Volume 3, No. 5 | September–October 2020

RAIL

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 3, No. 5 | September–October 2020

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Journal Designer: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8am–8pm Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)
ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

What's in the FAA's Proposed Drone Remote Identification Rule

Brent Connor and Jason D. Tutrone*

The Federal Aviation Administration has issued a proposed rule requiring remote identification of drones.

The Federal Aviation Administration ("FAA") has published a long-awaited proposed rule[1] that would require remote identification ("Remote ID") of unmanned aircraft systems ("UAS" or "drones"). The Remote ID rule is a critical step toward expanding drone operations, like package delivery and flights over people and at night, because it addresses many attendant drone safety and security issues, including operations near manned aircraft and overflights of critical infrastructure, large gatherings of people, recreational facilities, and military installations.

Recent news reports of mysterious drone swarms flying at night over Colorado and Nebraska[2] and unauthorized drone operations near airports underscore the need for Remote ID. Currently, the FAA and others can primarily only identify and locate drones and their operators by sight, but because of their small size and remote operation, visually identifying a drone that poses safety and security risks, and locating its operator is difficult.

Remote ID would enable the FAA and law enforcement to electronically locate and identify drones, similar to how the FAA electronically tracks commercial airliners. It also can provide airspace users and air traffic controllers with location information for drones that might pose a collision risk.

Thus, Remote ID provides the FAA and law enforcement with important capability to identify and address drone safety and security risks. It also is critical to establishing UAS traffic management capabilities that will help manage traffic conflicts for drone operations beyond visual line of sight ("BVLOS").

The FAA envisions that full implementation of Remote ID will require three elements:

Robotics, Artificial Intelligence & Law / September–October 2020, Vol. 3, No. 5, pp. 311–316.

ISSN 2575-5633 (print) /ISSN 2575-5617 (online)

1. The Remote ID rule, which establishes operational requirements and UAS design and production standards necessary to enable Remote ID.
2. A network of third-party Remote ID UAS Service Suppliers ("Remote ID USS") that will collect identification data from in-flight UAS. Remote ID USS would operate under a contract with the FAA, and some may charge for their services.
3. A collection of technical requirements developed by standards-setting organizations to meet the performance-based design and production requirements in the Remote ID rule.

UAS Operating Requirements

Under the rule, all UAS operations, with a few limited exceptions, must comply with one of three Remote ID operating categories:

1. Standard Remote ID, which requires the UAS to broadcast identification and location information from the aircraft and simultaneously transmit that information via the internet to a Remote ID USS.
2. Limited Remote ID, which only requires the UAS to transmit identification and location information via the internet to a Remote ID USS. The unmanned aircraft in these operations must be designed to operate no more than 400 feet from the control station and the operations must occur within visual line of sight.
3. No Remote ID, which does not require the UAS to transmit identification and location information, but limits UAS operations to within visual line of sight and the boundaries of an "FAA-recognized identification area."

The FAA expects that the vast majority of UAS will operate within the Standard or Limited Remote ID categories. Also, UAS manufactured with Standard or Limited Remote ID capability must operate within their respective category (e.g., they cannot be operated in the No Remote ID category).

Manufacturer Requirements

To ensure that Remote ID is generally available, the rule would require all UAS, with a few limited exceptions, to be designed and produced to meet certain performance-based standards for Standard or Limited Remote ID. Manufacturers can use any FAA-approved means of compliance with the performance-based standards, and the FAA encourages consensus standards bodies to develop means of compliance with the standards.

Additionally, the rule would require manufacturers to assign each unmanned aircraft a unique serial number that would enable identification of the aircraft.

Other Important Aspects of the Rule

ADS-B Out

UAS would generally be prohibited from using Automatic Dependent Surveillance-Broadcast ("ADS-B") Out and transponders, which are technologies that manned aircraft use to provide location and identification information, unless specifically authorized by the FAA. These technologies do not have the bandwidth to accommodate UAS operations and would require additional infrastructure to support the low-altitude operations common among UAS.

FAA-Recognized Identification Areas

The rule envisions that FAA-recognized identification areas will be operated by community-based organizations ("CBOs"). Under the rule, only CBOs may apply to the FAA for the establishment of identification areas, and they must do so within 12 months after the FAA finalizes the rule.

Means of Compliance

The rule would prescribe requirements for a means of compliance, developed by a standards-setting organization or other person, that describes how a person designing or producing a

UAS can comply with the performance standards for the design and production of UAS with Remote ID capability. In addition, it prescribes procedural rules for obtaining FAA acceptance of a means of compliance and recordkeeping requirements for persons who submit an accepted means of compliance.

Registration

To ensure that the Remote ID information can be traced to a particular unmanned aircraft, the rule would generally require each one to be registered with the FAA. Today, multiple unmanned aircraft used for certain recreational operations can be registered under a single registration without identifying each individual aircraft.

Remote ID USS

Consistent with its desire to partner with third parties to provide aviation-related services to UAS, the FAA envisions partnering with Remote ID USS to provide four key functions:

1. Collect and store Remote ID messages.
2. Provide identification services on behalf of a UAS operator and act as the operator's access point to identification services.
3. Provide the FAA access to the Remote ID information collected and stored by the USS through a data connection that may be on demand or continuous.
4. Inform the FAA when the services are active and inactive.

A Remote ID USS may provide its services to the public or for a private fleet and it may charge for its services. The FAA anticipates that most Remote ID USS would come from private industry.

Tamper Resistance and Functionality Limits

The rule would require all Standard and Limited Remote ID UAS to have design features that inhibit tampering with the Remote ID functionality. In addition, these UAS must have features that

prevent takeoff when unable to make required transmissions of Remote ID information.

Compliance Dates

The requirements under the rule would be phased in according to the following schedule:

Date	Requirement
1 year after effective date	Applications for FAA-recognized identification areas must be submitted.
2 years after effective date	New UAS must meet Standard or Limited Remote ID design and production requirements. UAS registrations will require the aircraft's serial number.
3 years after effective date	All UAS operations must comply with Remote ID requirements.

Conclusion

In summary, the key points to keep in mind regarding the FAA's proposed rule:

- Remote ID would enable FAA and law enforcement to locate and identify drones.
- Commercial operators effectively must acquire Remote ID capability.
- The proposed rule eventually could lead to traffic management and BVLOS operations.

Notes

* Brent Connor is senior counsel in the Transportation and International Trade practice groups at Thompson Hine LLP. Jason D. Tutrone is an associate in the firm's Transportation group. The authors may be contacted at brent.connor@thompsonhine.com and jason.tutrone@thompsonhine.com, respectively.

1. https://www.federalregister.gov/documents/2019/12/31/2019-28100/remote-identification-of-unmanned-aircraft-systems.

2. *See, e.g.*, Brittany Shammas, "Drones Are Swarming over Colorado and Nebraska at Night," *The Washington Post*, Jan. 2. 2020, *available at* https://

www.washingtonpost.com/transportation/2020/01/02/drones-are-swarming-over-colorado-nebraska-night-authorities-say-they-have-no-idea-why/; Evan Simko-Bednarski, "Reports of Drone Disrupt Flights at Newark Airport," CNN, Jan. 22, 2019, *available at* https://www.cnn.com/2019/01/22/us/newark-drone-sightings/index.html.