Remote Identification

A Primer for Security Professionals

By Tom Adams (CEO of AeroVigilance, Co-Architect of C-UAS Hub) & Dawn Zoldi (Colonel USAF, Ret. & CEO/Founder P3 Tech Consulting)

Introduction

The Federal Aviation Administration (FAA) informally refers to its remote identification (RID) requirement as being akin to a "digital license plate" in the sky. The rule mandates that drones possess an in-flight capability "to provide certain identification, location, and performance information that people on the ground and other airspace users can receive."

According to the FAA, the purpose of the RID rule is "to help the FAA, law enforcement, and other federal agencies find the operator or the control station when a drone appears to be flying in an unsafe manner or where it is not allowed to fly. RID also lays the foundation of the safety and security groundwork needed for more complex drone operations."

Importantly, RID is coming to a drone near you...soon. The mandatory RID compliance date for registered drone operations begins on September 16th. This White Paper supplies the information that security professionals need to know to get up to speed on RID, including the history of the rule, what it requires (and does not), the status of the RID rollout and practical tips to operate in a post-RID environment.

This paper focuses on the RID rule in the United States. Similar RID rules have been or will be implemented in other countries around the world. The concepts for security and law enforcement professionals discussed here remain the same.

Historical Context

Appreciating the origins of the RID rule lends to a better understanding of it. The FAA did not decide to create the rule on its own; Congress directed the FAA to create it. It's also important to know that the RID rule builds on a series of other FAA rules all aimed at fully integrating drones into the national airspace system (NAS).

The first significant step towards drone integration occurred with the 2015 small uncrewed aircraft system (sUAS) registration and marking requirements, now found in 14 CFR 48. This original registration and marking rule underwent judicial scrutiny, Congressional fixes and later agency finalization. All drones weighing 0.55lbs up to 55 lbs, must be registered with the FAA, regardless of purpose.

The next big move occurred in 2016, when the FAA published the long-awaited Operation and Certification of sUAS, or "Part 107" rule. While it enabled a wide range of civil UAS operations, it also contained significant operational constraints. Notable limitations included the need to maintain visual line of sight (VLOS) and a prohibition on night operations, among others.

That same year, in its FAA Extension, Safety, and Security Act of 2016 (FESSA 2016), for the first time, Congress mentioned the need for an RID capability to provide near real-time situational awareness of sUAS in the NAS. Two years later, in the FAA Reauthorization Act of 2018, Congress provided the FAA with additional guidance and the explicit authority to create a mandatory RID rule.

In 2019, the FAA pushed out several important documents. In February, it published the Notice of Public Rulemaking (NPRM) on Operation of sUAS Over People (OOP rule). Then in December, it published the NPRM on RID.

The public had three months to comment on the RID NPRM. During that period, a wide range of interested parties provided an unprecedented 53,000 public comments. It took the FAA almost nine months to adjudicate them.

At the end of December 2020, one year after the NPRM launched, the FAA published an advance copy of the final RID rule. It officially published the rule on January 15, 2021, which created a new Part 89 in the Code of Federal Regulations, Remote Identification of Unmanned Aircraft. (Note - The final OOP rule came out on the same day. It tied Category 2 & 3 operations to RID. It generally enabled most night flights. (Click here for info on the OOP rule).

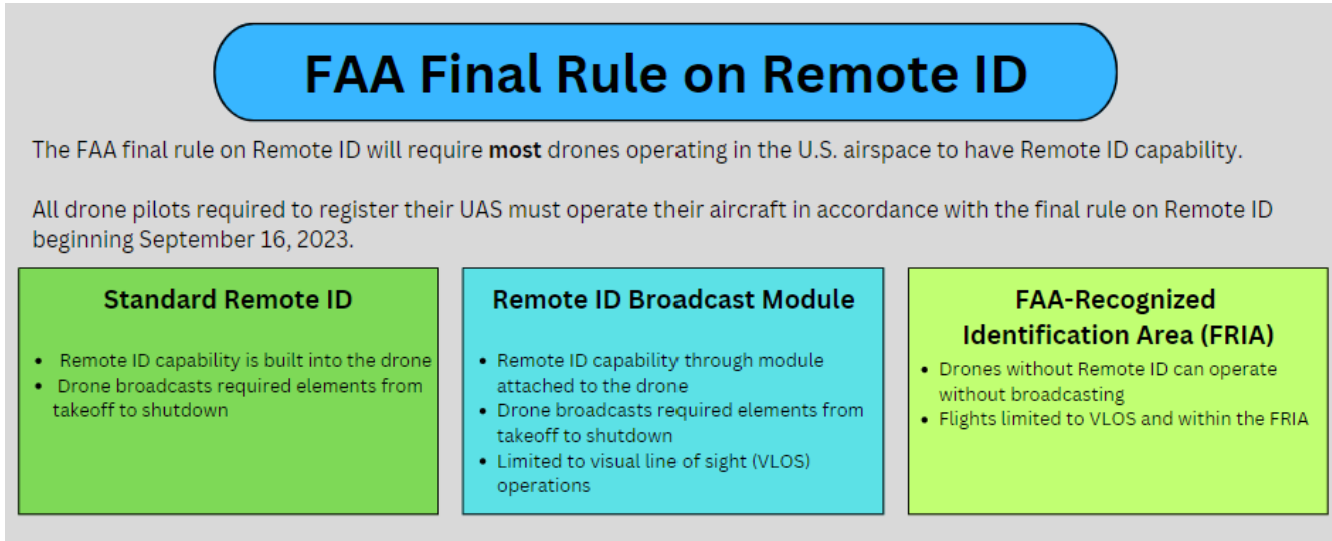
Then RaceDayQuads sued the FAA over the RID rule. The suit challenged both the rule's constitutionality and procedural regularity. The case dragged on for over a year, leaving the industry wondering about its fate. Ultimately, in July 2022, the court found in favor of the FAA. (Click here for a detailed analysis of the case and the court ruling).

