encouraged to contact the Virginia Freedom of Information Advisory Council at http://foiacouncil.dls.virginia.gov/ or (804) 225-3056.

Image Retention

The Government Data Collection and Dissemination Practices Act (Va. Code §§ 2.2-3800 – 3809), or the "Data Act," addresses how agencies handle personal information obtained through various methods. The Data Act defines personal information as information providing a basis for inferring personal characteristics, such as "photographs or things done by or to such individual." The Data Act specifies that personal information shall not be collected unless need for the information has been clearly established, shall be relevant for the purpose it is collected, shall not be misused, and must be collected within the confines of the law. However, the Data Act does not apply to personal information systems maintained by the Department of the State Police or other police departments that deal with investigations and intelligence gathering relating to criminal activity. (Va. Code § 2.2-3802(7)).

A recent Attorney General opinion addresses the use of license plate readers and whether information obtained by these devices can be kept by law enforcement. (2013 Op. Va. Att'y Gen. No. 12-073, *available at* www.ag.virginia.gov.) The answer depends on whether the information collected is for a specific criminal matter, which is exempt from the Data Act, or whether the information is collected for potential future use, which is subject to the Data Act. As applied to law enforcement's use of UAS to collect images, if the images are obtained for no particular reason, the Data Act prohibits law enforcement from storing the information for future use. However, if the UAS is deployed for a particular purpose directly related to "investigations and intelligence gathering related to criminal activity" the Data Act does not apply.

Federal Aviation Administration

Law enforcement agencies utilizing UAS technology must comply with federal laws and regulations which currently require public entities, such local police departments, to obtain a Certificate of

Authorization or Waiver (COA) before using an UAS in civil airspace. The primary purpose of the COA is to avoid in-air collisions with other objects in the air. Applicants apply online and the FAA evaluates the proposed operation for safety feasibility. For a complete listing of regulations, visit: www.faa.gov/regulations_policies/faa_regulations

The COA allows an operator to use a defined area of airspace and includes special provisions unique to the proposed operation. COAs usually are issued for a specific period and most require the applicant to coordinate with an air traffic control facility. Because UAS technology cannot currently comply with "see and avoid" rules that apply to all aircraft, a visual observer must maintain visual contact with the UAS and serve as its "eyes" when operating outside airspace restricted from other users.

Applying for a COA: https://ioeaaa.faa.gov/oeaaa/

Who may apply for a COA? Only public agencies operating an unmanned aircraft. A public agency is any agency that operates a public aircraft (14 CFR Part 1.1). If you receive funding from the federal government at some level, you are probably a public agency. A public agency can never operate under the guidelines of Advisory Circular 91-57 (Model Aircraft Operating Standards).

Additional Resources: "*Unmanned Aircraft Systems Operations in the U.S. National Airspace System – Interim Operational Approval Guidance*" provides FAA guidance for public use of unmanned aircraft by defining the COA evaluation process.
www.faa.gov/about/office_org/headquarters_offices/ato/service_units/systemops/aaim/organizations/uas/coa/faq/media/uas_guidance08-01.pdf

4th Amendment Considerations

The 4th Amendment protects individuals and their homes from unreasonable, warrantless searches and seizures by government actors. People have certain expectations of privacy in their property, particularly in their homes. Several doctrines have emerged by courts in balancing individual privacy and the need for government to keep people safe. The plain view doctrine authorizes warrantless searches when an officer, in a lawful place, can plainly see an item of incriminating character. The open fields doctrine recognizes that a person has less expectation of privacy outside of his home.

Applying the 4th Amendment to UAS surveillance is new territory for both law enforcement and the courts. The constitutionality of this technology as used by law enforcement will depend on many factors, including how and where the surveillance takes place. Whether a target is at home or in a public place will affect a court's analysis of how strong his expectation of privacy is. Other factors include the type and length of surveillance. The following cases primarily focus on manned airplane and helicopter flights but may be helpful to law enforcement agencies navigating the unchartered waters, or airspace in this instance, of using UAS technology in a manner that respects the 4th Amendment.[1]

Privacy in the Home

Kyllo v. U.S., 533 U.S. 27 (2001). Receiving tips from an informant, a federal agent acting without a warrant used a thermal imaging device to view Kyllo's home to help determine whether he was growing marijuana inside. Based on information yielded by the device, a warrant was obtained to search the home.

[1] See "*Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses*," by Congressional Research Service, April 3, 2013, at www.fas.org/sgp/crs/natsec/R42701.pdf for additional information.

The Supreme Court ruled that use of the thermal imaging device to gather information about the inside of the home constituted a search under the 4th Amendment.

Property Rights

Florida v. Jardines, 569 U.S. __ (2013). Officers brought a narcotics dog to defendant's front porch, which alerted for the presence of drugs. A search warrant was obtained for the home and marijuana plants were subsequently found. Using a property-rights analysis, the court concluded that using a trained dog on the front porch of a home was a physical intrusion on defendant's 4th Amendment rights. Unlike simply knocking on the door, which is a customary and routine act, bringing a police trained dog is neither customary nor routine. Because the officers only learned about the drugs by physically intruding on the defendant's property in order to gather evidence, an unlawful search occurred. (This case may be applicable if UASs are used in close proximity to homes in order to peer into windows.)

Open Fields and Manned Aerial Surveillance

Wellford v. Virginia, 227 Va. 297 (1984). After receiving a tip that Wellford was growing marijuana plants, law enforcement used a helicopter to fly 1000 feet above his fields and observed marijuana plants. Defendant was arrested after being observed caring for the plants. The court ruled that the open field was not part of the home's curtilage and therefore defendant had no expectation of privacy.

California v. Ciraolo, 476 U.S. 207 (1987). After receiving a tip that Ciraolo was growing marijuana plants in his backyard, which was shielded from view at ground level with a fence, law enforcement conducted warrantless aerial surveillance at 1000 feet. Officers, using nothing more than their "naked eyes," observed marijuana plants in the yard, which led to a search warrant of the property. The naked-eye aerial surveillance did not violate a reasonable expectation of privacy because it "took place within public navigable airspace in a physically nonintrusive manner."

Giancola v. West Va. Dep't of Pub. Safety, 830 F.2d 547 (4th Cir. 1987). Aerial surveillance from a helicopter flying at 100 feet did not violate the 4th Amendment. The aerial surveillance tactics were not unreasonably intrusive after considering the total number of surveillances conducted (two), the frequency of the surveillance, the length of each surveillance, altitude, number of aircraft (one), the degree of disruption of legitimate activities on the ground, and compliance with flight regulations.

Florida v. Riley, 488 U.S. 445 (1989). After receiving an anonymous tip that marijuana was growing in a greenhouse located ten to twenty feet behind a mobile home, law enforcement flew a helicopter over the property at an altitude of 400 feet. Marijuana was observed growing inside the greenhouse, which led to the issuance of a search warrant. In denying the motion to suppress the Court reasoned the helicopter was flying at a legal altitude, met all flight regulations, and that any member of the public could have legally taken the same flight and made the same observations. Therefore, Riley had no reasonable expectation of privacy in the greenhouse.

U.S. v. Breza, 308 F. 3d. 430 (5th Cir. 2002). During a drug interdiction helicopter flight, law enforcement officers observed what they thought were marijuana plants in an area surrounding Breza's dwelling. After descending to approximately 200 feet, this suspicion was confirmed and officers on the ground, without a warrant, searched the garden and seized hundreds of marijuana plants. The 4th Circuit held that the surveillance did not violate the 4th Amendment because the flight fully complied with all laws and regulations and were a regular occurrence. The court also upheld the warrantless entry because the defendant was observed burning the marijuana plants.

