

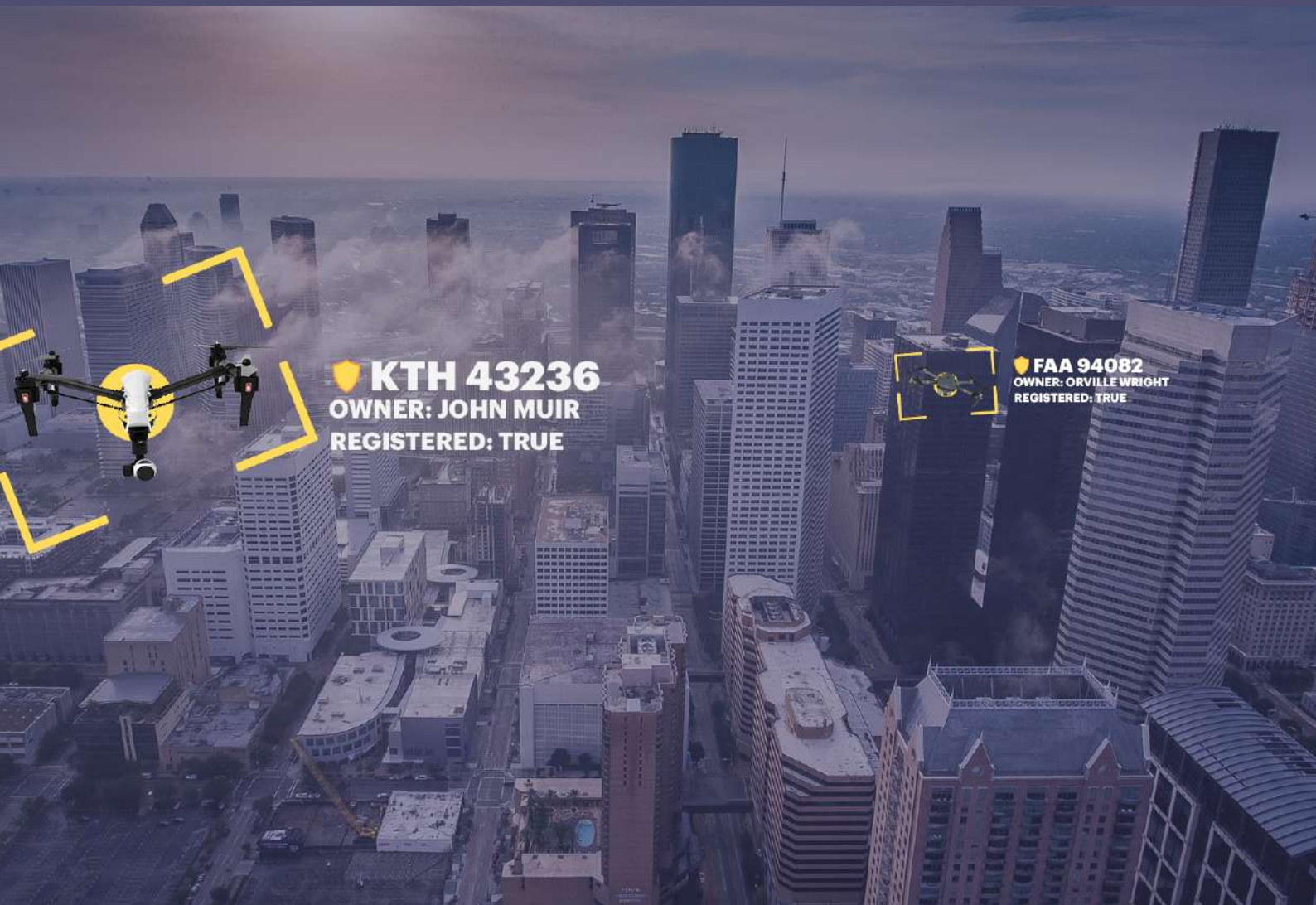


Remote ID



Remote ID & Commercial Drones

Enabling Identification and Transparency
in the National Airspace



EXECUTIVE SUMMARY

The commercial drone industry is booming. By 2022, International Data Corporation predicts that the number of U.S. commercial drones will hit 5.7 million by 2022 up from 1.8 million in 2018.