RID Rule Requirements

The RID Rule states that any sUAS which must be registered (again, those weighing in at 0.55 - 55 pounds), and all commercial drones flown under Part 107 must also have RID broadcast capabilities to legally fly in the NAS. The broadcast must include specific Message Elements (MEs) which will beam out to the public, law enforcement agencies (LEAs) and security agencies.

The FAA says there are three ways to comply with RID, but really there are two. Either an operator uses a Standard RID UAS with baked-in RID broadcast capabilities or attaches a Broadcast RID Module to the drone. Otherwise, the drone must either fly in specially approved non-RID areas called Federally Recognized Identification Areas (FRIA) or stay on the ground.

The MEs that RID broadcasts must include: a unique identifier to establish the UAS identity (its serial number or a session ID); latitude, longitude, geometric altitude, and velocity; control station latitude, longitude and geometric altitude (for Standard RID only); time mark and emergency status indication (for Standard RID only). Broadcast Modules will need to broadcast the drone's takeoff location (not control station). They will not indicate an emergency status. Session ID is not an option for Broadcast Modules.



The broadcast MEs will be available to the general public. LEAs and security agencies will additionally be able to correlate them with information in the FAA's UAS registration database.

As with any rule, exceptions exist for RID too. RID does not apply to: drones flying indoors; U.S. armed forces' drones (*they don't need to be registered, so that makes sense); drones that weigh 0.55 pounds or less on takeoff and are flown exclusively under the Exception for Recreational Flyers (again, this links back to registration requirements); certain aeronautical research and test drones (with an FAA deviation); drones that the FAA administrator otherwise waves off (technically with an exception or deviation under 14 CFR § 89.10. This can include Part 91 drones that have specific permission to transmit ADS-B Out).

The RID Rule also contains related requirements for UAS manufacturers and designers. The original compliance deadline for manufacturers was September 2022. However, given the close-to-the-wire RDQ v. FAA ruling, the FAA published a notice that it would gracefully apply its discretionary enforcement authority through December. As mentioned earlier, drone operations must comply by this September.

Current Status

Today, all drone manufacturers are supposed to be RID compliant. FAA Advisory Circular (AC) 89-2 outlines the process for FAA approval of a manufacturer's Standard RID drone or RID Broadcast Module.

It begins with the manufacturer's submission of a declaration of compliance (DOC) to the FAA attesting that all production requirements of the final rule have been met because they followed an FAA-accepted means of compliance (MOC). Anyone can submit a RID MOC. FAA AC 89-1 explains the RID MOC process. This same process applies to the OOP rule.

The FAA maintains a dynamic and growing list of RID-compliant drones and Broadcast Modules here: https://uasdoc.faa.gov/listDocs. So far, the site lists over 70 drone models and modules. The majority of entries are for drones. The FAA has only approved a few Broadcast Modules so far.

When the September compliance date for drone operators hits, either the drone operator should fly either a Standard RID drone or one outfitted with a Broadcast Module. It should work from takeoff to touchdown. If RID stops working during flight, the remote pilot must land the drone as soon as it is safe and practicable to do so.

