Proceedings of The White House Office of Science and Technology Policy Workshop on Drones and the Future of Aviation

Published: October 12, 2016

Table of Contents

Introduction

On Aug. 2, 2016, the White House Office of Science and Technology Policy (OSTP) and the AUVSI Foundation held a workshop for industry, government and academic members of the unmanned aircraft systems (UAS) community. The goal of the workshop was to address the continuing issues UAS will face as they are integrated into the National Airspace System (NAS).

The workshop was held a few weeks prior to the implementation of the Federal Aviation Administration's (FAA) Part 107 Small Unmanned Aircraft Rule, which took effect on Aug. 29. This rule provides a formal pathway for businesses to legally fly UAS for commercial purposes; however, these operations have some limits, such as visual line of site, daytime only, and up to 400 feet above ground level (unless within 400 feet of a structure). Businesses will need to apply to the FAA through waivers to be able to fly at night, beyond visual line of sight or over people, for example.

The workshop event came with a large financial investment pledge from the White House. OSTP announced the Obama administration has put $35 million in new research funding on unmanned aircraft research through the National Science Foundation over the next five years.

FAA Administrator Michael Huerta discussed drones' transformative path thus far.

"UAS are transforming entire industries," he said. "They are improving the safety of our transportation infrastructure. … They are tackling jobs that are dangerous for other people or aircraft to do."

He said the FAA wants to move at a faster pace with this technology, so it doesn't stifle innovation and enthusiasm. The agency aims to have a proposed rule about drone flights over people by the end of the year.

Huerta announced that the FAA is forming an unmanned safety team and then he handed things over to Intel Group CEO Brian Krzanich, who is the chairman of the Drone Advisory Committee (DAC). Krzanich spoke and he showed a video of a swarm of drones flying over Sydney. He said it Intel's goal to have swarms like that one, numbering up to 1,000 at a time, so companies can inspect quicker and more thoroughly. However, Krzanich outlined that work still needs to be done on technology, like collision avoidance, and drones also need to get smarter and be much more autonomous vehicles.

He commended the FAA for its work on the small UAS rule, which paves the way for widespread, legal commercial drone operations.

"Don't tell me what I can't do. Just tell us what we have to invent; tell us what we have to overcome. Give us those rules and methods. Give us what we need to invent, … and we'll go invent it," he said.

Phil Moeller, senior vice president of energy delivery at Edison Electric Institute, discussed how drones have been a boon to utilities inspection, but there remains a need for beyond-line-of-sight flights, an application not permitted in the small UAS rule but available through a waiver process. EEI is teaming with drone company Sharper Shape and they will apply to fly beyond-line-of-sight in the United States for these types of applications.

During a panel discussion on the role of data and research and development in policymaking, Howard Zemsky, commissioner of economic development for the state of New York, announced that the governor, Andrew Cuomo, made a $5 million investment in the UAS industry in Central New York. The investment will support NASA's UAS Traffic Management infrastructure, UAS testing and rating facilities, and a UAS innovation corridor between Syracuse and Rome, New York.

The final panel, moderated by AUVSI President and CEO Brian Wynne, discussed advancing technological progress in UAS.

"We've been talking a lot about policy. At the end of the day it's incumbent on industry to bring technology solutions to the marketplace," said Wynne.

The White House OSTP drone workshop was accompanied by a slew of announcements:

- $35 million in research funding by the National Science Foundation
- $5 million in support of UAS research for state of New York
- Department of Interior commitment to expand UAS use for search-and-rescue to augment manned aircraft. DOI will also start rapid prototyping and approval of UAS payloads for 2018 fleet.
- Charter of UAS Safety Team by the FAA
- NASA and FAA launched joint data exchange working group
- NOAA to use UAS for precise gravity measurements, to augment ships
- U.S. Post Office to explore UAS for mail and package delivery
- Northern Plains UAS Test Site in North Dakota to research beyond-visual-line-of-sight flights
- Zipline International working to demonstrate viability of medical drone use for remote communities
- Know Before You Fly campaign and Sinclair Broadcasting to create drone public service announcements
- Google's Project Wing to work with a test site to research delivery service

- Drone Racing League to create best practices for safe events
- PrecisionHawk announced Pathfinder program phase-one results
- Women of Commercial Drones group launched
- DJI announces support of 4-H National Youth Science DayDroneBase and Drones & Good announce plans to transition veterans to drone jobs
- Future of Privacy Forum, Intel, PrecisionHawk released report on drone privacy

Upon conclusion of the morning portion of the workshop at the White House, the event moved over to the Newseum where six concurrent breakout discussions were held. The following report captures what was discussed in each of these sessions and serves as a starting point for potential steps forward to address each area.

Low-Altitude Airspace Management/UAS Traffic Management

SUMMARY

The breakout session titled "Low-Altitude Airspace Management/UAS Traffic Management" sought to address three main issues:

1. Milestones for success
2. Technology transition
3. How stakeholder will receive the technology necessary to bring UTM to an operational capability

During the course of this session's discussion, enhancing industry and government collaboration emerged overarching theme for the dialogue. As there are many factors for enabling civilian low-altitude airspace unmanned aircraft system operations related to traffic management, this session discussed some of those factors that are ripe for increasing collaboration efforts: collision-avoidance technology, automating regulatory procedures, and a service-provider system concept.

The full discussion is presented below.