As the industry matures, how we identify and track the rapidly-growing numbers of commercial drones in the sky is quickly becoming the most important problem to solve to encourage this growth. Individual pilots, drone service providers, large companies and law enforcement alike all have a vested interest in bringing order and transparency to our skies.

Remote ID is the concept of a system that identifies drones operating in the NAS and can be thought of as similar to a digital license plate for drones. In 2019, it is the much-needed solution to many issues which must be solved in order to kick off the next stage of growth that commercial drone industry stakeholders know is right around the corner.

In this whitepaper, we cover what Remote ID is, why Remote ID is so important, what Remote ID will allow enterprise drone programs to do, how Remote ID will work in practice, and predictions for progress in the very near future.

We spoke with a variety of industry stakeholders who shared their thoughts on what Remote ID means for their business and what will be possible with widespread Remote ID in the NAS. Many of these experts expressed similar themes about Remote ID, its progress thus far, and its promise for the future of the commercial drone industry.

Remote ID in practice, not concept will normalize advanced, high-ROI operations in the NAS, increase public trust in and comfort with widespread commercial drone operations, enable safety data-gathering to inform smarter policy-making and prevent unnecessary over-regulation that might otherwise stunt growth.

A Brief History of Aircraft Identification

THE HISTORY OF IDENTIFYING AIRCRAFT IN THE UNITED STATES IN THE FORMATIVE YEARS OF AVIATION IS VERY RELEVANT TO THE CURRENT SITUATION WITH IDENTIFYING DRONES.

Then, a new technology (airplanes) grew quickly and necessitated a way of identifying and differentiating among various aircraft. From the 1920s, when aircraft in the United States first began to operate in significant enough numbers to warrant identification and registration, until 1960, the FAA and its predecessor agencies went through a variety of ways of identifying aircraft operating in the National Airspace (NAS).

First, different letters were used depending on whether the operating entity was commercial, state, or private. Then, N-numbers (the letter N followed by a combination of numbers) were introduced and required for aircraft engaged in foreign air commerce. By 1960, N-numbers as we know them today were required for all fixed-wing aircraft, required to be in the same format, and required to be located on the same location of the aircraft.



Original Aviation ID Solutions Were Very Low Tech

ALL YOU HAD TO DO WAS...

1. REGISTER WITH THE FAA
2. PAINT THE NUMBER ON THE WING
3. USE IT WITH AIR TRAFFIC CONTROL

In recent years, the FAA has been struggling to figure out the right way of identifying the potentially millions of commercial drones operating in the national airspace in the near future.

Previous efforts at generating consensus around Remote ID have hit a variety of roadblocks in the past few years. Throughout 2017, the FAA gathered industry stakeholders and experts in a series of meetings and working groups to discuss and inform future rule-making, leading to the December 2017 Remote ID and Tracking Aviation Rulemaking Committee. This report had a lot of great ideas about how Remote ID might work, but it suffered from disagreement over who would be subject to Remote ID requirements.



“There is broad agreement that Remote ID is important and necessary, but it has been difficult to get broad agreement on specific details about how it will work and who it will cover.”

Uber

- Kate Fraser
Head of Policy, Aviation

What Exactly is Remote ID?

DISTILLED INTO ITS MOST BASIC ELEMENTS, REMOTE ID IS THE CONCEPT THAT DRONES IN THE AIR NEED A WAY TO BE IDENTIFIED TO INCREASE SAFETY, ACCOUNTABILITY, AND ENFORCEMENT OF LAWS AND REGULATIONS - JUST LIKE WE DO WITH MANY OTHER METHODS OF POWERED MOBILITY AND TRANSPORT.

The concept of Remote ID begins with establishing that there are a few crucial differences between drones, cars, manned aircraft, and other types of transportation and mobility methods. The identification aspect is familiar, since we already have methods of identifying many other vehicles used to transport people or objects (e.g. license plates, N-numbers, etc.).

The remote aspect is the more novel problem to solve for - the biggest difference between drones and nearly every other method of powered transportation is that the operator and the vehicle are not located in the same place, which makes accountability more complicated.



