United States Government Accountability Office

Report to Congressional Requesters

June 2024

DRONES

Actions Needed to Better Support Remote Identification in the National Airspace

GAO-24-106158

June 2024

DRONES

Actions Needed to Better Support Remote Identification in the National Airspace

GAO Highlights

Highlights of GAO-24-106158, a report to congressional requesters

Why GAO Did This Study

Drones are the fastest-growing segment of aviation in the U.S., according to FAA. Remote ID is intended to help FAA, law enforcement, and others locate drone operators flying in an unsafe manner or where prohibited. FAA is responsible for safely integrating drones into the national airspace and notes that Remote ID could help enable advanced drone operations.

GAO was asked to review issues related to Remote ID. This report assesses (1) potential law enforcement uses for Remote ID, and related federal support, and (2) any limitations FAA and stakeholders may face using Remote ID for advanced operations.

GAO reviewed FAA guidance and resources for Remote ID. GAO also reviewed FAA's plans for integrating drones into the national airspace. GAO interviewed FAA and DHS officials, and law enforcement and industry stakeholders that GAO identified based on their participation on FAA committees and input from other stakeholders. GAO also reviewed DHS efforts to develop a Remote ID application.

What GAO Recommends

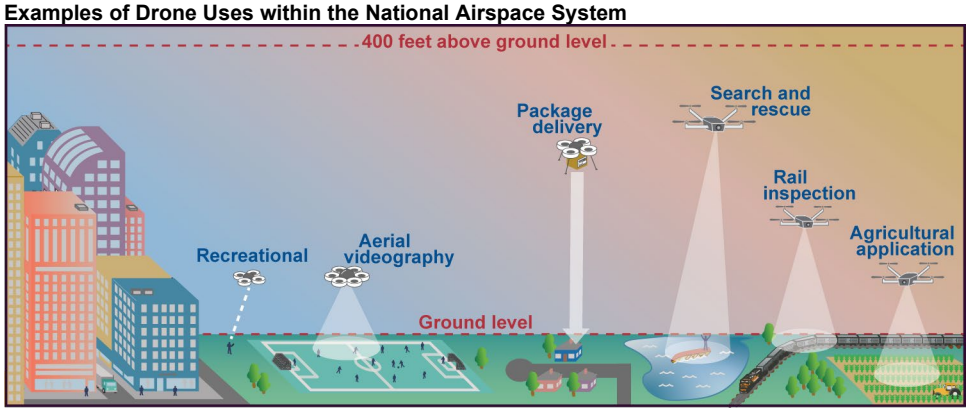
GAO is making three recommendations to FAA and one to DHS, including that FAA develop resources to help tribal, state, and local law enforcement use Remote ID; FAA develop a plan and timeline for a Remote ID interface; FAA identify a path forward for providing real-time, networked data about the location and status of drones; and DHS develop a plan and timeline for its Remote ID application. FAA and DHS concurred with our recommendations.

View GAO-24-106158. For more information, contact Heather Krause at (202) 512-2834 or krauseh@gao.gov.

What GAO Found

The Federal Aviation Administration (FAA) generally requires drones to be equipped with Remote ID technology, which FAA describes as a "digital license plate." Law enforcement can use Remote ID to identify and investigate unauthorized drone activity, in line with FAA's goal for Remote ID to help law enforcement. However, GAO found that FAA has limited resources to support tribal, state, and local law enforcement on using the technology. Tribal, state, and local law enforcement agencies GAO contacted had little knowledge of Remote ID or how it could be used in their investigations. Developing such resources could help FAA better support law enforcement's ability to use Remote ID. Further, FAA is developing an interface to provide drone registration information from Remote ID to law enforcement but does not have a plan or timeline for releasing it. At the same time, the Department of Homeland Security (DHS) is developing an application for law enforcement that would link to FAA's interface, but DHS similarly does not have a plan or timeline for the effort. As a result, law enforcement may continue to experience delays with accessing real-time information needed to track and investigate unauthorized drone activity.