Agency/Operator Certifications

Pilot & Observer Certifications/Qualifications

It should be noted that all certifications/qualifications herein are applicable to operations of UAS at and below 400 feet. All pilot and observer training records will be maintained by the agency employing those persons and are subject to state and federal inspection.

Pilots:

Each UAS pilot must be an FAA-certificated airman or successfully pass either the FAA's pilot knowledge exam or complete an FJ\1\-approved UAS pilot training curriculum. However, if operating in controlled airspace, additional certifications are required. *Note*: Certification does not require the practical fight requirements of a manned aircraft.

Pilots will receive training specific to the UAS to be operated. This training must be conducted and documented by a qualified instructor designated by the proponent as being the individual(s) trained and certified by the manufacturer to provide training on the specified UAS.

Pilots must not perform duties for more than one UAS at a time and are not allowed to perform concurrent duties both as pilot and observer.

Pilots are prohibited from flying any law enforcement mission without having completed three UAS flight events within the preceding 90 days.

Law enforcement standard operating procedures (SOP) must include Crew Resource Management (CRM) techniques to ensure the highest possible situational awareness and effective communication by pilots during each flight operation. Pilots must be trained in these procedures and techniques. ***Note*:** CRM training involves a wide range of knowledge, skills and attitudes to include communications, situational awareness, problem solving, decision making, and teamwork. CRM is defined as a management system which makes optimum use of all available resources – equipment, procedures and people – to promote safety and enhance the efficiency of operations.

All pilot training must be conducted and documented by a qualified instructor designated by the proponent as being an individual trained and certified.

Pilots must be medically qualified and have in their possession a second class (or higher) airman medical certificate that has been issued under 14 CFR Part 67, Medical Standards and Certification.

Pilots are subject to the provisions of 14 CFR § 91.17, Alcohol and Drugs.

Observers:

Observers must successfully complete a UAS observer training curriculum that includes, at a minimum, instruction on rules and responsibilities described in 14 CFR § 91.111, Operating Near Other Aircraft, 14 CFR § 91.113, Right of Way Rules, Cloud Clearances, and that emphasizes "See and Avoid" concepts and fundamental radio communications, including standard ATC phraseology. Observer training must include thorough instruction regarding manned aircraft traffic conflicts and pilot communications for any maneuvers/actions required to avoid traffic conflicts.

Observers must not perform duties for more than one UAS at a time and are not allowed to perform concurrent duties both as pilot and observer.

Law enforcement standard operating procedures (SOP) must include Crew Resource Management (CRM) techniques to ensure the highest possible situational awareness and effective communication by observers during each flight operation. Observers must be trained in these procedures and techniques.

All observers training must be conducted and documented by a qualified instructor designated by the proponent as being an individual trained and certified by the manufacturer to provide training on the specified UAS.

Observers must be medically qualified and have in their possession a second class (or higher) airman medical certificate that has been issued under 14 CFR Part 67, Medical Standards and Certification.

Observers are subject to the provisions of 14 CFR § 91.17, Alcohol and Drugs.

It should be noted that the FAA is working to change the requirement for a second-class airman medical certification to self-certification as to being healthy to fly and a letter from a competent medical authority certifying the operator's eyesight to the second-class medical certification requirements of correctable to 20/20.

Memorandum of Understanding Between Federal Aviation Administration and the U.S. Department of Justice, Office of Justice Programs, National Institute of Justice Concerning Operation of Unmanned Aircraft Systems by Law Enforcement (www.alea.org/assets/pressReleases/assets/1805/DOJ%20FAA%20MOU.pdf)

Regulatory Considerations

24VAC5-20-100. Operation of aircraft.

All aircraft operations shall be conducted in conformity with Federal Aviation Regulations as amended from time to time and violation of such federal regulations shall also constitute a violation of this chapter.

Statutory Authority

§§ 5.1-2.2 and 5.1-2.15 of the *Code of Virginia.*

Historical Notes

Derived from VR165-01-02:1 § 2.9, eff. September 9, 1992.

Section 11

Privacy Impact Assessment
for the

Aircraft Systems

DHS/CBP/PIA-018

September 9, 2013

Contact Point
Lothar Eckardt
Executive Director, National Air Security Operations
Office of Air & Marine
U.S. Customs and Border Protection
(202) 344-3950

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) employs several types of aircraft including manned helicopters and fixed-wing aircraft, and Unmanned Aircraft Systems (UAS) for border surveillance and law enforcement purposes. These aircraft are equipped with video, radar, and/or other sensor technologies to assist CBP in patrolling the border, conducting surveillance as part of a law enforcement investigation or tactical operation, or gathering raw data that may assist in disaster relief or responses to other emergencies. Video, images, and sensor data collected through these Aircraft Systems alone cannot be used to identify a person, but they may later be associated with a person as part of a law enforcement investigation or encounter with CBP officers or agents. DHS/CBP is conducting this Privacy Impact Assessment to evaluate the privacy impact of these technologies on persons.

Introduction

The Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) is responsible for guarding nearly 7,000 miles of land border the United States shares with Canada and Mexico and 2,000 miles of coastal waters surrounding the Florida peninsula and off the coast of Southern California. The agency also protects 95,000 miles of maritime border in partnership with the United States Coast Guard. To achieve these missions, CBP employs several types of aircraft, including manned helicopters and fixed-wing aircraft, and Unmanned Aircraft Systems (UAS) for border surveillance and law enforcement purposes. These aircraft are equipped with video, radar, and/or other sensor technologies to assist CBP in patrolling the border, conducting surveillance as part of a law enforcement investigation or tactical operation, or gathering raw data that may assist in disaster relief or other emergencies. This Privacy Impact Assessment (PIA) is necessary because the aircraft are equipped with technology that captures information that may be associated with persons whom CBP encounters.

Overview

CBP employs several types of aircraft to achieve its mission objectives. All aircraft, manned or unmanned, have some type of imaging capability such as video, still images collection, and/or radar. The UAS differ from CBP's manned aircraft only in that the pilot controls the aircraft from the ground and the aircraft are capable of flying farther distances and longer hours continuously. All aircraft are owned and operated by the Office of Air and Marine (OAM); the Office of Intelligence and Investigative Liaison (OIIL) is responsible for processing, exploitation, and dissemination (PED) of imagery transmitted from aircraft.

CBP aircraft, both manned and unmanned, are used in the following scenarios: (1) to patrol the border; (2) to conduct surveillance for investigative operations; (3) to conduct damage assessment in disaster situations; and (4) in response to officer safety scenarios. While CBP also allocates its air assets in a manner that reflects this prioritization, CBP reviews and considers all requests for assistance. Lastly, CBP does not equip its aircraft with weapons. While the crew in all manned aircraft and the officers and agents onboard the aircraft during tactical missions do carry weapons, the various aircraft are not equipped with armaments.

Helicopters

CBP operates several types of manned rotary-wing aircraft (helicopters) in support of its mission, notably, the American Eurocopter AS-350, Augusta Westland AW-139, Bell Huey UH-1, and Sikorsky UH-60. CBP uses helicopters for observation, for tracking suspects and supporting ground units, aerial reconnaissance of moving objects and persons, external lift capability for seizures and equipment delivery, and tactical support and transportation for law enforcement activities. Areas of operation include the border environment, both land and sea, to observe and interdict unlawful crossings of persons and goods, the airspace surrounding defined DHS National Special Security Events or critical venues, and populated or unpopulated areas that are the subject of defined law enforcement activity or investigation. CBP's helicopter fleet operates out of 30 locations maintained by OAM across the United States.