Remote ID is Like the License Plate of Drones

- NUMBER AND LETTER STRING THAT UNIQUELY IDENTIFIES THE OBJECT
- REQUIRED BY LAW (SOON TO BE FOR DRONES)
- ENSURES TRANSPARENCY AND RESPONSIBILITY WITHOUT ENABLING TRACKING

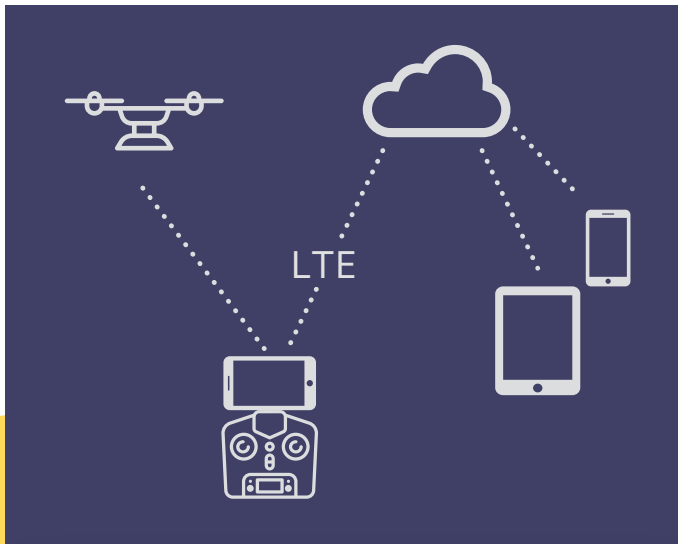
Comparing Approaches to Remote ID

THERE ARE TWO POPULAR METHODS OF REMOTE ID - "BROADCAST" AND "NETWORKED".

Some commercial drone industry stakeholders strongly prefer one method over the other, but in reality, the two methods are complementary and future Remote ID systems could utilize both methods depending on the mission. In December 2017, the [UAS Identification and Tracking Aviation Rulemaking Committee](#) included these methods among their top recommendations, and standards bodies have coalesced around developing standards for each method. Though the end goal of each method is to send data collected to an FAA-approved internet-based database, there are significant differences, benefits, and drawbacks to each approach, which we will explain and go into detail below.

The direct broadcast method involves transmitting data in one direction only, with no specific destination or recipient. Among the envisioned broadcast methods are a variety of protocols to send signals from the drone itself to some sort of receiver on the ground. Most notably, broadcast protocols include [Bluetooth-based solutions](#), ADS-B modified and restricted for use with drones, ground-based radar solutions, and others.

The networked method involves transmitting data to an internet-based service. Most networked methods under development take advantage of the fact that most drone operators have a handheld supercomputer that they almost always have in their pocket - their smartphone.



NETWORKED

Software enables multiple parties to both consume and populate data. Relies on networks like LTE and the forthcoming 5G. Interoperable.



BROADCAST

Hardware transmits a specific signal that can only be consumed by parties with receiver capabilities. Not dependent on network coverage. Often proprietary.

BROADCAST REMOTE ID

Broadcast Remote ID is a useful method of identifying drones operating nearby and is worth mentioning in the conversation about Remote ID. Having a drone broadcast a signal to a receiver on the ground may be a solution for some mission types operating in a small area. However, over longer distances, maintaining a signal between broadcaster and receiver might not be possible, or there might be too many receivers required to be a feasible solution.

Two examples of Broadcast Remote ID are Intel's Open Drone ID concept and DJI's Aersoscope product.

NETWORKED REMOTE ID

The FAA envisions this type of Remote ID as a networked system where operators connect to one of many FAA-approved UAS Service Suppliers (USS), who serve as the middle-man between those operators and the FAA systems via an FAA API.

The FAA's current vision and process for Remote ID is conceptually similar to the FAA's LAANC (Low Altitude Authorization and Notification Capability) program. FAA-approved USS will be able to provide LAANC authorizations and/or Remote ID services to the general public via the USS's connection to an FAA API which feeds into a number of FAA systems and data sources.