If the drone operator does not have RID capability, then he or she should only fly outdoors in a FRIA. The FAA will publish the locations of approved FRIAs on the FAA's UAS Data Delivery Service (UDDS) website: https://udds-faa.opendata.arcgis.com/

Implementation

From an airspace awareness and protection standpoint, in its most simplistic form, a RID broadcast indicates that a cooperative drone with RID capability is broadcasting data within range of a RID-enabled sensor or receiver. That's about it.

However, a RID-compliant flight does not equate to a "legal flight." A drone broadcasting RID could be flying in a Prohibited Area, flown from a moving aircraft, or by someone who is under the influence of drugs or alcohol, all of which are illegal under FAA regulations.

RID compliance also does not rule out potential nefarious intent or purpose. While unlikely, a drone broadcasting RID MEs could still be conducting criminal or otherwise illicit activity (*we say "unlikely," because it's more likely bad actors will choose not to use RID at all). Alternatively, a drone broadcasting RID MEs could purposefully send spoofed GPS information or other data to mislead security or law enforcement.

Receiving Remote ID Message Elements from a Drone Tells Us:
• That a drone with Remote ID capability is broadcasting Remote ID message elements within range of a Remote-ID enabled sensor or receiver.
Receiving Remote ID Message Elements from a Drone Does Not Tell Us:
• Whether a flight is a "legal flight" or an "illegal flight," aka is or is not in accordance with all aspects of the Remote ID rule or other FAA drone rules and regulations. • Whether the operator has nefarious intent (threat vs non-threat). • That the RID message element data is accurate; RID message elements could be spoofed or designed to purposefully mislead law enforcement and security personnel.

On the other hand, when a drone (not located in a FRIA) is flying in the immediate airspace, and a RID-enabled sensor or receiver is not receiving RID MEs, a law enforcement or security professional could logically assume that the operator is non-compliant or might even be a "bad guy." But the lack of receiving a RID broadcast could also mean several other things. The drone may not be required to broadcast RID MEs because it weighs less than .55lbs/250g and is being flown for recreational purposes. The drone could be broadcasting RID MEs that, for whatever reason, a nearby sensor failed to detect. In the case of a RID Broadcast Module with limited range, perhaps the drone is out of range of the RID sensor. The area could lack the density of RID receivers/sensors needed to receive the broadcast. Maybe RF interference, terrain, buildings, vegetation, or other obstructions inhibited the RID broadcast.

What Failure to Receive Remote ID Message Elements from a Drone Tells Us:

- That a Remote-ID enabled sensor is not receiving Remote ID message elements from a nearby drone.

What Failure to Receive Remote ID Message Elements from a Drone Could Mean:

- That the drone is not required to broadcast Remote ID message elements (drone weighs less than .55 lbs/250g and is flown for recreational purposes only, or other authorized exemptions from the FAA).
- The drone is required to broadcast Remote ID message elements and is not compliant with the Remote ID rule.
- The Remote ID broadcast module hardware and/or software have been tampered with.
- That there may be radio frequency interference, terrain, buildings, vegetation, or other obstructions inhibiting the Remote ID broadcast from the drone and/or the reception of the signal by a nearby Remote ID sensor or receiver.
- There is a technical issue with the Remote ID broadcast module and/or the Remote ID sensor or receiver.
- The drone is out of range of a Remote ID sensor or receiver; or the area lacks the density of Remote ID sensors to be able
- to receive the Remote ID message elements.

What Failure to Receive Remote ID Message Elements from a Drone Does Not Tell Us:

- Whether the operator has nefarious intent (threat vs non-threat).
- Whether or not a nearby drone is or is not broadcasting Remote ID message elements.

For all of these reasons, security professionals should first, know the rules applicable to drones and second, view RID as merely one piece of data in a much broader information context.

RID should not be used as a stand-alone drone detection system. However, it should be a component of a robust layered defense strategy for airspace awareness and protection. Because of the technical limitations of RID and other issues highlighted in this paper, RID can not be a replacement for traditional drone detection technologies that include EO/IR cameras, radars, RF detection systems, and acoustic sensors. The technical limitations and challenges of RID highlight the need for lawmakers to update legislation to allow law enforcement and other security entities to be able to use the full range of drone detection equipment, including RF detection systems that would currently violate federal criminal statutes, to secure mass gatherings, critical infrastructure, and other important assets.

Knowing the Rules

The FAA, and other drone-focused, public safety and security-focused organizations, provide a wealth of resources for security professionals to understand the rules applicable to drones.

The FAA has published a Public Safety Toolkit to help law enforcement and public safety professionals understand safe drone operations and their authority. Its Law Enforcement Assistance Program (LEAP) consists of field investigative and operational activities to support federal, state, and local agencies by denying anyone who would threaten national security access to the NAS. Run by FAA headquarters Office of National Security Programs and Incident Response and special agents assigned to the LEAP Division, this team takes regulatory enforcement actions, provides aviation-related support to LEAs seeking criminal prosecution or conducting airborne drug interdiction and provides training to law enforcement officers in aviation smuggling techniques and FAA resources.