Fixed-wing Aircraft

CBP has manned fixed-wing P-3 AEW/LRT Orion aircraft operating out of specific operations centers in Corpus Christi, TX and Jacksonville, FL. CBP practices a defense in depth strategy of the borders of the United States and in active prosecution of attempts to smuggle persons or contraband by extending surveillance over international and coastal waters. As part of this strategy and as a means of integrating with the overall U.S. Government strategy to interdict the flow of narcotics and controlled substances across the U.S. southern borders, this defense in depth includes expanding the area of patrol to include the Caribbean and Eastern Pacific waters that border Source and Transit Zone countries.[1] Together the operations centers operate the P-3 aircraft primarily in Central and South America. Certain P-3s are used to intercept and track both aircraft and vessels for hours at a time while maintaining a covert standoff. CBP also operates several smaller, manned, fixed-wing aircraft out of OAM operational locations. These fixed-wing aircraft include piston-engine propeller-powered aircraft (Cessna models), larger turbo-prop powered aircraft (Bombardier Dash Eight, Pilatus, and Beechcraft Super King Air), and jet aircraft (Cessna Citation). These aircraft variously perform surveillance, tracking, interdiction, intercept, and information gathering roles. Fixed-Wing Aircraft employ various types of sensor technology including video, still, and radar images, and Law Enforcement Technical Collection (LETC) (electronic signals information across the electromagnetic spectrum).

---

[1] Source and Transit Zone countries are those nations working in partnership with the United States to interdict the flow of narcotics and controlled substances to the United States through the Caribbean Basin and along the coastal waters of the eastern Pacific Ocean. http://www.whitehouse.gov/ondcp/transit-zone-operations.

UAS

A UAS encompasses an unmanned aircraft, digital network, and personnel on the ground who operate the aircraft. CBP currently owns and operates ten such aircraft. The UAS aircraft include the Predator B[2] and the maritime variant of the Predator B, the Guardian, which allows CBP to conduct missions in areas that are remote, too rugged for ground access, or otherwise considered too high-risk for manned aircraft or personnel on the ground. The aircraft are stationed and principally controlled at four locations: Sierra Vista, AZ (4 aircraft); Grand Forks, ND (2 aircraft); Corpus Christi, TX (2 aircraft); and Cape Canaveral, FL (2 aircraft). CBP's UAS operate in accordance within the Federal Aviation Administration (FAA) Certificate of Authorization (COA) process. CBP works with the FAA to develop the COAs to define airspace for UAS operation. Consistent with the primary mission for the UAS, these COAs, which are in effect for a period of two years, define airspace (altitude, latitude, and longitude (geography)) along the border and outside of urban areas to support CBP UAS flight operations. As the FAA develops its roadmap to integrate UAS into the National Airspace System (NAS)[3], CBP will adjust to these new requirements and continue to employ UAS in pursuit of its primary border security mission.

Uses of Aircraft

Patrol

CBP uses all of its aircraft to patrol different parts of the border based on the specific strengths of the different aircraft. CBP P-3s patrol in a 42-million square mile area of the Western Caribbean and Eastern Pacific, known as the Source and Transit Zone, in search of drugs that are in transit towards U.S. shores. The P-3's distinctive detection capabilities allow highly-trained crews to identify emerging threats well beyond U.S. land borders. By providing surveillance of known air, land, and maritime smuggling routes in an area that is twice the size of the continental U.S., the P-3s detect, monitor, and disrupt smuggling activities before they reach shore.[4] As part of this patrol responsibility, images and radar information obtained in detecting, monitoring, or supporting activities is collected and maintained either for direct case support or to permit historical trend analysis regarding smuggling routes.

Along both the northern and southern borders CBP also employs UAS and smaller manned aircraft to help agents detect, identify, apprehend, and remove individuals and

---

[2] The General Atomics Aeronautical Systems MQ-9 Predator B is a mid-size Unmanned Aerial Vehicle (UAV) approximately thirty-six feet in length, with a maximum gross weight of 10,500 pounds and a wing span of sixty-six feet.

[3] See, *FAA Modernization and Reform Act of 2012*, Pub. L. No.112-95, sec. 331, 126 Stat. 11, 72, which mandates that the FAA prepare a roadmap to integrate UAS into the NAS by 2015.

[4] The Anti-Drug Abuse Act of 1988 established the Office of National Drug Control Policy (ONDCP) to set priorities, implement a national strategy, and certify Federal drug-control budgets. Interdiction of the flow of illicit drugs through the Source and Transit Zone is a critical component of the National Drug Control Strategy prepared annually by ONDCP.

contraband illegally entering the United States at and between Ports of Entry (POE). The COA defined airspace establishes operational corridors for UAS activity both along and within 100 miles of the border for the northern border, and along and within 25 to 60 miles of the border for the southern border, exclusive of urban areas. CBP helicopters and manned fixed-wing aircraft may operate in and around urban areas; however, the principal mission remains focused on those areas between the POE. Images, LETC, and radar information, specifically with respect to border areas between the POEs, are collected in support of case development or to permit trend analysis.

Following a flight, the images are provided to OIIL for processing, exploitation, and dissemination. Subsequently, and only upon request, OIIL provides access to the forensic analysis of a particular image and area to authorized persons who have a "need to know;" when the dissemination is in response to a particular law enforcement activity or case, that analysis may include PII.

Persons who are apprehended and who were video recorded from a UAS or a manned aircraft may have the video of their crossing and/or apprehension associated with a case file that contains their PII.

Separately, CBP also deploys manned fixed-wing aircraft with LETC sensors over the border area in support of its counter-terrorism and interdiction of smuggling operations. The LETC sensors permit surveillance of the electromagnetic spectrum for the purpose of identifying organized border crossing activity between the ports of entry.

Investigative Operations

CBP uses both UAS and manned aircraft in support of other DHS components, such as U.S. Immigration and Enforcement (ICE), or other federal law enforcement agencies, such as the Federal Bureau of Investigation (FBI) or Drug Enforcement Agency (DEA). Requests for aircraft support that are related to the border surveillance must be directed to the Assistant Commissioner, OIIL, for authorization. Each request for information follows a standard process and is reviewed and considered in terms of the requesting agencies' authorities to receive the sought after information, CBP's own authority to lend assistance, and CBP's ability to integrate the information collection into its mission. Separately, OAM must determine the availability of aircraft type and the integration of the requested activity into its flight operations.

Typical support missions include overhead observation of previously identified persons, specified locations, and particular conveyances for enhanced situational awareness and increased officer safety. For example, the UAS could conduct surveillance over a building to inform ground units of the general external layout of the building or provide the location of vehicles or individuals outside the building. When flying a UAS in support of another component or government agency for an investigative operation, CBP may provide the other agency with a direct video feed through access controls or with a downloaded video recording of the operation, in whole or in part, based on the request. Similarly, CBP may deploy a helicopter or manned fixed-wing aircraft to provide over top visibility into a developing incident. Video images from the Electrical Optical/Infrared ball (EO/IR) ball are fed through the DHS firewall to "Big Pipe," a video and image distribution network operating within the CBP/DHS firewall, to identified users, analysts, and decision makers for real-time mission support and border protection.

Disasters

The P-3 may be used to conduct reconnaissance missions during natural disasters in support of FEMA. During these missions, P-3s can provide near real-time, high quality video of affected areas to first responders and FEMA. P-3s are equipped with similarly capable EO/IR Ball cameras; the images are also fed through a transmission to a ground station where the video is decrypted and fed to Big Pipe to disseminate inside the DHS firewall to authorized users within DHS and any other requesting agency.