DISCUSSION

This session sought input from academia, government and industry stakeholders on their expected outcome from the research coming out of the UAS Traffic Management (UTM) program—an effort spearheaded by NASA—and opportunities for public-private partnerships.

Government representatives emphasized that the federal government has no plans to mirror the traditional type of infrastructure used to safely manage manned aircraft in order to manage UAS traffic. Rather, the FAA seeks to partner with private entities that would be making investments in the field, including by offering the government their research findings.

"The idea here is to understand the needs of the community — what we know, what we don't know, what we need to talk through — giving people an opportunity to ask questions and gathering their input," a government representative noted.

Another representative from a government entity said their organization has a vision of a shared environment, but they want to know how the community plans to coordinate with each other and the FAA. However, a representative from academia wondered whether it would be in a commercial UAS operators' interest to share information via UTM, particularly with other commercial UAS operators.

All representatives emphasized the need to develop a collision-avoidance technology.

A government representative noted one aspect of collision avoidance would require some form of notification to other airspace users, particularly when UAS are operating at 300 to 400 feet of altitude, in closer proximity to manned aircraft.

One representative wondered: “Does [the FAA] need to know your trajectory? I don’t know.”

Representatives from academia agreed there is a need for a collision-avoidance system. An industry attendee opined that the UTM system could become a mechanism that would allow UAS operators to get into Class C airspace or other regulated airspace, which UAS cannot currently access without prior approval.

According to one government representative, one federal agency wants an environment where operators are notifying each other, aware of space regulations, and in uncontrolled Class G airspace.

Federal government representatives responded that regulating within the FAA’s Part 107 will move down the path of being automated, but anything beyond that will be difficult to mandate within the current budget.

“[The FAA] is not staffed to answer calls about you getting into other people’s space. [They] want you to grow the industry and don’t want to get in the way.”

One of the industry representatives questioned if that was possible. “We will have more traffic flying in low-altitude. How is safety going to be handled?”

Another industry representative echoed the concern.

“[The] point of UTM is to use data exchange to increase safety. We probably overvalue UTM in the near term for localized visual line of sight operations. When we go beyond these localized locations, UTM will be helpful to scale up. As a pilot, even if I fly in uncontrolled airspace, I still have to be aware of my surroundings and avoid other traffic. At its core, we need to start with these basic exchange protocols.”

A member of the academic community said that the key issue in a UTM discussion is how much its commercial participants would be willing to pay for this information exchange service and what they would be getting in return.

One of the industry representatives asked about the FAA’s plan to manage low-altitude operations around airports or other restricted areas.

“[The FAA’s] ability to generate authorizations is very manual right now, but as the [UAS] community grows, we hope to be engaged with the community through some form of formalized information exchange within the next six months,” said a government attendee. This

information exchange would respect proprietary issues, so that “we don’t give out information that we don’t need to.”

Two government representatives agreed that “there might be status changes for B and C class airspace” and more operations could be allowed in that airspace.

Related to UTM system specifications, a government representative suggested that it “would be a bad idea” for the FAA “to write the specs,” and the FAA would just need its planned information exchange system in place.

The session attendees debated the role of the FAA in creating a seamless way for commercial users to enter the airspace above 400 feet.

An industry representative stressed that what commercial users would be most looking for is rules for flying above 400 feet. Currently, “we don’t have an elegant way of getting into that airspace. That’s where the value is for us rather than just having an information exchange.” A system is needed for exceptions to Part 107. In the end, they wondered, “could a government contractor build this system and have everyone use it?”

However, a government representative reiterated that it wasn’t something the FAA would want to do and noted that the FAA saw no point in having a line to operators flying under 400 feet.

An industry representative suggested that some kind of “Verizon of drones” would be needed to handle all the new traffic. He said this should be part of the FAA’s vision on UTM.

Asked about the timeframe for a new UAS management system, a government representative expected that something may be developed within a year, but hopefully not take longer than three to five years. “Otherwise, we’ll get bulldozed over.”

Asked about international experience in UAS management, government representatives said that other countries, particularly in the European Union, were looking at the U.S. experience.

An industry representative noted that there was also a centralized system for robotic transportation in China. He reiterated that his primary interest was in “permission for more airspace” that would be regulated by a UTM manager.

Overall, the group discussed the benefits of UTM are as follows:

1. The potential over time to request and receive approvals beyond PART 107 or exceptions allowed in Part 107.
2. Ability to keep track of UAS areas of operations and be able to safely operate multiple vehicles BVLOS.
3. Ability for FAA to send in directives related to airspace use for safety and security reasons (e.g., Critical flights, Public Safety needs).
4. Ability to share information about UAS operations to manned aviation and vice-a-versa.

5. Ensuring a shared environment which can evolve into more direct government engagement in high density operations if there becomes a need to balance demand and capacity to ensure balance of safety and efficiency.

Beyond Part 107: Expanded Operations for Small UAS Breakout Session

SUMMARY

The breakout session titled "Beyond Part 107" sought to address four main questions:

1. If government and industry want to have full airspace integration by 2020, for example, what next steps should be taken in addition to the FAA's current rulemaking plan?
2. What kinds of standards should we focus on when using a risk-based and performance-based approach for regulatory development?
3. Besides the UAS Traffic Management (UTM) effort, what are the key enabling technologies? How do we manage and share data and ensure data integrity?
4. What are international and global considerations, e.g., harmonization, manufacturing, certification and registration? What international bodies should the FAA be working with?