THE INTERUSS MODEL

One form that a near-future network-based Remote ID solution could take would be similar to the InterUSS project. Aloft participated in a demonstration of this solution in December 2018, in order to showcase the ability to provide Remote ID using current technology. InterUSS is a project that allows law enforcement, companies, other pilots, and the general public to identify drones operating in their vicinity. The InterUSS platform allows multiple USS to show certain information from their operations in order to inform other stakeholders. InterUSS is a demonstration of a network-based Remote ID solution that is functional today without any special hardware. As a proof of concept, it shows that the future of Remote ID lies in collaboration amongst the many stakeholders of the commercial drone industry, including the general public.



Benefits of Remote ID

Initial public interest in drones sparked news cycles promising package and food delivery via drone. As that hype has worn off, more practical questions about how safety and security can be governed have emerged. Virtually all of these critical questions

bring the role of identity front and center. Remote ID is the key to addressing these challenges that brings with it benefits to the industry, public safety and privacy alike.

- 1. Advanced operations without special authorizations**
- 2. Increased public trust**
- 3. Data to inform better policy-making**
- 4. Operator accountability and compliance**
- 5. Avoiding over-regulation**

1.

Remote ID unlocks the ability to perform routine, advanced operations in the national airspace (NAS)

For some time now, industry stakeholders have known that despite the significant ROI they see from their enterprise drone programs, the highest value operations are not routinely available - and this is largely attributable to the slow progression of Remote ID.

High-ROI operations that are most compelling to enterprise drone programs are the ability to fly

commercial drone operations over people, beyond visual line of sight (BVLOS), and at night. These operations are not allowed under the current regulatory framework of Part 107. Currently, these operations are only available to companies that apply to the FAA for waivers from these prohibitions - often a lengthy, time-consuming, and expensive process.



“Outside of some limited operations conducted under waivers, commercial operators are being locked out of operations over people and other expanded operations until the Remote ID rule is implemented.”



- Diana Cooper
Senior VP of Strategy and Policy



Why are routine, advanced operations in the NAS a game-changer for enterprise drone programs?

For the commercial drone industry in the US to grow and mature, these advanced operations are going to need to be routine and easily repeatable, without the burdensome waiver process. Most advanced operations currently are not routine - they require significant investment of time, money, and energy to work with consultants, lawyers, aviation experts, and others in order to get permission to perform advanced operations. The mentality here should be that compliant, identified operators should be allowed to perform these operations without the mountain of extraneous paperwork currently required. Instead, a definitive rule-

making by the FAA allowing waiverless operations within a limited scope, verified to be compliant by using a Remote ID solution, means that companies can go fly the missions they want to fly with the ability to prove their compliance with FAA rules.

For example, drone delivery is simply not feasible if the drone must be in visual line of sight of the operator at all times. If the drone has to stay within a few hundred feet of the operator, it is not cost effective to send out a drone operator to every location in advance of delivery.

2.

Remote ID increases public trust in and comfort with widespread commercial drone operations

Remote ID will increase public trust and acceptance of drone operations, which is needed to make the public more comfortable with increased operations. The ability to put fear and potential hostility at ease is a big deal to

Remote ID allows enterprise drone programs to operate with a much greater level of transparency. When most of the general public sees a drone operating, they really want to know two things about that drone to put themselves at ease:



“The commercial drone industry in general benefits from Remote ID. Ultimately, Remote ID will enable wider enterprise adoption and should be able to open the skies for commercial flights over people.”

- Amber McDonald
President and CEO



enterprise drone programs - the more comfortable the public is with drones operating around them in their daily life, the more comfortable they will continue to be as enterprise drone operations become more commonplace.

Who are they and what are they doing? If that drone belongs to a known entity doing something ordinary, most people’s concern with the drone operating above them goes away. Ultimately, just the peace of mind that in most cases they can identify or report a drone if it is doing something abnormal is probably enough to make most people a lot more comfortable with seeing a drone flying overhead more often.

3.

Remote ID is necessary to gather data and inform better policy-making

In speaking with multiple drone-industry experts, policy-makers, and commercial drone operators, a repeated assertion was that Remote ID will give policy-makers better data to make better decisions. Without data, we can't make smart policy, and Remote ID will provide that data.

In the absence of information, decision-makers tend to choose the decision that comes closest

to make educated, precise, and justifiable decisions.