UAS may also be used outside existing COAs during natural disasters once the government has issued a disaster declaration. For example, the UAS may fly missions in support of other government agencies such as the National Oceanic and Atmospheric Administration (NOAA) or FEMA to provide video or radar images of flooding. In disaster situations, CBP works with the FAA to construct a COA defining the airspace where a CBP UAS may operate. The UAS may provide a real-time feed during flight through Big Pipe or, subsequently, an analyzed image comparing the raw feed to an image with identified details, noting changes, to FEMA, state emergency operations centers, United States Geological Survey (USGS), and/or the Army Corps of Engineers. Video from these operations are not used to identify individuals. As with other requests for support, disaster area overflight requests are assigned in accordance with the national policy regarding the tasking of CBP air assets.

Officer Safety and Support to State and Local Law Enforcement

State and local law enforcement officials may request aircraft support (e.g., UH-60, P-3, UAS) in emergency situations; often this involves circumstances when officer safety is implicated, and in which aerial surveillance is necessary or the terrain would be too difficult for law enforcement personnel to navigate. OIIL reviews each request to determine whether to respond and OAM reviews how and in what context it may respond. Based on both organizations within CBP, a decision is made whether to provide assistance. Access to video taken during emergency situations may be provided, either at a DHS/CBP facility or by temporarily granting direct access through the DHS firewall. Sharing of this information with state, local, or other government agencies is on a case by case basis as determined through CBP's Request for Information process.

As in the mission uses discussed above, UAS and manned aircraft offer several options for deploying information gathering equipment. The UAS can serve as force multiplier insofar as the UAS enables the monitoring of large areas of land more efficiently and with fewer personnel than other aviation assets. UAS can enhance situational awareness and increase officer safety by providing aerial support to officers on the ground by monitoring a fixed location while flying at a high altitude to reduce the likelihood of detection. Manned aircraft offer the ability to fly in more congested airspace and to transport officers, agents, equipment, and seized assets.

Technology on Board the Aircraft

The various aircraft have different types of surveillance technology. Most aircraft, manned and unmanned have an EO/IR ball attached to provide a means of collecting information. The EO/IR ball installed on the UAS also assists the pilot during take-off and landing. While the cameras on each aircraft are not identical, they have almost identical performance specifications. The EO/IR ball is a camera, which employs a fixed-focus lens, that is capable of providing video at any altitude and allows operators, using digital zooming (software based image enhancement), to take small-scale aerial video images of buildings, vehicles, and people. Aircraft altitude directly affects a fixed-focus camera's performance; the higher the aircraft's altitude, the less detail an operator is able to see.

A lower altitude permits the EO/IR ball to provide greater detail in an image, which may permit identification; this observation activity, however, does not occur unnoticed or subject to attempts at evasion, and therefore is more often part of a defined law enforcement operation. Persons are often successful at hiding their identity from known surveillance aircraft by simply looking away.

At present, the flight and mission parameters for the UAS place their operation within an altitude block of 19,000 to 28,000 feet, thereby effectively limiting the altitude for the EO/IR ball on a UAS to a minimum of 19,000 feet. At this minimum altitude, the camera does not provide enough detail for an operator to identify a person (that is to discern physical characteristics such as height, weight, eye color, hair style, or a facial image). The camera operator may have enough detail to identify whether an individual is carrying a long gun or wearing a back pack. At an altitude of 19,000 feet the camera operator cannot read a license plate, nor are license plate readers effective.

Conversely, the flight parameters for helicopters and fixed-wing aircraft are broader in terms of altitude and geography; their flight operations are integrated into the NAS and do not require a COA. The mission parameters and physical capabilities for helicopters and manned fixed-wing aircraft, however, place different operational restrictions upon the aircraft.

The EO/IR ball can provide daytime or nighttime visual video observation of movement or objects on the ground. The images, depending upon the aircraft deploying the camera, tend to be small in scale, to provide environmental context. A principal purpose for tracking a person or vehicle from an aircraft with an EO/IR ball is to assist CBP or law enforcement personnel on the ground with information to permit a safe encounter—this requires environmental context more than a best possible close-up of a face. When viewing vehicles, an operator can distinguish a car from a truck, and depending on the altitude at which the aircraft is flying, may be able to identify the model of the vehicle. During daytime flights, an operator may also be able to determine the color of the vehicle. The images of vehicles and/or individuals recorded by the EO/IR ball are not associated with any biographical information unless the individual is apprehended, at which point the video may be associated with the Personally Identifiable Information (PII) contained within the individual's case file.

In addition to EO/IR CBP deploys a UAS stationed along the Southwestern border in Sierra Vista, AZ, with the Wide Area Surveillance System (WASS). WASS uses a sensor mounted to the wing of a UAS to sweep large areas of border territory (approximately six kilometers in width) as the aircraft moves along its flight path. WASS alerts CBP to the existence of persons and/or vehicles along the border and provides coordinates to determine their location. The UAS pilot and sensor operator can then inform ground units of the location so that Border Patrol may coordinate an interdiction of the persons or vehicles. WASS provides a radar sensor image, which CBP may share through Big Pipe during operation.

Some manned and unmanned aircraft are also equipped with synthetic aperture radar that can provide black and white images in all weather. This radar can provide silhouettes of people and vehicles, but provides no identifying details. Using this technology, an operator is not able to pick up identifying characteristics of a person or a vehicle. The synthetic aperture radar is primarily used for change detection. For example, the operator can identify tire tracks on the ground that were not present in prior images provided by the radar. Similarly, an operator can use the synthetic aperture radar to determine the extent of flooding in a particular region by noting the changes to the topography.

Certain manned fixed-wing aircraft deploy LETC sensors used to detect electronic signals in the electromagnetic spectrum. These specifically designed aircraft operate in support of counter-terrorism efforts and to interdict organized smuggling (people, contraband, and controlled substances) operations within the border area. Like with the EO/IR ball, information from LETC sensors may be employed to support officers and agents on the ground as they move to a position where they can safely encounter observed persons. LETC aircraft sensors are solely deployed on manned fixed-wing aircraft.

Data on the digital video recorders on CBP aircraft are maintained for a maximum of 30 days and then overwritten by new data. The images and related data from CBP aircraft, both manned and unmanned, are provided through Big Pipe to identified users, analysts, and decision makers for real-time mission support and border protection. Images from the EO/IR ball mounted on the UAS are sent by an encrypted transmission, first to the satellite providing the control signals, and then, again by encrypted transmission, to the ground control station where the pilot and sensor operator are located. The image data is decrypted and brought inside the

DHS firewall at the ground control station, where Big Pipe can ingest the data and provide a feed to assigned users and analysts.

Big Pipe is a fully distributed network hosted by CBP and supports not only event-based law enforcement missions, but also FEMA's National Response Framework.[5] Big Pipe employs role-based access controls to provide users possessing a need to know access to distinct video feeds at command centers, other CBP/DHS locations, and for authorized persons with technical access through the DHS firewall. OAM retains control over defining users for Big Pipe and assigning access. After the creation of live mission data, Big Pipe manages the transmission, processing, distribution, consumption, and storage of the live mission data. Big Pipe archives selective mission data on a Big Pipe server hard drive for a maximum of 7 days, after which the data is deleted. Big Pipe does not use PII to retrieve stored mission data. Stored data is retrieved based on the date and time of the mission and only by authorized users on a need to know basis. If data is used for investigative purposes, and associated with a particular individual it goes into a case management system, which is covered by the corresponding Privacy Act System of Records Notice (SORN) for the case management system. Big Pipe, separately, provides a feed of video and radar images from UAS to the Air and Marine Operations Center (AMOC), where OIIL operates one of several PED cells to review this data over time to perform trend analysis and change detection. Video and radar images maintained by a PED cell, such as at the AMOC, are stored on a separate server dedicated to the PED cell mission for up to five years. The analyzed images may be shared by OIIL in response to law enforcement needs.