At the session, government representatives gave a high-level overview of the FAA's steps to complete the regulatory structure for full UAS integration and its current rulemaking plans. The conversation then turned to the four questions posed above. A large portion of the conversation was focused on the need for the government to implement Part 107 correctly while still moving ahead with new rulemakings. The overall consensus was that it is vital for the U.S. government to ensure that Part 107 works well. By doing so, the U.S. will be a leader in UAS regulations and essentially become the global standard.

Additional discussion focused on the need for the government and industry to share data to help ensure safe integration, standards that should be used for a risk-based and performance-based approach, UAS Traffic Management and other technologies, and international considerations.

The full discussion is presented below.

DISCUSSION

The discussion on what the FAA should focus on going forward, now that the small UAS rule is in place, began with a review of the upcoming FAA agenda.

The FAA's approach is to tackle the integration of UAS operations in order of least complex operation to most complex. This complexity-based distinction differs from a weight-based determination, and instead focuses on risk. For instance, a heavy platform operating over the desert would carry less risk than a small UAS flying a package in an urban area.

The agency has been tasked to release a Notice of Proposed Rulemaking (NPRM) related to operations over people by the end of 2016. The FAA is also seeking information on expanded operations from its Pathfinder programs, which have the primary thrusts of visual line of sight operations for newsgathering in populated areas, extended line of sight operations for agriculture in rural areas, and beyond line of sight operations for fixed-infrastructure inspection in rural or isolated areas. These types of operations will be permissible through a waiver process built into Part 107, and the FAA has a notional goal of integrating these operations through an NPRM released in either 2017 or 2018.

Another FAA rule following that one, potentially slated for public notice around 2019, would include non-segregated operations, which would enable flight operations like package delivery without a waiver process.

The agency is also grappling with a significant cultural challenge — many of the new airspace users (remote pilots) do not come from a traditional aviation background, and the FAA is cognizant that it cannot integrate these users in a traditional manner. The volume of people entering the airspace is higher than ever. In order to navigate this new landscape, the FAA knows it needs to digitize more of its process, particularly since drone technology is constantly evolving, and at a swifter pace than traditional manned aircraft.

The agency will also need to handle how it distributes safety information. To examine how best to interact with this new constituency of airspace users, the FAA created the Drone Advisory Council (DAC).

Question No. 1

An industry representative said that giving the FAA access to data might help advance its upcoming goals. For instance, the agency could use a Request For Information (RFI) or a basic solicitation for people willing to come forward and share their flight data.

The agency currently performs an annual safety survey through a general aviation committee. The FAA could collect the same information in the same way from the drone community. A government representative said the FAA would look to industry, particularly representatives of the insurance industry, to sit on that committee to see what sort of questions it should ask.

It was also suggested by a government representative that remote or sparsely-populated areas, such as the FAA Test Sites, could provide the agency with lots of flight opportunities, which would enable further data collection. Another government representative said that he regularly flies nighttime missions abroad in hazardous conditions and could supply that data.

Representatives from industry wondered what sorts of data the FAA was looking for.

“I have no idea if operator profiles are interesting or average flight time. If I knew it would be useful to collect, I would start,” an industry representative said.

Another member of industry said perhaps the FAA could tell the public its top 10 most needed data types.

However, a government representative pointed out that the FAA is bound by some rules and regulations, namely the Paperwork Reduction Act, which limits the amount of forms the government can ask the public to fill out.

In order to aid with that, an industry representative said that if the FAA articulated those barriers, then companies and organizations could try to help remove those obstacles.

Additionally, industry could feed the FAA information on safety by performing its own tests. For instance, crash test dummies used by the automotive industry were funded by the insurance industry with the help of auto manufacturers.

The FAA is considering performing similar tests about drones falling on a person's head to collect data, which will provide details in developing its proposed rulemaking on flights over people. Specifically, it is performing simulated crashes in populated areas to determine the risk.

Multiple members of the industry expressed concern over what types of flights the FAA would permit through its waiver process after Part 107 is put into place. Some were concerned the process would be redundant to the Section 333 exemption process, which for companies was long and arduous. Others were interested to learn what the FAA would consider an acceptable level of risk in an operation.

Members of academia wondered if the FAA had specific measurements it was looking for in the waiver process, for instance, the number of lumens that would determine acceptable night flights, or a particular wind condition that would open up another currently banned type of flight.

A government representative said there would be no hard-and-fast definition of safety, and an operation would pass a "socially acceptable level of safety" test. For instance, the aviation accident rate of the 1970s would no longer be socially acceptable.

Question No. 2

Workshop attendees discussed the standards work that has already been done by ASTM International and the Radio Technical Commission for Aeronautics (RTCA).

An industry representative discussed RTCA's work on developing phase one standards around command and control and detect and avoid. The group passed a milestone in July and expects to have final review and for the standards to go to the RTCA's program management committee in September. RTCA intends to take a different approach for its phase two efforts that is more innovative.

A government official opined that the FAA could move away from working solely with formalized standards committees. For instance, working through a committee created outside of a standards body could speed things up and provide a more innovative approach. However,

that is already occurring through a working group formed under a committee by a nonprofit technology organization, according to an industry representative. Instead of taking years to formalize standards, that committee created an industry benchmark in 75 days.

Industry also questioned how the FAA was going to implement knowledge about these standards to the air traffic control (ATC) community. For instance, some industry members pointed out, ATC representatives are not present at meetings like this one. They are, however, present at UTM meetings, according to a government representative.