Examples of Drone Uses within the National Airspace System



Source: GAO illustration of National Aeronautics and Space Administration information. | GAO-24-106158

FAA officials and stakeholders identified limitations with using current Remote ID technology to enable advanced drone operations, such as traffic management. FAA regulations call for drones to use broadcast-based Remote ID technologies, such as Wi-Fi and Bluetooth to transmit their location. However, commercial drone stakeholders told GAO that a broadcast-based signal is not sufficient for providing real-time, networked data about drone location and status as needed for advanced operations. FAA has stated it expects industry will pursue network technologies for Remote ID, such as cellular, while continuing to transmit the required broadcast-based Remote ID signal. However, stakeholders representing a commercial drone group said that there is a general lack of willingness by industry to develop network-based Remote ID alongside the required broadcast-based approach due to practical limitations, such as signal interference. FAA officials said that in the future, FAA may begin assessing what additional technology can be developed. FAA's progress toward integrating drones into the national airspace may be at risk if the agency does not assess these issues and identify a path forward.

Contents

Letter		1
	Background	5
	Law Enforcement Can Use Remote ID to Track Drones but Federal Efforts Do Not Fully Support Its Use	10
	FAA and Stakeholders Face Limitations with Using Remote ID to Enable Advanced Operations, and FAA Has Not Identified a Path Forward	17
	Conclusions	20
	Recommendations for Executive Action	21
	Agency Comments	21
Appendix I	Stakeholders Interviewed	23
Appendix II	Comments from the Department of Transportation	25
Appendix III	Comments from the Department of Homeland Security	26
Appendix IV	GAO Contact and Staff Acknowledgments	28
Table		
	Table 1: List of Stakeholders Interviewed	23
Figures		
	Figure 1: Examples of Drone Uses within the National Airspace System	6
	Figure 2: Broadcast-Based Remote ID Methods for Compliance	8
	Figure 3: Depiction of How Law Enforcement Application Would Access FAA's Interface for Drone Owner Registration Information	16

Abbreviations

app	application
ARC	Aviation Rulemaking Committee
DHS	Department of Homeland Security
DOJ	Department of Justice
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
ID	identification
interface	application program interface
LEAP	Law Enforcement Assistance Program
SORN	System of Records Notice
UAS	unmanned aircraft systems

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

June 6, 2024

The Honorable Sam Graves
Chairman
Committee on Transportation and Infrastructure
House of Representatives

The Honorable Garret Graves
Chairman
Subcommittee on Aviation
Committee on Transportation and Infrastructure
House of Representatives

Unmanned aircraft systems (UAS), commonly referred to as "drones," have emerged as the fastest-growing segment of aviation in the U.S., according to the Federal Aviation Administration (FAA).[1] The emergence of drones has the potential to provide significant social and economic benefits. In 2023, FAA forecasted that based on registration data, the commercial drone fleet (those operating in connection with a business) would grow from around 727,000 at the end of 2022 to 955,000 by 2027. For the same period, FAA forecasted the recreational fleet (those operated for personal interest and enjoyment) would increase from 1.69 million to 1.82 million.[2] FAA is tasked with safely integrating drones into the national airspace system—a complex network of airports, aircraft, air traffic control facilities, employees, and pilots—by developing various policies, regulations, and standards.

According to FAA officials, one of the biggest challenges faced by law enforcement when responding to drone incidents is locating the operator of a drone. In January 2021, FAA issued a final rule generally requiring drones be equipped with Remote ID technology, which provides identification and location information to other parties that can receive the

[1]For the purposes of this report, we use the term "drone" to refer to small, unmanned aircraft, which are defined as weighing less than 55 pounds at takeoff, including everything that is on board or otherwise attached to the aircraft. 14 C.F.R. § 107.3. Small UAS consist of the aircraft and its associated elements—including the control station and the associated communication links—that are required for safe and efficient operation in the national airspace system. *Id*.