Summary of Privacy Risks

The use of these aircraft and accompanying surveillance technologies presents several privacy concerns. The first concern is ensuring that CBP's collection and use of data from aerial surveillance remains within the scope of its authorities to protect the border and provide support for law enforcement activities, while continuing to preserve a person's right to privacy. CBP's border security mission has a broad mandate to determine the admissibility of persons and ensure that goods are not introduced into the United States contrary to law.[6] Similarly, the statutory language in CBP's annual appropriations directs CBP Air and Marine to provide integrated and coordinated border interdiction and law enforcement support for homeland security missions, including assistance to federal, state, and local agencies and emergency humanitarian efforts; to provide airspace security for high-risk areas or National Special Security Events[7]; and to combat

[5] The National Response Framework is a DHS/FEMA led effort, which provides the guiding principles that establish a comprehensive, national, all-hazards approach to domestic incident response—from the smallest incident to the largest catastrophe. http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf.
[6] Title 8, United States Code (U.S.C.), sections 1225, 1357, other pertinent provisions of the immigration laws and regulations; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1595a(d), and other pertinent provisions of customs laws and regulations.
[7] See Title 18 U.S.C. Section 3056, which authorizes the designation of National Special Security Events.

efforts to smuggle narcotics and other contraband into the United States[8]. Deploying OAM's various air assets to support these missions improves DHS/CBP's capability to obtain streaming video, and to assess critical infrastructure before and after events.

CBP's use of manned and unmanned aircraft to conduct aerial observations is consistent with CBP's authorities and obligations. To the extent that aircraft flying in support of tactical operations overfly private residences, there is a minimal risk that a person's privacy might be unintentionally violated. The images captured are not personally identifiable without further investigative information. Neither manned nor unmanned aircraft physically intrude upon or disturb the use of private property. Further, the cameras deployed on UAS or manned aircraft do not have the capability to see through walls or otherwise collect information regarding what occurs in the interior of a building, nor is that their purpose. UAS operate primarily at an altitude between 19,000 and 28,000 feet pursuant to their COA approved by the FAA, and are focused as previously described.

A second privacy concern, specific to UAS, is that they present a perceived risk to privacy because they are able to fly for longer hours than manned aircraft and conduct surveillance undetected. Like other aircraft, UAS are useful for monitoring remote land border areas where patrols cannot easily travel and infrastructure is difficult or impossible to build. Unlike manned aircraft, UAS are operated by personnel on the ground, allowing the crew to be relieved while the UAS is still in the air. This capability allows UAS to provide long-range surveillance for greater lengths of time than manned aircraft. Because of their small size compared to manned aircraft, and the altitude at which UAS can operate, these physical attributes may serve to conceal the presence of a UAS and reduce detection of their operating noise while still being able to maneuver over a small area and provide surveillance. Other OAM operated long range fixed-wing aircraft cannot steadily monitor a set location because of their size and turning radius. Helicopters are more easily detected because of their noise and lower operational altitudes. This means that, unlike fixed-wing aircraft and helicopters, UAS can monitor either a moving target or a fixed location for relatively longer periods of time without the likelihood of detection.

While UAS can fly for longer periods of time, they are equipped with the same technology to conduct surveillance that is presently deployed on CBP manned aircraft. The only sensor available on UAS that is not used by CBP manned aircraft currently is the WASS sensor. The WASS sensor can only detect the presence of a person and track his or her movements (much the same way other radar technology can detect an object and track its movement); it cannot be used to identify a person. The WASS sensor is designed to sweep large areas of land and is only used to patrol along the southwest border and to assist with interdictions. Other technologies on the UAS are shared by CBP's manned aircraft. Putting these technologies on a

[8] See National Drug Control Strategy, http://www.whitehouse.gov/ondcp/2013-national-drug-control-strategy.

UAS only enhances CBP's ability to perform its existing functions. For instance, CBP's surveillance video of a location used to smuggle persons or contraband using a UAS instead of a P-3 may be longer in duration with less interruption and less likelihood of detection.

To mitigate the risk presented by longer sustained surveillance of an individual or residence without the individual's knowledge, CBP has strict mission priorities for UAS and all aircraft operations. For instance, CBP aircraft may only be used in support of an authorized mission or investigation, the video or other data collected from CBP aircraft may only be accessed by authorized personnel with an authorized need to know, and the CBP-held video or other data is controlled through chains of custody and stored in secure locations until it is destroyed. In addition, the FAA requires CBP to construct a COA, in the instance of deploying a UAS, for a duration determined by the investigative activity or emergency circumstance, before conducting an operation away from the border and already established COAs.

The third privacy concern, unique to UAS, pertains to the security of the system itself and the potential for hijacking of the unmanned aircraft. CBP has taken several steps to protect UAS against potential hackers. All UAS are controlled and monitored at all times by operators in ground control stations using satellite communication that is relayed through an encrypted data feed. The ability to interfere with such an encrypted data feed requires disrupting the signal from satellite to UAS, for the purpose of acquiring the data feed or controlling the UAS. In the event that the ground control station loses its ability to control the UAS, another ground control station can pick up control of that UAS. The UAS use redundant navigation systems and GPS receivers so that if a signal is lost or someone attempts to override the signal, the UAS relies on these other systems and the GPS receivers for flight operations. In order to protect the airspace, the FAA is notified immediately if a UAS loses its signal. Furthermore, if communication between ground control and the UAS is ever interrupted or lost, the UAS are pre-programmed to fly to a pre-coordinated point in a remote location to orbit while waiting for the signal to be reestablished, or to continue to orbit this Flight Termination Point until the aircraft runs out of fuel and crashes.

Because of the unique privacy concerns raised by CBP's use of Aircraft Systems, CBP has conducted this PIA to evaluate the privacy risks associated with the use of Aircraft Systems and to enhance public understanding of the authorities, policies, procedures, and privacy controls related to that use.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the Federal government should treat individuals and their information and imposes duties upon Federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. Section 222(2) of the Homeland Security Act of 2002 states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.[9] The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208, and the Homeland Security Act of 2002, Section 222. Given that Aircraft Systems and their associated devices are mechanical and operational systems rather than a distinct information technology system or collection of records pertaining to an individual that would be subject to the parameters of the Privacy Act, this PIA is conducted to relate the use of these observation and data collection platforms to the DHS construct of the FIPPs. This PIA examines the privacy impact of Aircraft Systems operations as it relates to the DHS FIPPs.

1. Principle of Transparency

Principle: *DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.*

This PIA provides a level of transparency to the public about the current surveillance programs undertaken by CBP. The video, still images, signals information, and/or radar images do not clearly identify individuals. The only information about individuals that is collected and/or retained is the indication of a human form. These images, however, may be associated with a person if the person is apprehended. For example, video collected by an EO/IR ball may show several individuals traversing the land border and being intercepted by officers or agents of CBP. While the video resolution or radar mapping images are not sufficiently precise to permit actual identification, the circumstances of CBP interdiction and apprehension of a suspect in conjunction with the aerial surveillance are sufficient to link the indistinct images of persons traversing the ground to the case file. Individuals who are apprehended by CBP as a result of observation by aircraft at or near the border may have video of their crossing and apprehension associated with their enforcement case file. CBP obtains biographical data pertaining to the apprehended person at the moment of apprehension. CBP stores all biographical information

[9] DHS Privacy Policy Guidance Memorandum 2008-01, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*, December 29, 2008.

obtained from apprehended individuals and any video or radar images of their movement obtained from the aircraft in the appropriate law enforcement case management system.