Industry representatives closed the topic, noting that a hybrid approach — working both with formal and informal committees on standards — could prove most effective.

Question No. 3

All representatives stressed that UTM is vital to managing the future of the airspace. However, there are other technology options available, but they are divisive.

Technologies like geofencing could further safety, but it is difficult for the industry to know exactly where and what needs to be geofenced without another party supplying that information, said an industry representative. Also, more restrictive measures like operator identification information validation could prove to be a dangerous precedent to place on drone manufacturers. That move is unprecedented in other transportation modes and would be akin to asking car manufacturers to make sure only the car owner can use a vehicle.

The FAA has required that, by 2020, general aviation pilots outfit their manned aircraft with automatic dependent surveillance-broadcast (ADS-B) devices. This measure could improve safety in scenarios where drone operators are responsible for avoiding collision incidents.

Question No. 4

Attendees noted that there are a lot of overlapping organizations that handle international drone regulations, and many of them are doing duplicitous work.

Government representatives wondered if there was anything the FAA could do to learn from or collaborate with other countries.

Unanimously, members of industry in attendance said they were pleased with the results from Part 107's passage and would like the FAA to focus on getting the implementation right. While the FAA could perhaps learn from the international community, for the most part, the attendees said the United States is now the leader in drone regulations.

"I personally think we've gone from saying the FAA's behind, and now I say we're ahead for the first time in unmanned," said an industry representative. "Not everything is in [Part 107] that we would have liked, but we're in the lead now."

Another industry representative said that in developing countries that have sparse or no drone regulations, users saying that they are following U.S. standards would be enough to appease those governments.

Attendees did note, however, that state and local governments in the United States still need to be dealt with, since many have passed drone regulations that are federally preempted. Government representatives said there is increasing attention paid to this issue.

Implementing Comprehensive Integration: A Smarter National Airspace System

SUMMARY

The breakout session titled "Implementing Comprehensive Integration" was broken into three main parts:

1. Defining a vision for integrated airspace
2. Defining the technical challenges in achieving the vision
3. Defining the policy challenges in achieving the vision

Consensus began to coalesce around a vision for "truly democratized access to the airspace" defined as "four-dimensional freedom for all." Participants further outlined the fundamental tenets of this vision: it must be safe, secure, seamless and sustainable.

The conversation then moved on to the technical and policy challenges that will need to be overcome in order to make the vision a reality. Participants listed several technical challenges including sense and avoid, command and control, and automation. Policy challenges included public engagement, privacy, agreeing upon an adequate definition of safety, the authentication of users, the self-certification of operators, security and cybersecurity considerations, the increased visibility of UAS platforms, and mitigating the environmental impact of UAS operations. Geofencing and noise were considered both policy and technical challenges.

The full discussion is presented below.

DISCUSSION

Workshop participants outlined a vision for a collaborative, integrated unmanned aircraft system driven by industry, with limited government involvement, open to industry ownership and inclusive of varied business-use models.

One of the session moderators from the UAS industry coined the phrase "four-dimensional freedom" to define the objective of the group's vision for a collaborative, integrated system open to various business models. Group discussion on the equity of such a system led to the addition of the words "for all" to the end of that phrase.

Tenets that fall within this vision include safety, security, seamless integration, and sustainability. These terms helped shape discussion on the potential technology and policy considerations.

The extent to which government should be involved in regulating airspace use by UAS became a primary topic of debate. Some argued the government's role should be limited to safety measures, while others wondered if measures should be taken to prevent monopolistic or anticompetitive practices regarding the ownership of an integrated system.

"I think that should be left to the market to figure out great solutions," an industry representative said. "Regulations generally have double-edged sword characteristics, and, depending on which side you're cutting with, it may be in your favor or not."

Others noted that existing standards for the aviation and auto industries could help inform certification and authentication guidelines for UAS operators. These industry standards could also have implications for the UAS industry and an integrated system.

"If there are standards set for autonomous technologies, they are going to be driven by the auto industry," a government representative said. "You're going to end up with things that are just going to have to be accepted by the aviation industry, because of economies of scale, in terms of the way that a particular capability is being deployed. So I think there are significant implications, but I don't know if there is a policy issue there. I think it's going to be a market-based challenge."

A government attendee argued that federal agencies should be communicating with one another, not necessarily to draft regulations but to consider existing rules and regulations and what implications they could have for UAS.

"To [the attendee's] point, is it more that we should coordinate at the federal level to stay out of the way of industry?"

Another government representative said, that government could make the decision to let the market take over, but "we need to make that conscious decision."

Another member of the government said that a certain level of coordination could result in the government becoming overly cautious.

"I think that's a risk," an industry representative said. "The more people involved in the conversation who are not experts in this field, the more the process slows down. I think the technology world does a remarkably good job of leveraging each other's domain space."

A government representative questioned how ATC would fit into an open business model for an integrated system. Participants generally agreed that the industry would design systems to accommodate ATC, and ATC would likely adapt to new technologies.

The group identified public participation in integration planning as another challenge. While an industry member argued that public participation will complicate and draw out the process, government representatives argued that excluding public participation can backfire — if the public decides late in the process that it wants to be included, it could dramatically slow down progress. There are significant implications related to public engagement and participatory

policymaking for aspects of integration on matters such as privacy, noise control, issues of local governance, and more.