[2]Federal Aviation Administration, *FAA Aerospace Forecast Fiscal Years 2023-2043* (Washington D.C.: May 2023).

signal.[3] According to FAA, Remote ID is intended, in part, to help FAA, law enforcement, and other federal agencies find the operator of a drone appearing to be flying in an unsafe manner or where prohibited. In addition, FAA noted that information on the location, status, and flight paths of drones in real-time could be useful for enabling advanced operations, such as beyond visual line-of-sight operations and complex traffic management services.[4]

You asked us to review progress on using Remote ID technology for public safety and advanced drone operations. Our report assesses: (1) potential law enforcement uses for Remote ID technology, and related federal support for these uses; and (2) any limitations FAA and stakeholders may face using Remote ID to enable advanced operations.

To address both objectives, we reviewed relevant policies, plans, and guidance documents describing FAA's approach to developing and implementing Remote ID, as well as relevant statutes and regulations related to registering and operating drones. These documents include FAA's UAS ID and Tracking Aviation Rulemaking Committee Final Report; Remote ID of Unmanned Aircraft rule; and Enforcement Policy Regarding Production Requirements for Standard Remote ID Unmanned Aircraft.[5] We also reviewed our prior reports and those from the Department of Transportation's Office of Inspector General on drone

[3]As FAA imposed these operating requirements on drones registered or required to be registered under 14 C.F.R. part 47 or 48, the rule applies more broadly than just to small, unmanned aircraft. *See* 14 C.F.R. § 89.101. For the purposes of this report, however, we focused on small, unmanned aircraft.

[4]According to FAA, many drone operations can be conducted under FAA's Small UAS Rule (14 C.F.R. Part 107), or under 49 U.S.C. § 44809 as a recreational flight within the guidelines of a modeler community-based organization. However, more complex operations (advanced operations) may need additional certification or approval.

[5]Federal Aviation Administration, *UAS Identification and Tracking Aviation Rulemaking Committee (ARC), ARC Recommendations, Final Report* (Sept. 30, 2017). Remote Identification of Unmanned Aircraft, 86 Fed Reg. 4390 (Jan. 15, 2021) (codified at 14 C.F.R. Part 89). Enforcement Policy Regarding Production Requirements for Standard Remote Identification Unmanned Aircraft, 87 Fed. Reg. 55685 (Sept. 12, 2022).

integration, traffic management, detection and mitigation, safety, and enforcement.[6]

In addition, we interviewed officials from FAA and other federal entities including the Department of Homeland Security (DHS), Department of Justice (DOJ), Federal Communications Commission, and National Telecommunications and Information Administration. We also interviewed representatives from a nongeneralizable sample of 23 law enforcement and drone stakeholder groups about their roles and responsibilities related to Remote ID, the implementation of Remote ID, and any limitations they face related to Remote ID. We selected these representatives based on their participation in FAA's aviation rulemaking committees, such as the UAS Identification and Tracking rulemaking committee and the UAS Beyond Visual Line-of-Sight rulemaking committee, their participation in FAA's Advanced Aviation Advisory committee, and recommendations from other drone stakeholders. More information about stakeholder selection and a list of stakeholders we interviewed are included in appendix I.

To determine potential law enforcement uses for Remote ID technology and related federal support, we reviewed FAA's internal guidance and external resources provided to law enforcement, including *FAA's Drone Response Playbook for Public Safety* and *Supplement to the Drone Response Playbook for Public Safety*.[7] We also reviewed FAA-developed video resources for law enforcement, including a three-part video series and webinar on responding to unsafe drone operations. We assessed FAA's efforts to provide resources to law enforcement on using Remote ID against the *FAA Law Enforcement Assistance Program Handbook*.[8] Additionally, we interviewed DHS and DOJ officials to understand how

[6]We reviewed our prior reports on drones from 2018 to 2024. We also reviewed the following U.S. Department of Transportation, Office of Inspector General reports: Department of Transportation, Office of Inspector General, *FAA Has Made Progress on a UAS Traffic Management Framework, but Key Challenges Remain*, AV20220041 (Washington, D.C.: Sept. 28, 2022); *FAA Made Progress Through Its UAS Integration Pilot Program, but FAA and Industry Challenges Remain To Achieve Full UAS Integration*, AV20220027 (Washington, D.C.: Apr. 27, 2022); and *While FAA Is Coordinating With Other Agencies on Counter-UAS, Delays in Testing Detection and Mitigation Systems Could Impact Aviation Safety.* AV20220026 (Washington, D.C.: Mar. 30, 2022).