When CBP associates video, still images, signals information, and/or radar images with an individual after apprehension, that information becomes subject to the requirements of the Privacy Act in the same manner and to the same extent that the apprehension of the individual becomes a record in a Privacy Act system. The Privacy Act requires that agencies publish a SORN in the Federal Register describing the nature, purpose, maintenance, use, and sharing of the information. This PIA serves as notice to the public that information captured by Aircraft Systems may become subject to the Privacy Act once it is associated with an individual.[10] Additionally, the video images associated with an individual's case file are covered by the appropriate law enforcement case management SORN, which maintains the case file. CBP will periodically re-assess the means by which the images from the aircraft are retrieved to determine whether the requirement for a SORN is triggered.

2. Principle of Individual Participation

Principle: *DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.*

Individual participation provides complementary benefits for the public and the government. The government is able to maintain the most accurate information about the public, and the public is given greater access to the amount and uses of the information maintained by the government. A traditional approach to individual participation is not always practical or possible for CBP, which has law enforcement and national security missions. Aircraft are primarily used to sweep the border area to locate individuals who are crossing the border illegally. Allowing an individual to consent to the collection, use, dissemination, and maintenance of video, still images, and/or radar images would compromise operations and would interfere with the U.S. government's ability to protect its borders, thereby lessening overall homeland security.

Individuals do not have the opportunity to restrict CBP's ability to collect information in the public sphere. Any information associated with an individual is part of a case file that is created as part of a law enforcement investigation or encounter.[11] Providing individuals of interest access to information about them in the context of a pending law enforcement

[10] For example, video information from an aircraft of an apprehension of a person at the border that is identified to that person would be referenced in the case notes pertaining to that person's apprehension in TECS (DHS/CBP – 011 TECS System of Records Notice December 19, 2008 73 FR 77778)

[11] CBP also incorporates images from surveillance or encounters into reports and analyses maintained in the Analytical Framework for Intelligence (AFI) (DHS/CBP – 017 System of Records June 7, 2012 77 FR 13813).

investigation may alert them to or otherwise compromise the investigation. Consequently, there is no mechanism for correction or redress for the video collected by the aircraft. Once that video is associated with an individual's case file, the individual must follow the procedure outlined in the corresponding privacy documents for that system. While individuals cannot participate in the initial collection of this information, they may contest or seek redress through any resulting proceedings brought against them. More information on redress is provided below.

3. Principle of Purpose Specification

Principle: *DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.*

The purpose specification principle requires DHS to 1) articulate the authority to retain the PII in question; and 2) articulate the purpose(s) for which DHS uses the PII.

CBP is authorized to collect video, other images, signals information, and data using aircraft in support of its border security mission and pursuant to the appropriations language mandating support for law enforcement as part of the mission of CBP Air and Marine.[12] Together, these authorities allow CBP to obtain information in support of border interdiction of narcotics and other contraband, the prevention of the illegal entry of aliens into the United States, the security of airspace for high-risk areas or National Special Security Events, and in support of federal, state, and local law enforcement, counterterrorism, and emergency humanitarian efforts.

CBP may use video, still images, signals information, and/or radar images, obtained from aircraft, to apprehend individuals and to provide evidence of an illegal border crossing or other violation of law. Consistent with applicable laws and SORNs, the information may be shared with other state, local, federal, tribal, and foreign law enforcement agencies in furtherance of enforcement of their laws. [13]

Video, still images, and/or radar images collected during investigative operations as part of a law enforcement investigation are used for enhanced situational awareness and increased officer safety, and may be used to provide evidence of a violation of law. These images are maintained in association with the investigative or case file that they support; their retention is managed by the same SORN and follows the handling of the investigative or case file.

[12] *See, e.g.*, H.R. REP. No. 112-91, at 46 (2011) stating "CBP Air and marine provides integrated and coordinated border interdiction and law enforcement support for homeland security missions; provides airspace security for high risk areas or National Special Security Events upon request; and combats efforts to smuggle narcotics and other contraband into the United States. CBP Air and Marine also support counterterrorism efforts of many other law enforcement agencies."

[13] *See* Consolidated Appropriations Act of 2012, Pub. L. No. 112-74 (2011), providing for "the interdiction of narcotics and other goods; the provision of support to Federal, State, and local agencies in the enforcement or administration of laws enforced by the Department of Homeland Security; and at the discretion of the Secretary of Homeland Security, the provision of assistance to Federal, State, and local agencies in other law enforcement and emergency humanitarian efforts…."

Video, still images, and/or images collected in natural disaster and/or emergency situations are used for relief work and disaster reconnaissance. CBP typically provides a direct feed of the video captured by aircraft in these scenarios to provide support to FEMA or state emergency operating centers. Video, still images, and/or radar images are not associated with an individual and are only used to indicate where an individual or group of individuals may be for emergency response purposes.

4. Principle of Data Minimization

Principle: *DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).*

CBP seeks to minimize the collection and retention of video, signals information, and radar to that which is necessary and relevant to carry out CBP's mission. Accordingly, when aircraft are flown to patrol the border, they are authorized to fly the designated border surveillance mission area to ensure they are only capturing images and information necessary to detect, identify, apprehend, and remove persons and their possessions illegally entering the United States at and between POE. When aircraft are flown for investigative operations, officer safety incidents, or natural disaster reconnaissance, CBP approves and defines the specific mission that is authorized, and in the case of UAS, works with the FAA to construct a COA to establish airspace for that specific UAS operation. The video (that has not been associated with a case) remains on the digital video recorder originally used for recording until it over-written through re-use, which is after approximately 30 days.

After the creation of live mission data, Big Pipe manages the transmission, processing, distribution, consumption, and storage of the live mission data. Big Pipe archives selective mission data on a Big Pipe server hard drive for a maximum of 7 days, after which the data is deleted. Big Pipe does not use PII to retrieve stored mission data.

The information collected by the aircraft is not subject to the Privacy Act unless it is retrieved by using an individual's name or other unique identifier. If an individual is apprehended by CBP as a result of observation by aircraft or subsequent association from the presence of CBP assets, CBP may have video of that individual's apprehension associated with his or her enforcement case file. That video is retained according to the retention schedule of the SORN of the corresponding case management system. Video and Radar images obtained from UAS patrols of the border are also provided to PED cells operated by OIIL for use in analyses and intelligence products concerning historical, change detection (e.g., natural and man-made alterations to geography) along the border, and patterns of movement of persons across the border. This unassociated data, in conjunction with meta-data (such as latitude, longitude, date and time of the imagery) is retained for a maximum of five years.

5. Principle of Use Limitation

Principle: *DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.*

CBP only collects video and/or radar images, and signals information via aircraft pursuant to its law enforcement authority, as part of its border security mission, or when flying a mission in support of another agency, and when that other agency's authority covers the mission either through delegation of authority or direct control of the information collected. For example, CBP has provided support to the U.S. Forest Service in response to large scale wild fires to permit an overview of the extent and scale of the fire and identification of hot spots; this activity is pursuant to a request from the Forest Service, is performed pursuant to their authority, and the images are conveyed through designated access to the Big Pipe video distribution service. While the video resolution, radar mapping images, and signals information are not sufficiently precise to permit actual identification of a person, the images or information may be associated with an individual from context within the image, circumstances surrounding the activity occurring in the image, or additional information obtained directly from the person by an officer or agent. The images or information are only associated with an individual if the individual is apprehended or if the images are taken as part of an ongoing law enforcement investigation. Accordingly the data can only be used for the purposes specified in section 3 of this PIA.