The group agreed that concerns about privacy rights would also pose a major policy challenge to an integrated open business model.

“Complications arise when privacy law gets thrown into the mix,” a government representative said. “Because policy at the local jurisdictional level sometimes overrides federal preemption authority specifically related to privacy. Examples of such laws are Peeping Tom laws (and not specifically drone applications), which govern the way in which you can or cannot surveil people. There’s deep confusion at the local level about these matters right now that are playing out in court. Preemption—and privacy—is an unresolved challenge.”

The group agreed that the government would be responsible for setting safety measures around those issues, including geofencing, but also that government shouldn’t regulate beyond safety concerns.

An industry attendee expressed a desire from the energy sector for the authority to protect their facilities from “nefarious” acts. “Do you have a right to shoot down a drone?” the attendee wondered.

The group discussed whether specific rules should govern security of private facilities and guidelines for handling UAS in violation of those rules.

Another industry attendee also suggested the “authentication of users to ensure that they are truly good citizens and collaborative participants in the airspace.” The group emphasized that “respect for all” would be a foundational objective for the UAS community.

Technological challenges to the framework include the articulation of safety performance expectations and defining an acceptable level of risk. An industry representative argued in favor of performance- and risk-based expectations that leave room for innovation.

Another industry attendee added that these kinds of expectations would be subject to a factor of scalability.

“The more the population density increases, the more the risk will increase. The challenge is articulating the challenge in a way that’s scalable.”

It was again offered that aviation standards could serve as a foundation for safety rules. For example, situations where no existing rule offers guidance, UAS operators could defer to sense-and-avoid tactics.

An industry representative noted that even in FAA regulations for safety, risk cannot be entirely eliminated. At some point, the standard will have to be “safe enough.” He also argued for a threshold or criteria that define a minimum expectation for performance- and risk-based safety, rather than rigorous standards, to accommodate innovation.

The group also tackled the need for full automation for ATC and aircraft — in other words, getting pilots and controllers into a monitoring system. Communications, navigation and surveillance would also need to be refined.

Other technological and policy challenges the participants discussed included noise, visibility, geofencing, cybersecurity and physical security of UAS.

Privacy

SUMMARY

The breakout session titled “Privacy” attempted to address three main issues:

1. Giving prior notice before flying UAS
2. UAS identification
3. Which communities should also be a part of the discussion on privacy

The session began by discussing questions surrounding transparency when operating UAS. There was lengthy debate amongst participants over whether or not it is feasible to have a system of informing citizens that a UAS is operating in the area. The conversation then developed into one about the anonymity of UAS. While it is currently fairly easy for specific UAS to remain anonymous, this could present challenges when it comes to reporting bad actors, or simply the curiosity of citizens nearby. Many participants agreed that there should be some way to identify UAS in order to ease some public suspicions and current perceptions of drones. Finally, the conversation closed with the discussion of who was missing from the debate on privacy and who should be included going forward. Many agreed on including colleges and universities since they are educating about UAS operations.

The full discussion is presented below.

DISCUSSION

In the privacy breakout session, a significant focus was on the question of whether or not there needs to be prior notice given to citizens when an unmanned system is flying in a person’s vicinity and possibly collecting data. Initially, many in the room felt that there wasn’t a real need to inform anyone of a UAS’s presence when flying in different areas, but the tenor of the conversation adjusted over the course of the session, and many in the room became more open to the idea of transparency.

When the conversation started, there were some objections given about not wanting to provide prior notice. Participants talked about the possible inconveniences that could be presented to businesses in the industry by creating a system where it was mandatory to inform citizens that a UAS is in the area.

“I cannot have a system that’s going to require me to ring up 500 people or make use of critical infrastructure when I’ve got another dozen flights that day in another state, for example,” said an industry representative. “So the system has to be incredibly easy to use and efficient.”

Another objection dealt with not knowing who and how many people to give notice to or what scope of an area should be covered in terms of relative distance to a UAS. Participants also posed the question of why operators and administrators of unmanned systems should have to provide prior notice, when manned aircraft don't have to provide notice when they're airborne and possibly collecting data.

As the conversation progressed, and the best practices document created by a multi-stakeholder process under the National Telecommunications and Information Administration agency was introduced as a talking point, most agreed that while individual notice might not be necessary, group notice to an entire neighborhood or area where an unmanned system may be flying might be something that the industry should consider looking into.

"I think that there's probably a middle ground there, in terms of providing some kind of transparency," said one industry representative. "The problem is the physical frame of most of these devices when covering small UAS," the representative said, commenting on how it is more difficult to notice the presence of smaller platforms.

One interesting point that was made surrounding the topics of privacy and notice dealt with people within their respective industries assuming that UAS are going to fly completely anonymously, which was not smart according to one participant, because manned systems typically have some way of being recognized or observed, and there's no precedent in place to believe that unmanned systems would get different treatment.

"We're starting to fall into the trap with UAS of thinking that we're going to have anonymity," said one member of academia in the room. The representative added that automobiles and manned aircraft have tag and tail numbers, respectively, and that members of the UAS community should not believe that unmanned systems will be flown anonymously. "We may have to shift our thinking," the representative added.

Immediately following the discussion of anonymity, one participant said that recognition would probably go a long way in eliminating questions from citizens who are wondering what a UAS is doing around them and what kind of information it might be collecting. According to this participant, questions often arise from a place of curiosity, not an initial objection. They went on to give an example of how identification, such as in this case of a UPS truck delivering a package, goes a long way in eliminating people's questions, because they associate systems with a brand, as opposed to having a UAS with no affiliation that only adds to people's concerns.

