REMOTE CONTROL

Travis Scott *on why remote ID is just a good start and not an entire solution*

In recent years, the increasing popularity of drones has brought both tremendous advancements and significant challenges. One crucial challenge is ensuring the security of any given airspace from potential threats posed by nefarious and non-compliant drones – not just in and around airports, but around other sensitive areas or critical infrastructure like power plants, chemical facilities or even at borders or near prisons where drones can ferry drugs or other contraband.

While the implementation of Remote ID regulations by the FAA is a step in the right direction, relying solely on this technology is simply insufficient for complete airspace security. This overview explores what Remote ID is, what the upcoming regulations are, the limitations of a drone detection system solely dependent upon Remote ID, and the necessity of more complete and proactive drone detection solutions to effectively safeguard airspace.

Remote ID, mandated by aviation authorities, requires drones to broadcast identification information. This information includes the drone's identity, location and flight details, providing valuable insights for authorities to monitor and track drone activities to keep airspaces clear and prevent possible collisions.

Some have likened Remote ID to a drone license plate. Much like license plates, either a serial number or session ID is broadcast, although the drone operator's information may not be. This information can be used by authorised individuals, like police officers, to contact the FAA and get the drone owner's information, provided that the drone is registered with the FAA.

As of 16 December, 2022, all new drone manufacturers are now required to equip their drones with a Remote ID 'beacon' that can broadcast the required information during the manufacturing process.

A proactive drone detection solution offers a comprehensive approach to airspace security

As of 16 September, 2023, the US Federal Aviation Administration (FAA) now requires all Uncrewed Aerial System (UAS/aka drone) operators, who are already required to register their drones with the FAA, to be compliant with Remote ID rules. However, at the last minute, the FAA also announced that it will: "consider all factors in determining whether to take enforcement action" through 16 March, 2024, due to some availability issues for broadcast modules, which are pieces of hardware that can be affixed to the aircraft to ensure compliance if it does not have Remote ID functionality built in. The FAA also has a database that can be consulted to ascertain whether or not a specific model is already compliant (even if it was built before the December 2022 deadline, as some models had the hardware prior to this date).

This regulation applies to drones over 250g and all non-recreational drones regardless of weight. Recreational drones under 250g do not have to transmit Remote ID information. The lack of exceptions for non-recreational drones acknowledges the rate they are being adopted in a number of industries despite the slow development of beyond visual line of sight (BVLOS) regulations.

Currently, piloting a drone in the United States requires someone to have eyes on the drone no matter where it is, resulting in law enforcement posting officers on every fifth roof or so to keep eyes on it for example. Research is being conducted to help change these regulations to allow for BVLOS flying or, if nothing else, make it easier to obtain waivers to pilot drones BVLOS.

Currently, these waivers are so difficult to obtain that there have only been about 211 total issued since 2019, and many of those are repeat applications based on expiration dates of previous waivers. (Looking at the first page alone shows that one company alone had five waivers issued, for example.)

Once this changes, expect to see the non-recreational use of drones to explode. With capabilities in payload quickly expanding, drone delivery of packages may become ubiquitous, reducing congestion on the roads. In other areas, increased payload capacity could lead to drones delivering medical supplies or treatments to remote or rural areas around the world, potentially saving lives. Law enforcement and emergency services can send drones in to act as first responders and gather more information about an incident before humans are even on the scene. In agriculture, drones can be used for a number of purposes, including monitoring crop and plant health, water quality, and herd health; pest detection and control; and data collection for resource and land management. They can similarly be used to assess the impacts of climate change on different environments globally. Finally, drones can be used to inspect critical infrastructure – from power lines to buildings themselves. With so many uses already feasible and likely many more to come in the future as technology continues to advance, Remote ID broadcasting will be a major factor in preventing aerial collisions and otherwise protecting the skies.

SYSTEMS THAT DON'T RELY ON PILOT COMPLIANCE PRESENT A FAR MORE ROBUST SECURITY OPTION

Does Remote ID ensure safe skies? Not on its own. Remote ID is a significant step in creating safer airspaces, but despite the clear advantages of Remote ID over nothing at all, it is vital to acknowledge its two key limitations.