CBP has procedures and processes in place for sharing any data collected by aircraft, including when that information becomes associated with a case and is used as evidence against an apprehended individual. In addition, all requests for aerial surveillance for intelligence gathering purposes must receive prior approval by the Assistant Commissioner, OIIL, before the air asset can conduct the flight. Similarly, requests for analytical products incorporating historical analysis of the border topography must be approved by the Assistant Commissioner, OIIL.

6. Principle of Data Quality and Integrity

Principle: *DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.*

As explained in section 4 (above), to ensure that the PII captured by aircraft is relevant and timely, any video, still images, signals information, and/or radar images must be associated within 30 days with the individual CBP apprehends, or the video/digital image is overwritten by OAM. Video and/or radar images are of no continuing value in a law enforcement support context unless they are associated with an individual during an apprehension because the video resolution or radar mapping images are not sufficiently precise to permit actual identification of individuals. Video and/or radar images that are not associated with a person provide value in an intelligence context for helping to demonstrate the state of change occurring over time along the border. These unassociated images are separately maintained by OIIL for a maximum of five years.

To preserve the quality and integrity of the information collected that is used as evidence, CBP requires its officer/agents to successfully complete training on the proper operation of the recording equipment on its aircraft. The training includes correct techniques to copy recorded evidence from a non-portable hard drive to portable digital media and procedures to ensure that such evidence is not co-mingled with data from other investigations. The training also includes procedures to maintain an adequate chain of custody for all recorded evidence. Each officer/agent making a recording must ensure that the time and date shown in the original recording is accurate. After a mission is completed, the officer/agent must ensure that the original record is transferred entirely, in its original format, to portable media. The transferred data must not be edited or altered in any way. The officer/agent making the recording must label all copies of portable media with the corresponding case number (if available), the date and place of the original recording, and the names of the officer/agent and aircraft commander. The officer/agent making the recording must also label, initial, and maintain possession of the evidence until custody is properly transferred to the appropriate designated evidence custodian, case agent, Assistant United States Attorney, or other appropriate government official. As with any information associated with a case file, once the images are cross referenced to an investigation or case, they become covered by the system of records for that case file system and subject to the access and amendment provision of that system.

7. Principle of Security

Principle: *DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*

CBP has taken steps to protect live video feeds, signals information, and recorded video, radar, and/or still pictures captured by its aircraft. Live video and flight information, which are sent from the UAS, are passed along an encrypted feed from the UAS through the satellite relay to the ground control station. Similarly, control information from the ground control station to the UAS also passes along an encrypted feed. Video and data transmitted in real time via Big Pipe, a closed system with restricted access, is subject to access controls and an approval process requiring clearance by one of two CBP/OAM system administrators to ensure that only authorized users with a need to know have access to the video feeds. The real time video feeds are not recorded and archived. Any recorded images that are saved to be used as evidence or for intelligence gathering must be handled in accordance with CBP policy. Images that are used as evidence must be handled according to the procedures detailed in section 6 of this PIA. All recorded evidence must be kept in a locked container, segregated from other property and/or equipment. Video that is collected during an investigative operation that contains sensitive analytical surveillance, or reconnaissance related data may not be disclosed unless a request for disclosure has been submitted to the OIIL Collections Division Director. The request must include a copy of the information that is to be disclosed, must clearly specify the name of the intended recipient, how the information will be used, and the reasons justifying the disclosure. In the event that the information is disclosed, the OIIL Collections Division Director or his/her designee is required to redact law enforcement sensitive information, PII, and other sensitive related data unless the requestor has a need-to-know.

8. Principle of Accountability and Auditing

Principle: *DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.*

All CBP employees are required to complete annual privacy awareness training, in addition to training on ethics and the CBP Code of Conduct. Access controls, both physical and technological, are in place to ensure only authorized access to the aircraft systems and the collected data/images.

Moreover, CBP requires its employees to successfully complete training on techniques to copy recorded evidence to portable digital media and requires them to follow procedures to ensure that such evidence is not co-mingled with data from other investigations. Employees must follow procedures to maintain an adequate chain of custody in the event that the information is used as evidence.

OIIL has a process in place for restricting the dissemination of video, still images, and radar images and keeps a log of the disclosures. Also, OIIL redacts law enforcement sensitive information, PII, and other sensitive related data unless the requestor has a valid need-to-know. Separately, CBP periodically reviews the logs or disclosure records to ensure compliance with established privacy policies, practices, and procedures for associated systems.

Conclusion

CBP operates aircraft systems in support of its border protection and law enforcement support missions. These systems provide a variety of mobile platforms from which to obtain signals information, video, still, and radar images of persons and vehicles in the border area or that are the subject of an investigation or law enforcement activity. The collection of these images and signals information complies with the same internal procedures and practices required of any surveillance using any means by CBP officers and agents. The distinct capabilities of the different aircraft operated by OAM enhance CBP's ability to conduct certain missions pertaining to information collection, surveillance, or reconnaissance; however, the processes and procedures for authorizing and accounting for how, when, and where information is obtained remain consistent with CBP's traditional border security and law enforcement practices and policy. As technology improves, operating environments change, and policies adapt, this PIA will be updated and amended to refresh the analysis of these changes on the privacy of persons, who directly or indirectly come into contact with the information and data collection activities associated with CBP Air operations.

Responsible Officials

Lothar Eckardt
Executive Director, National Air Security Operations
Office of Air & Marine
U.S. Customs and Border Protection
202-344-3950

Laurence Castelli
CBP Privacy Officer
Office of Privacy and Diversity
Office of the Commissioner
U.S. Customs and Border Protection
202-325-0280

Approval Signature Page

Original signed and on file with the DHS Privacy Office.

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

Section 12

U.S. Department
of Transportation
**Federal Aviation
Administration**

Public Unmanned Aircraft Operations in the National Airspace System

The Federal Aviation Administration (FAA) is responsible for processing and approving all requests for Unmanned Aircraft Systems (UAS) operations in the National Airspace System (NAS). For UAS operators, this authorization is generally granted via the issuance of a Certificate of Waiver or Authorization (COA). Typically, Law Enforcement Agency (LEA), Fire, or First Responder UAS flight operations are considered "public aircraft" operations. The guidelines for operating as a "public aircraft" entity are described in the FAA's Unmanned Aircraft Systems (UAS) Operational Approval Notice N8900.207, which may be found on the FAA web site: http://www.faa.gov/about/initiatives/uas/.