Additionally, anonymity creates challenges when it comes to reporting bad actors. As one government representative continually pointed out, it is difficult to report a bad actor if you have no way of identifying the UAS in the first place.

Continuing along the lines of concern and distrust from the public when it comes to UAS, representatives pointed out that there seems to be an inherent fear from the public of

unmanned systems, especially when it comes to these systems being in someone's personal space. Participants pointed out that many people don't have a problem when a UAS takes a photo of a person from a mile away, but they have an issue when it comes to unmanned systems flying in "personal or proprietary airspace," although that UAS might not be doing anything differently than it would be miles away. That led into a conversation about a need for formal education of the public to help eradicate fear and concerns about unmanned systems and the industry as a whole.

To cap off the conversation, the room agreed that there needs to be better education and regulation at all levels. They talked about the need for expansion into different communities, such as colleges and universities, and informing these communities about the use of UAS so that people can understand the challenges and opportunities associated with the technology, including privacy issues. In terms of regulations, the participants discussed a need for uniformity in rules and laws surrounding unmanned systems' operations and allowing for the public to freely access this information.

Spectrum

SUMMARY

The breakout session titled “Spectrum” addressed three main issues:

1. Spectrum capacity and sharing for UAS communications
2. UAS test sites and their role in spectrum research
3. UAS identification

The session began by discussing the increasing number of UAS users and the impact that they will have on spectrum capacity, including the possibility for a channel exclusively for UAS. Participants also explored ways in which industry, states and the federal government could partner on these issues, including through test site experimentation and incentives for the industry to work with regulators. The session also explored whether UAS can and should identify themselves in real-time and whether any such system should be standardized.

The full discussion is presented below.

DISCUSSION

Federal regulators have said they have two main concerns about the use of the radio frequency spectrum for command and control of unmanned aircraft — human safety comes first and noninterference with the transmissions of spectrum licensees (like telecommunications and media companies) comes next.

They explained how the Federal Communications Commission (FCC) and the FAA are working to accommodate the expected exponential increase in unmanned aircraft use in the coming years.

“And the hardest part,” said one government representative, is “trying to plan today for what’s going to be needed in the next five, 10, 15 years [and] knowing what is the need now. And for spectrum, understanding what they will need in the future and making sure we make smart decisions now.”

Most of the unmanned aircraft in the United States today are small drones being flown below 400 feet by hobbyists and amateur pilots. They must be kept within the view of the operator who controls them, through a radio link. That connection uses part of the radio frequency spectrum, which also supplies unlicensed Wi-Fi connections for smartphones and laptops. Government and industry officials are concerned that as more unmanned aircraft are flown below 400 feet by individuals and commercial interests in the future, spectrum congestion issues could arise and cause problems for drones, public safety or other spectrum users.

To maintain control of their aircraft, drone operators need a communications link. That link can also communicate the drone's position and status, such as altitude or battery life. Command and control requires spectrum, in the form of links from the ground to the drone to control the aircraft and from the aircraft to the ground to give the drone's diagnostics. If the drone is carrying certain payloads, like a real-time streaming video camera, that payload will also require a communication link. For more elaborate drones, RF spectrum may also be needed for radar capabilities to support collision avoidance or detect-and-avoid technology.

"Well, those radar pings require spectrum. It's not necessarily considered a communication link in all cases, but it requires use of radio frequency spectrum," a government representative said. One trend he noted was the use of unlicensed devices as the predominant method for controlling what are now recreational, and soon to become more prevalent, uses of UAS. "The radio frequency spectrum can be used for unlicensed purposes under various conditions. There are certain power requirements so it avoids interference issues. And one important thing to note is that there is really no restriction on where in the spectrum you can operate an unlicensed device, with the exception of restricted frequency bands, typically where there are receivers that are sensitive to interference, like GPS receivers."

But over the course of time there have been some "sweet spots" in spectrum in the 400 megahertz, 900 megahertz, 2.4 gigahertz and 5.8 gigahertz ranges. UAS have tended to use the 2.4 gigahertz band for control and the 5.8 gigahertz band for payload video streaming. The 2.4 and 5.8 gigahertz bands are also where Wi-Fi access points operate.

It will be a different story when more unmanned aircraft are allowed to fly beyond line of sight and more elaborate communication capabilities are required on the aircraft. Officials said they wanted to hear from industry where those additional frequency bands might be in the range of spectrum and how much bandwidth and power is going to be needed to complete the link and meet commercial requirements.

One government official made the observation that some companies are testing UAS operations on various frequency bands and that there may be an opportunity for the wireless industry, the UAS industry and the FAA test site directors to collaborate on future tests. We are interested in knowing the results of the testing to determine the possibility of using particular wireless frequencies and infrastructure.

Another government official recognized the importance of tracking small UAS flights from an air safety perspective, particularly if a UAS traffic management system is implemented. He recognized the existing capabilities for tracking manned aircraft might not be capable of supporting large numbers of small UAS. He further suggested that any use of existing tracking technology would have to be standardized for small UAS uses.

Industry speakers said they were concerned about harmonization of spectrum and control regulations both in the United States and worldwide.