Notable among nonprofits that support public safety, DRONERESPONDERS, created to unite aerial first responders, emergency managers, and search and rescue specialists under a unified organization to help learn, train, and test with one another, has a vast resource center for its members. Membership is free.

Security professionals should consider taking a Part 107 course and the associated practice tests, if not the actual remote pilot certification test. Even if a security expert never plans to fly a drone, the knowledge about drone regulations and airspace gained from this experience is incomparable. Many different organizations and companies provide valuable Part 107 certification training.

The Drone Assessment and Response Tactics (DART) course, hosted by the New Mexico Tech Energetic Materials Research and Testing Center, is a Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA) funded course that offers a residential delivery option in Playas, New Mexico, or a one-day mobile delivery option locally anywhere in the U.S. or its territories. DART helps front-line first responders and emergency management personnel recognize and assess an unmanned aircraft for a potential threat and develops basic awareness of how to assess a suspicious situation and mitigate unsafe UAS operations.

The C-UAS Hub also provides a central source for counter-unmanned aircraft systems technology, information, news and resources. Its content consists of publicly available, open-source information, as well as original content generated by C-UAS Hub and its partners, and includes: information on counter-UAS-related products and services, news, articles and thought leadership on topics related to or important to the UAS and counter-UAS communities, a reference library of publicly available documents, employment opportunities as well as counter-UAS, UAS, defense, and security-related events such as trade shows, conferences, industry days, etc. The site will soon add webinars and podcasts, plus training and educational opportunities.

If you are new to Counter-UAS (sometimes referred to as Counter-Drone, Counter-UAV, Counter-sUAS, and Anti-Drone to name a few), take a look at C-UAS Hub's "New to Counter-UAS?" page with some selected articles and references to get you started. A recently published article- What is Counter-UAS? will provide you with a common framework that is important to understanding this emerging area of expertise and align expectations for its implementation. Many FAA-related law enforcement and drone response reference documents can be found on the website at- FAA UAS Law Enforcement Reference Documents.

Besides a baseline understanding of the rules applicable to drones, security professionals must have an appreciation of the limits of their authority as well. RID will likely be incorporated as part of counter-UAS technology, to provide additional data to authorized C-UAS system operators. But today, only a handful of federal law enforcement agencies, including the Department of Defense, Department of Homeland Security, the Department of Justice and the Department of Energy remain authorized to employ a full range of detection and mitigation equipment that would otherwise violate federal laws and regulations.

In 2020, several federal agencies jointly issued an Advisory on Use of Technology to Detect and Mitigate Unmanned Aircraft Systems that still applies today. It identifies the specific agencies authorized to employ C-UAS tech and all of the laws that a non-authorized agency could trip over by doing so with that explicit authority.

Practical Tips & Recommendations

When conducting airspace awareness and protection operations, RID data is a key element to consider. However, it is essential to understand what the data is and is not telling you. Foremost, RID does not tell you whether a drone is or is not a threat. Due to the many reasons that might inhibit a sensor/receiver from receiving RID MEs from a drone, it may be more prudent to say, “We are not receiving Remote ID message elements from the drone,” instead of, “The drone is not broadcasting Remote ID message elements.”

Putting the data into the proper context will help law enforcement and other security professionals to react, when appropriate, to the credible threat of drones in the airspace.

Understanding the airborne “rules of the road” will prevent unnecessary interactions with otherwise law-abiding drone pilots using drones for recreational or commercial purposes within the established FAA rules. Using RID as a tool to locate and harass law-abiding drone pilots could lead to decreased compliance with the RID rule in the drone community, making the NAS less safe.

Knowing the rules will also provide law enforcement and security professionals with the opportunity to positively interact with and educate otherwise clueless drone pilots of the FAA

rules or, when necessary and authorized, take further law enforcement action based on federal, state or local drone laws.

In closing, RID is merely one part of a bigger and holistic airspace picture for UAS integration into the NAS. Whether a law enforcement or security professional receives or does not receive, RID message elements from a nearby drone provides only one datapoint to be considered as part of the overall airspace awareness and protection mission. In a post-RID world, security professionals will still need to assess any drone flight based on their knowledge of the rules, their training, and additional data gleaned from other drone detection capabilities (e.g., radar, RF, acoustic, camera).

Contact Us

If you have any other questions about Remote Identification or any other airspace protection and awareness issue, feel free to contact us.

Email: tom@aerovigilance.com

Thank you!