When the FAA receives a COA application through the FAA's *COA Online* portal, the Agency initiates a rigorous program review and application assessment. Included in this review and assessment are: 1) concept of operations (CONOPS) or type of missions; 2) launch/recovery/operation location(s); 3) operational altitudes; 4) flight procedures; 5) communications; 6) emergency procedures, such as lost communication and loss-of-control link; and 7) Pilot in Command (PIC), flight crew, and observer qualifications and training requirements. The typical COA application approval process is completed within 60 business days of receipt, provided there are no submittal errors, missing information, or safety or airspace issues. New authorizations are valid for two years and must be renewed while valid or a new application must be submitted. Before the FAA grants access to the *COA Online* application process, the Proponent will be asked to provide preliminary information that includes, but is not limited to:

- The Proponent's address and contact information, including the accountable executive's name
- The name and manufacturer of the UAS technology being considered
- How the Proponent anticipates using the UAS technology (Concept of Operations)
- The level of aviation experience of the Proponent (e.g., does any member of the Proponent's organization hold a private or advanced FAA pilot certificate or an FAA Airman Medical Certificate, etc.)
- Will the Proponent be developing the UAS program "in house" or utilizing a third party to develop and/or implement its UAS program
- A letter from the LEA's County or State Attorney General formally acknowledging that the Proponent is recognized as a subdivision of the government of the State under Title 49 of the United Stated Code (USC) Section (§) 40102(a)(41)(c) or (d) and that the proponent will operate its Unmanned Aircraft in accordance with 49 USC. § 40125b (not for Commercial Purposes)

The FAA believes that the safest and most successful jurisdiction-wide deployment of UAS technology that supports public safety agencies is accomplished through a two-phase process. The *initial* COA (Phase I) is generally restricted to training and evaluation activities at a specific training site that is confined to Class G airspace, and remains well clear of housing areas, roads, any persons, and watercraft. This permits the public agency the ability to conduct necessary ground and flight training to bring pilots, observers and ground crewmembers to a high level of UAS flight proficiency and also enables them to develop and conduct training exercises to ensure efficient, standardized coordination amongst other supporting elements (e.g., SWAT or SRT team coordination for operational missions, search and rescue, disaster control, crime-scene or post-accident forensic photography, fire response teams, etc.). Along with the *initial* COA Application, several documents need to be submitted by the Proponent, including:

- An airworthiness statement from the Proponent's accountable executive acknowledging that the Proponent accepts all responsibility for ensuring that the UAS is airworthy and that the UAS will be operated and maintained in compliance with the manufacturer's operational and maintenance recommendations
- A lost-link procedures document that addresses the specific lost-link procedure that will be implemented in the event of a lost-link occurrence
- A lost communication procedures document that addresses what actions the Pilot-in-Command (PIC) will take if there is lost communication between PIC and Air Traffic Control, as well as lost communication between PIC and the Visual Observer (VO)
- An emergency procedures document that explains the protocols that will be executed at the site in the event of an emergency (this could include execution of procedures outlined in the operator's manual, possible alternative courses of action available for each phase of flight, and any outside agencies or resources for medical and fire or other assistance)

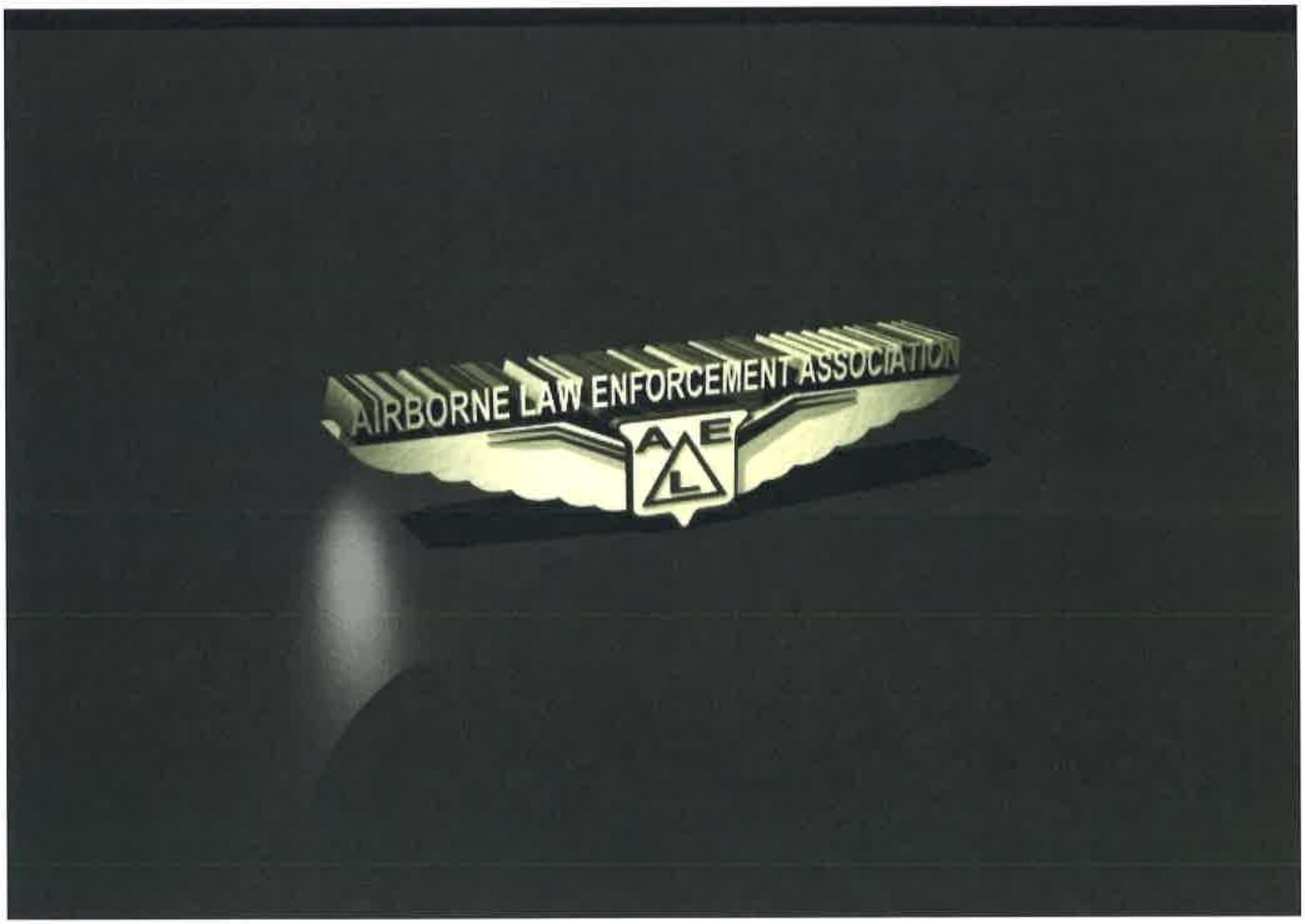
Once the Proponent feels confident that it can safely operate the UAS at a level of competency to safely support actual operational missions, the Proponent will apply for a second *operational* COA (Phase II) that typically incorporates the Proponent's jurisdiction. As part of the *operational* COA approval, the FAA will conduct an onsite program review and evaluation. This onsite review will include:

- Review of the Public Safety Agency's UAS training and proficiency program, including all training records
- Review of the Public Safety Agency's Standard Operating Procedures (SOPs) for each phase of flight operation from notification for deployment through preflight, launch, recovery, post-flight and mission record keeping. SOPs must include, at a minimum: emergency procedures and standards for expected scenarios (e.g., lost-link, lost communications between VO and PIC or between PIC and ATC, medical emergencies, etc.), Crew Resource Management, sterile ground control station protocols, PIC and VO standard communications and any special mitigation procedures
- Review of the Proponent's Safety Risk Analysis Plan (SRAP) that specifically identifies the boundaries of the Proponent's jurisdiction, and all unique operational areas within that jurisdiction and their attendant hazards (Note: The SRAP must include a description of specific risk controls the Proponent will employ to mitigate any attendant hazard for UAS)
- An evaluation by the FAA of a UAS exercise to demonstrate the competency and safety of the Proponent's program

The FAA is committed to safely integrating UAS into the NAS and looks forward to working with public safety agencies in developing UAS Programs. If you have questions, please direct them to one of the below contacts:

Douglas Gould
Manager
UAS Tactical Operations Section, AJV-115
Douglas.Gould@faa.gov
202.385.4579

Jim Ryan
Manager
UAS Safety & Data Mgmt. Section, AFS-84
Jim.Ryan@faa.gov
202.385.4322


AIRBORNE LAW ENFORCEMENT ASSOCIATION
A E L