Many cities and states are making regulations unfriendly to drone operations without the data to back up their stated concern. Local officials can offer many qualitative concerns (e.g. too noisy, privacy, lack of accountability, etc.) but there is a conspicuous absence of quantitative concerns to back up their assertions. Data,



“In the absence of data, regulators have trouble making rules. Data gathered by Remote ID will give regulators data they need to accelerate rule-making for advanced operations.”

AIRMAP

- Ben Marcus
Chairman

to guaranteeing a safe result - especially those whose decisions potentially affect the health and safety of the public. If we assume risk is infinite, regulators will recommend burdensome and expensive solutions. This illustrates the importance of informing policy-making with actionable data that allows decision-makers

gathered from Remote ID in an aggregated and confidential manner, can assist local officials in making educated policy decisions that allow for the smart growth of commercial drone operations.

4.

Compliant enterprise drone operations want Remote ID

Our customers want to be able to broadcast that they are trusted (usually well-known or name-brand) operators who are doing things the right way in a transparent manner - Remote ID helps them prove this and gets the public more comfortable with increasingly ubiquitous drone operations.

From our conversations with operators themselves and with platforms or products that serve enterprise drone operations, it became clear that most operators in enterprise drone programs want Remote ID. They see it as much more of a benefit than a burden to demonstrate their compliance to the general public.

“Responsible drone operators understand that Remote ID is a solution that might otherwise be replaced by some manner of flight restriction. But in order for Remote ID to be viable at all, we must achieve maximum voluntary compliance by keeping operators’ costs and burdens as low as possible, and ensure the privacy of their flight operations.”



- Brendan Schulman
VP of Policy and Legal Affairs

Remote ID will allow trusted operators to show who they are and show that they are operating compliantly. Mostly, enterprise drone programs see Remote ID as beneficial because it will open up opportunities to perform their valuable work with fewer interruptions.

5.

Remote ID will enable more effective enforcement of current laws, instead of limiting the commercial drone industry with over-regulation by cities and states

The needs of law enforcement to identify drones as part of their duty to protect public safety is a real and growing concern. Counter-UAS (C-UAS) is increasingly earning more mind-share in the commercial drone industry as drones become more ubiquitous and newsworthy (for good and bad reasons). The incident at London's Gatwick airport in December 2018, where allegedly multiple drones were spotted over the course of 72 hours, causing chaos as the airport closed and reopened many times, illustrates how Remote ID can play a role in protecting high-value and sensitive areas.

Remote ID will help limit the proliferation of laws enacted by a patchwork quilt of cities and states specifically targeting drones and drone operations. Particularly amongst those active in developing legal and policy matters around drones is the belief that Remote ID can lead to more effective enforcement of federal and state laws already in existence - thus eliminating the need for restrictive rules only applicable to drones.

Instead of over-regulating the drone industry with rules, restrictions, and laws, Remote ID will help enforce laws already on the books. This is one way to get state and local authorities to stop making unnecessarily restrictive rules that apply only to drones. There is a better way.

There is no need to make a new law that says that invading someone's privacy or causing a nuisance using a drone is a crime. We already have nuisance laws and privacy laws that protect the rights of individuals and property owners. Currently, with no ability to know anything about the drone flying over a particular place, current laws are difficult to enforce - imagine trying to file a police report on a car with no license plate. With implemented near-universal Remote ID, the public and law enforcement will be able to identify that drone and hold it accountable for potentially bad conduct.



PRIVACY CONSIDERATIONS

The general public has concerns about the effect that drones will have on their personal privacy, and operators have concerns about giving up too much of their personal information in order to participate in commercial drone operations. That is why beyond a small amount of required information, there should be a level of freedom to determine the amount of information you want to share when operating in the NAS.

Part of the reason Aloft has supported projects like InterUSS is that it replicates a mode of privacy usually found in reality. In reality, there is no universal view. Instead, there is a more ephemeral ability and need to see what is around you in real-time time.

Privacy is also important to enterprise drone operations because of the sometimes sensitive nature of their missions and the data they're collecting. However, it can't be overlooked that there really is not an expectation of privacy when operating in the NAS - some data has to be shared. Other times, certain drone operations might want to provide as much information as possible in the interests of transparency. A flexible approach to privacy in relation to commercial drone operations is necessary.