[7]Federal Aviation Administration, *Drone Response Playbook for Public Safety* (Sept. 2020); and *Supplement to the Drone Response Playbook for Public Safety*.

[8]U.S. Department of Transportation Order SH1600.83A*, Law Enforcement Assistance Program Handbook* (Washington D.C.: Jan. 26, 2018). This handbook is not publicly available due to its sensitive nature.

federal law enforcement may use Remote ID and how FAA supports these uses. We also compared FAA's efforts to develop a Remote ID interface for law enforcement to FAA's Security and Hazardous Materials Safety Fiscal Year 2023 Business Plan.[9] We also assessed DHS efforts to develop an application (app) that law enforcement could use to access the interface. To perform this assessment, we considered prior GAO work on interagency collaboration and the goals for Remote ID outlined in the final rule.

To identify any limitations FAA and stakeholders face using Remote ID to enable advanced operations, we reviewed FAA's *Unmanned Aircraft Systems Traffic Management Implementation Plan; Integration of Civil UAS in the National Airspace System Roadmap, Third Edition; UAS Integration Pilot Program*; and FAA office business plans.[10] We interviewed selected industry representatives to obtain their views on limitations stakeholders face using Remote ID to enable advanced operations. Our discussions with a commercial drone organization provided an industry-wide perspective on these issues for commercial drone users. As part of our assessment of the limitations identified by stakeholders and FAA, we determined the extent to which FAA was taking action to address them and assessed its efforts against *Standards for Internal Control in the Federal Government* related to identifying and managing risk.[11]

We conducted this performance audit from July 2022 to June 2024, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that

[9]Individual FAA offices and staff offices (such as FAA's Security and Hazardous Materials Safety Office) develop annual fiscal year business plans that describe activities each office will undertake in support of all FAA initiatives, including FAA drone integration efforts. Federal Aviation Administration, *Aviation Safety Fiscal Year 2023 Business Plan* (Washington D.C.: Mar. 6, 2023).

[10]Federal Aviation Administration, *Unmanned Aircraft Systems Traffic Management Implementation Plan* (July 31, 2023); *Integration of Civil Unmanned Aircraft Systems in the National Airspace System Roadmap, Third Edition* (2020); and *Unmanned Aircraft Systems Integration Pilot Program* (Dec. 17, 2021).

[11]GAO, *Standards for Internal Control in the Federal Government,* GAO-14-704G, (Washington, D.C.: Sept. 2014).

the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

FAA Drone Registration and Operations

FAA generally mandates that individuals register all drones.[12] This registration process involves providing essential information about the drone and its owner, along with receiving a unique registration number. FAA manages the drone registration database, which includes information about drone owners. FAA does not make registration information about drone owners from the database generally available to the public.[13] This aims to protect the privacy and security of individuals who have registered their drones with FAA.