One critical flaw of a Remote ID-only system is that it heavily relies on drone operators' compliance. Criminals, intent on exploiting drones for illegal activities, are unlikely to abide by the regulations or broadcast their location with Remote ID. By flying drones without identification signals, they can easily avoid detection, jeopardising public safety and national security alike. Similar to a bank robber removing the license plate of their get-away car to avoid capture, a nefarious pilot will simply disable or remove their drone's Remote ID.

In addition, recreational pilots may not even know about the regulations and continue flying their drones without a beacon of any kind, inadvertently causing havoc if and when they aren't detected near a sensitive area. This lack of awareness around regulations has contributed to the lack of a concrete number of drones in operation in the US. We know how many have been registered (over 860,000, both commercial and recreational) but it's extremely likely that many more have been sold without subsequently being registered. In part, this is due to drones under the 250-gram limit

not requiring registration – and aside from light toy drones, there are drones sold by major manufacturers like DJI that also come under that weight limit.

Second, it is very easy to 'spoof' a Remote ID. This is a clever way for bad actors to create fake drones that do not even exist in the sky or otherwise disguise the location of their drones with an app. They could show a dozen different fake drones with their respective pilot locations and hide the one real drone/pilot within the pretend drone swarm. Even with just one drone, spoofing its location and pilot location could get a security team to focus on one side of a location while the drone simply flies in on the other, unmonitored side. It's so easy, in fact, that simply searching "spoof remote ID" returns pages of results for both videos and online posts discussing how to do it, how easy it is, and whether or not the FAA might find itself with a problem when the mandate goes into effect.

Security teams that therefore decide that being able to detect Remote ID signals is good enough will only find that their drone issues will get worse. It is simply too easy to get around requirements. As with any security apparatus, layers and a more proactive approach to drone detection will be essential to provide adequate protection.

A proactive drone detection solution offers a comprehensive approach to airspace security. A successful system does not rely solely on a drone broadcasting node and can instead detect and identify all drones in the vicinity, regardless of whether they transmit Remote ID signals, by layering different technologies together. This approach allows for proactive threat mitigation, as suspicious drone activities can be promptly identified and thwarted before any harm is done.

A base system utilising radio frequency or other types of sensors can be enhanced with cameras or connected to already-extant cameras to enable security professionals to identify a drone's payload and even gather images of the pilot. Even radar can be easily added to extend the range of the system for larger and more sensitive areas.

Furthermore, the capabilities of a multi-sensor system go beyond mere detection. With advanced analytics and machine learning algorithms, a drone detection system can also distinguish between harmless recreational drones and potentially malicious ones by identifying if a payload is being carried, for example, enabling authorities to prioritise and respond to genuine threats more effectively.

Moreover, a layered approach like this also collects more information about each and every flight in a given airspace. This information can then be leveraged to identify and tag drones that have historically posed greater threats like breaking FAA altitude restrictions, flying into Temporary Flight Restriction areas or breaching other types of restricted airspace, such as around airports or even in cities such as New York, where all of Manhattan and the Bronx are considered no fly zones. Gathered data can also be used to identify weaknesses in a current system and further harden defences. Such comprehensive monitoring is essential, given the ever-evolving tactics employed by those seeking to exploit drone technology for illegal purposes.

To conclude, while Remote ID regulations are a necessary first step in enhancing drone accountability, they are insufficient for comprehensive airspace security. Criminal elements are unlikely to adhere to these rules, rendering a Remote ID-only detection system inadequate. The adoption of a proactive monitoring system that does not rely on pilot compliance presents a more robust and effective approach to airspace security, as it can detect all drones in the vicinity whether or not they have active Remote ID broadcast modules. By investing in such technologies, we can ensure a safer and more secure airspace for all ●

Travis Scott is Senior Director of Sales at Dedrone.

Manufacturers are required to equip their drones with a Remote ID 'beacon' that can broadcast the required information during the manufacturing process