Use Cases Enabled by Remote ID

Remote ID will extend the operating environment for drones in critical areas. New use cases will emerge as the technology becomes more mainstream and the capabilities of drones increases. With a more reliable operational and compliance framework established, special use cases will become everyday functions.

Drone delivery and inspection of road, rail, or pipelines will require Beyond-Visual-Line-Of-Sight (BVLOS) for flying miles away from the operator. BVLOS missions will likely require Remote ID because the operator and the aircraft will not be in the same place - and Remote ID is going to be most likely to be required when the operator is unidentified. Regulation aside,

it probably would not be economical to delivery items via drone if the operator had to maintain visual line of sight with the drone during the delivery process or while flying for miles at a time in remote areas.

Inspecting sensitive areas is another use case of commercial drones that will be enabled by Remote ID. When operating in sensitive or industrial areas, it is important to know the identity of the operator of every drone. If you have to treat every drone like a threat because you don't have information about its identity, operations will be less effective. The ability to identify drones as your own or as friendly goes a long way to maintaining security.



“For commercial drone operations to scale, Remote ID is going to be necessary. If you want to have a robust commercial operation and ecosystem, you will need Remote ID.”



- Harrison Wolf
Project Lead, Drones and Tomorrow's Airspace



The use of drones by journalists and media is another use case of commercial drones that will be improved by Remote ID. Instead of being interfered with on the ground while they exercise their First Amendment rights, journalists in particular often want to identify themselves to the public and to anyone else on the ground that they are from a media organization and that they have a right to be operating where they are.

Operating drones near populated areas is another use case of commercial drones that will be improved by Remote ID. Large enterprise drone programs who operate safely near populated areas

want to identify themselves as that trusted organization. If an enterprise drone program is well-trained and professional and belongs to a trusted organization like an insurance company, that organization's reputation can be used to prevent interference and explain their presence on scene.



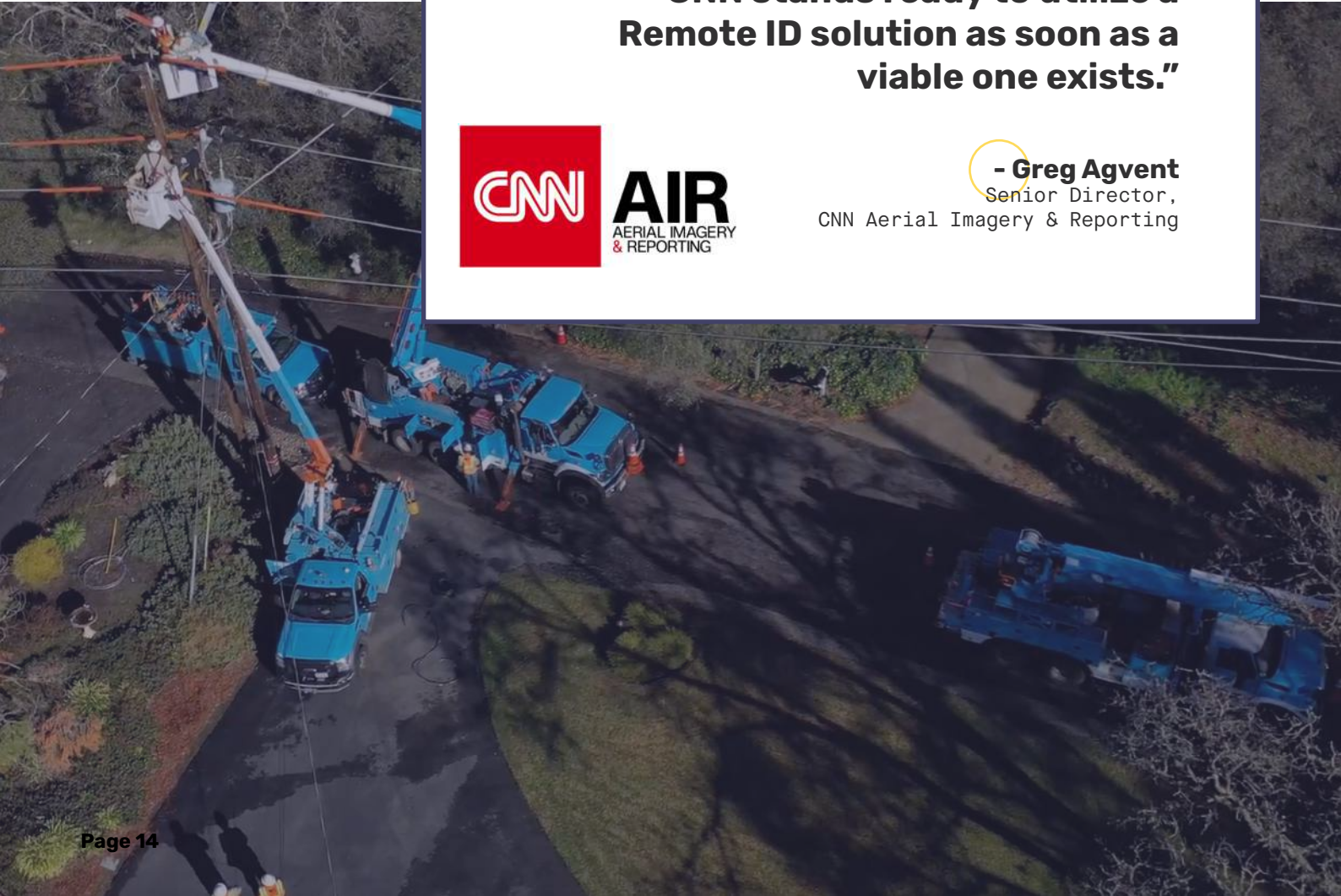
“Remote identification is necessary to enable the positive outcomes that are going to come from a drone enabled economy. CNN stands ready to utilize a Remote ID solution as soon as a viable one exists.”