“To know where the device is at any point as we go beyond line of sight, robustness gets more and more critical,” said one industry representative. Determining how robust the control link technology must be is crucial, he added, “so that we don’t have to design custom capabilities for each region.” He noted that industry thinks of the control issue from a range perspective, but government thinks of it in terms of spectrum utilization.

Below the 400-foot small drones ceiling, the FAA is not “deeply involved in telling you what you can and cannot do with the spectrum there. That falls to FCC,” a government representative said. But for operation in the national airspace, spectrum use for any aircraft — not just for unmanned aircraft systems — has to be in licensed, protected spectrum and there is spectrum set aside for that purpose. For example, there is spectrum in the C band put aside, both nationwide and worldwide, for UAS command and control. The FAA is concerned about two things regarding spectrum, one government representative said: safe operation of the airspace and, if an air operation — manned or unmanned — is causing spectrum interference to another licensed user.

Another government official asked if there was a role for satellite use in drone operations, either for payload or command and control. One industry representative suggested a search-and-rescue situation with multiple systems controlled by the operator over a wide-ranging area beyond line of sight. The individual drones could be set up as a mesh network in the sky to relay information in real time.

Had industry thought about using a satellite “hop” instead of terrestrial communications, especially at low altitude within line of sight, to improve small UAS communications, one government representative asked. Satellite control has worked well on large, mostly military drones, flying across continents and oceans. For small, mass-produced drones it could be done, but “it would be hard to make. Costs are high, and the equipment is complicated,” one industry representative said, especially since current rules limit small drones to flying within sight of the operator. The representative added that there were not as many spectrum bands dedicated for satellites and not that many small UAS would be appropriate for the upgrade.

However, another representative said it depended on how one described a “small” UAS, which can weigh up to 55 pounds. The representative noted that some technically small drones designed for the military operate more like a large UAS.

“Could you see satellite comms in a [Boeing-Insitu] ScanEagle? Absolutely. It has the space, weight and power to do that and it flies beyond line of sight. Would you see satcoms in a DJI product? Probably not,” the representative said.

In planning for future spectrum issues, government officials asked industry to “tell us what you need.” Several of the industry representatives advised: “Tell us what you want from us, and we can do the technological work arounds.”

UAS Security

SUMMARY

The breakout session titled “UAS Security” attempted to address two main questions:

1. How can industry cooperation encourage adoption of standards or guidance to help alleviate the potential for government over-regulation?
2. By 2025, UASs can be expected to possess an advanced suite of capabilities, some of which may be very difficult to counter with current technologies. What’s coming, and what can we do now to prepare?

Participants in the session from a variety of backgrounds brought numerous perspectives to the issue, but came to a consensus that no one solution is a panacea for UAS security. This is a complex issue which incorporates both inadvertent and unskilled operators as well as nefarious actors, and regulations and enforcement actions must address this. Confusion on where the enforcement jurisdiction falls was a concern, as was what industry should be doing to assist with government prevention efforts. In addition, the group discussed new technology solutions on the horizon as well as easing the regulatory burden to help identify and prevent security threats.

The full discussion is presented below.

DISCUSSION

A working group on UAS security discussed the role government and industry should play to encourage UAS users to adopt specific standards to obviate the need for significant regulatory burden.

Everyone agreed that the need for counter-UAS security measures is significant and urgent.

Domestically, the United States has so far been spared from a deadly UAS attack. But participants agreed it is only a matter of time before one is carried out. With “the clock ticking,” the U.S. has yet to establish the technology to prevent it or provide law enforcement with the tools to respond.

One government representative pointed out that, until the present, the military has “enjoyed more or less total air dominance,” while jersey barriers, walls and other security measures have provided protection on the ground. Now, border barriers can be bypassed by drones, prison walls can be bypassed with drones and security checkpoints at stadiums can be bypassed with drones.

“I’ve visited DOD facilities where we’ve spent literally a fortune putting in a big fence [that a] toy can go over,” the representative said.

The government representative went on to say that some people who appear to not yet acknowledge the danger that UAS pose are the hobbyists. An industry attendee said most think that because there hasn’t been a major lethal attack, a danger doesn’t exist.

“They’ll say, ‘how many hundreds of thousands have flown, and who’s been hurt by them? No one,’” the representative said. “They’re missing the point that it’s not a matter of ‘it hasn’t happened.’ It’s ‘when will it happen?’”

An industry representative that works closely with hobbyists didn’t disagree and pointed out that, unlike cars and firearms, which are often compared to drones when considering safety regulations, a teenager can easily assemble a drone in her or his garage.

“We can build a drone that can carry a significant payload at 90 miles an hour and go several miles to the site. That’s a pretty serious piece of equipment,” the industry representative said.

In that sense, the representative equated drones to hacking. “A 15-year-old can build one of these things from scratch, from parts they can order.” And the representative suggested that the private sector be given “wide berth to try to keep up.”

Some attendees said that a major challenge will be to convince the public that adopting some form of surveillance technology is necessary to ensure public safety. There was acknowledgement that it was critical to get that support before a catastrophic event occurs.

A government representative asked people to leave the session thinking about how the government could compare UAS risks to those on the ground that people are familiar with.

“How do we make sure that people out there begin to understand what the relative risk is of a drone falling out of the sky?” the representative said. “How do they stack up against all the other threats?”

In addition to overcoming the lack of perceived risk on the part of the public, government and industry face other challenges in ensuring high rates of adoption for counter-UAS technology. Privacy concerns will always be an issue. So, too, will complacency, if new technology must be added, installed or maintained by individual users.