AIR
AERIAL IMAGERY
& REPORTING

- Greg Agvent
Senior Director,

CNN Aerial Imagery & Reporting



Predictions for Remote ID

In December 2018, Aloft made our "[2019 Predictions for Remote ID](#)", where we predicted that Remote ID would progress in the FAA rulemaking process, would be backed by national and international technology standards currently under development, would become a standard security measure, and would see preemptive private industry action in the absence of progress at the federal level.

In addition to our research for this paper,

we asked our broad cross-section of industry experts for their own predictions about Remote ID. We're grateful for their participation, their leadership in our emerging industry and their willingness to look into the future with us.

"A successful 2019 would be the issuance of a technology-neutral interim final rule on Remote ID in line with the ASTM standard currently under development."

- Diana Cooper Senior VP of Strategy and Policy - PrecisionHawk

"By 2020, we will be discussing countries who have actually implemented universal Remote ID. The conversation will shift to how we build on Remote ID to unlock new operational capabilities and economic opportunity for the drone industry."

- Ben Marcus Chairman - AirMap

"Late 2019: The comment period has closed on the FAA's Remote ID proposal, the first set of industry standards have been completed, and we are awaiting FAA's review of comments and finalization of the requirements, which will probably take another year from that point."

- Brendan Schulman VP of Policy and Legal Affairs - DJI

"We will probably have an ASTM standard this year, which can be persuasive, but we might not have a Remote ID NPRM."

- Amber McDonald President and CEO - Indemnis

"Rules for flights over people or beyond visual line of sight will be restrictive until there are mechanisms for accountability - Remote ID is one way to do that."

- Harrison Wolf Project Lead, Drones and Tomorrow's Airspace - World Economic Forum

"There have been big steps in the right direction like the Integration Pilot Program (IPP) and the FAA Reauthorization Act but there's a lot that still has to happen."

- Kate Fraser Head of Policy, Aviation - Uber



Aloft (formerly Kittyhawk) is a leading enterprise software platform for drones. Aloft powers a platform that helps enterprise drone programs to operate and scale, comply with regulations, and fly safely. Enterprise drone programs - from small teams to large corporate operations with hundreds of licensed drone operators - use the Aloft platform every day.

Aloft is a member of the FAA's Unmanned Aircraft Safety Team, the ASTM F38 committee on Remote ID, and a participant in the InterUSS project. We are also an FAA-approved USS for the LAANC program, which enables on-demand airspace authorizations in controlled airspace, and the provider of the FAA's B4UFLy app.

To learn more about Aloft, visit www.aloft.ai and follow us on Twitter [@Aloftai](https://twitter.com/Aloftai)