“You have to realize the hobbyists have been doing things the hobby way for many, many, many years, and now we want to impose something on them that they have to stop and think about and they have to do,” said an industry representative.

The representative then told the story of one event where hobbyists were given strict instructions to fly only with a visual observer. Participants abided by the rules for the first two days of the four-day event before “complete chaos” set in.

“And unfortunately … I see it: the laziness, the complacency will set in fairly quickly,” the representative added. While requiring the installation of tracking devices aboard UASs may be one solution, they present legal challenges under existing law. Looking at the maritime and manned-flight space communities as an example, there is an incentive to turn on transponders and radar devices. “You turn on that transponder in order to be tracked,” said a government representative. “Furthermore, you don’t have to have a transponder,” for instance, if you’re flying a crop duster.

For ships, only those over 50 tons are required by law to turn on their automatic identification system. Post 9/11, the government faced the same dilemma with boats that it does now with drones: how to identify the potential bad actors from the thousands of small boats. The agency involved developed an app that would track boaters but also give them free access to data that would help them navigate more safely. “The intention is that down the road … it would be the case the boater would voluntarily agree to tell the database where they are.”

No technology will be a panacea. On that, everyone agreed. It is too easy for bad actors to disable or alter any technology embedded in drones.

At the same time, however, off the battlefield, even basic technology like beacons or mandated flight plans could help domestic law enforcement isolate the tiny percentage of potentially bad actors. “It helps detect the outliers,” said another government representative.

Regulations should not be viewed as a burden, but as an opportunity to clarify where industry should invest in solutions, said a government attendee. “The whole reason the GPS is even in your smartphone today is because of an FCC rule that said, ‘Hey, we’ve got to be able to find where the phone is.’ And that created a whole market around the ability to easily determine your position with a consumer-oriented device,” the representative said, adding that it’s early enough in counter-UAS technology to create the same kind of regulatory clarity. “If we can develop that framework in a way that’s flexible but codified enough so that people, communities, countries, can count on it, then I think that’s the touchstone.”

An industry representative equated the current period to the dawn of aviation, when there was a regulatory acknowledgment that safety had to take precedence. “I think we’re back at 1926 in many ways with a brand new technology,” the representative said, and called for greater collaboration between pilots, regulators and technologists at this critical time. Law enforcement, the representative and others agreed, also needs tools to respond.

“What we’re seeing right now is a culture of noncompliance among recreational operators,” the representative continued, who said data from manufacturers themselves can now support such an assertion. “We’re seeing thousands of operations in the vicinity of large hub airports weekly, with a dozen notifications. So now we know without any doubt that there are thousands of illegal operations [occurring] on a weekly basis. We need to find a way to bring them into compliance.”

Industry representatives in attendance did not object to the idea of regulations. An industry attendee warned that there could be pushback from industry and the public and that there could be unintended consequences of any uniform technology: for example, the potential hacking by hostile nations of a public key-encryption system.

The representative said its company has talked to insurance companies about leasing mitigation systems for events seeking protection from drone mishaps. The key may be to have multiple stakeholders all with a vested interest in safety.

If government could define the quality standards and lay out the legal parameters, then industry could quickly and inexpensively begin to produce solutions, said another industry representative. “I would propose that there’s technology out there today that’s mature enough to deal with the vast majority of the problems we see today, but we can’t do it because we’re not sure it’s legal, or it has some impact,” the representative said. “If you want to unleash innovation in industry, then you at least have to give them room to run.”

From there, government can create industry standards.

It’s an approach that’s in use in the maritime space today, said the government representative who spoke earlier about boat identification. Shippers are given access to higher tiers at port based on the security measures they’ve voluntarily employed. “They want to ensure they’re operating safely and in the most secure manner so government will leave them alone,” the government representative said.

Certainly greater technologies will emerge. One industry attendee said they’d like to see a more unified federal policy in research and development regarding UAS to facilitate research grants. “As a technologist and innovator, it’s hard for me to figure out where to go.”

The industry attendee’s further comments offered one of the only hopeful parts of a session largely focused on the challenges of providing UAS security with the current technology. Advanced systems in perception and autonomy may be able to identify drones by their behavior, for example.

“All systems need to comply with the laws of physics,” the industry representative said. “They all have trajectories. They all have masses. They exhibit behaviors whether they’re detectable by their friendly ID or whether they’re operating nefariously. You could sort of map that set of behaviors and identify whether he’s friendly and operating in a passive way. Similarly, someone closer to a higher value target who’s exhibiting a trajectory that’s anomalous could be rapidly identified.”

Federal research and development investment could have significant payoffs, for both domestic and overseas operations. A government representative said federal agencies dealing with counter-UAS are, in fact, now trying to coordinate into a single entity and overlap private and military research. “We share that dream,” the government representative said.

Conclusion

The UAS industry continues to advance towards a commercially viable position. However, the issues discussed at the workshop's breakout sessions illustrate how there still are technical, social and logistical hurdles that the unmanned systems community has to address before UAS can be fully integrated into the NAS.

All the sessions proved that communication between government agencies, industry and academia will be crucial to rapidly advancing the technology. To get there, the government is seeking a way to make communication more fluid and the tools it uses more agile, so it can respond quickly and efficiently. Industry and academic representatives overall expressed a willingness to help the government meet its goals for the industry and are eager to share their lessons learned as they begin to fly legally and commercially under the FAA's small UAS rule.