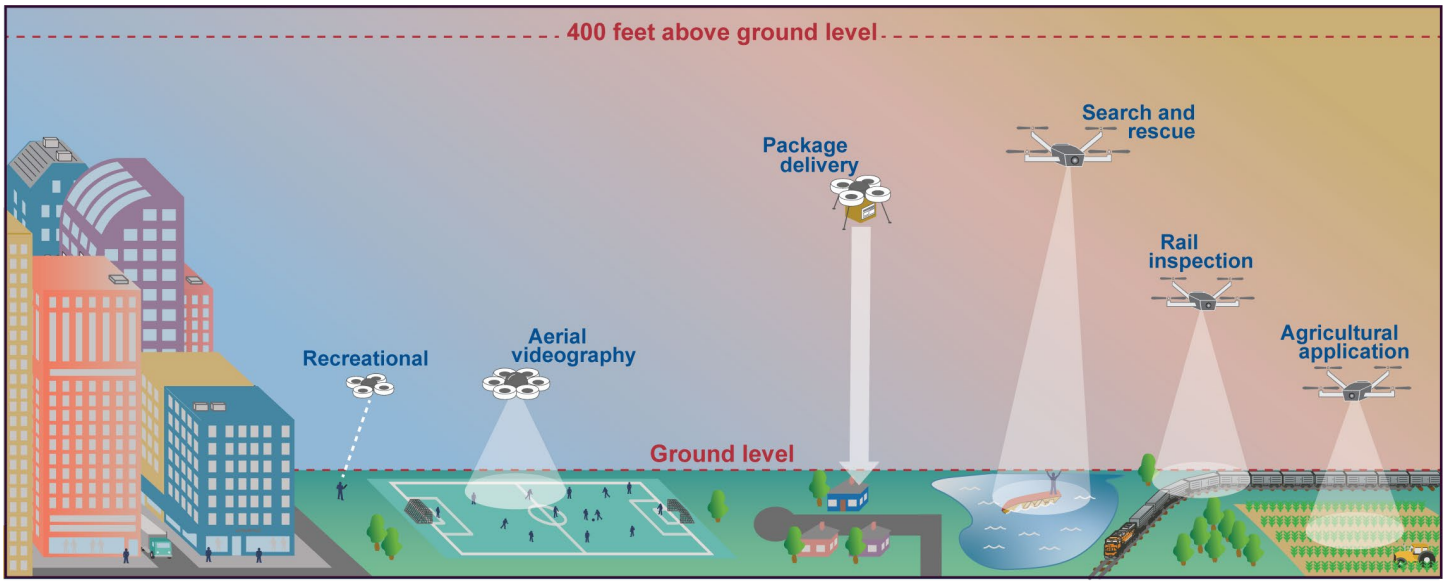
Additionally, FAA imposes an altitude restriction for drones, generally prohibiting them from flying more than 400 feet above ground level. These regulations, among others, are designed to promote safe and responsible drone operations, ensuring that drones do not pose a threat to other aircraft and the national airspace system. Figure 1 shows examples of drone uses within the national airspace system. FAA also has efforts underway aimed at expanding drone operations.[14]

[12]The registration requirement includes exceptions, such as for drones weighing 0.55 pounds or less and operated exclusively in compliance with rules for limited recreational operations in 49 U.S.C. § 44809. *See* 14 C.F.R. § 48.15.

[13]The Privacy Act of 1974, as amended, places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records, which are defined as groups of records under the control of any agency from which information is retrieved by the name of the individual or by an individual identifier. 5 U.S.C. § 552a.

[14]For example, in 2021, FAA established a beyond visual line-of-sight ARC to develop recommendations for a rule that would enable operations beyond the visual line-of-sight of a drone operator. The final report, issued in March 2022, included several recommendations to FAA for developing a final rule. In addition, in September 2020, FAA published a policy stating that it would begin accepting applications for type certification of some drones. FAA has already awarded type certifications for some drones conducting commercial delivery operations in the U.S. Type certification approves the design of the aircraft and all component parts (propellers, engines, control stations, etc.).

Figure 1: Examples of Drone Uses within the National Airspace System



Source: GAO illustration of National Aeronautics and Space Administration information. | GAO-24-106158

Remote ID Rule

According to FAA, in its basic form, Remote ID is an electronic identification or a "digital license plate" for drones. Remote ID transmits certain identification, location, and performance information from a drone to people on the ground and other airspace users. According to FAA, Remote ID will serve as a fundamental tool for enhancing public safety and plays a pivotal role in safely integrating drones into the national airspace system, providing essential information about drones operating in the airspace.

To establish requirements for Remote ID, FAA published a Notice of Proposed Rulemaking on Remote ID for drones on December 31, 2019.[15] The Notice of Proposed Rulemaking initially proposed requirements for both broadcast (e.g., Wi-Fi or Bluetooth) and network (e.g., cellular) Remote ID, seeking to strike a balance between the interests of all

[15]Remote Identification of Unmanned Aircraft Systems, 84 Fed. Reg. 72438 (proposed Dec. 31, 2019).

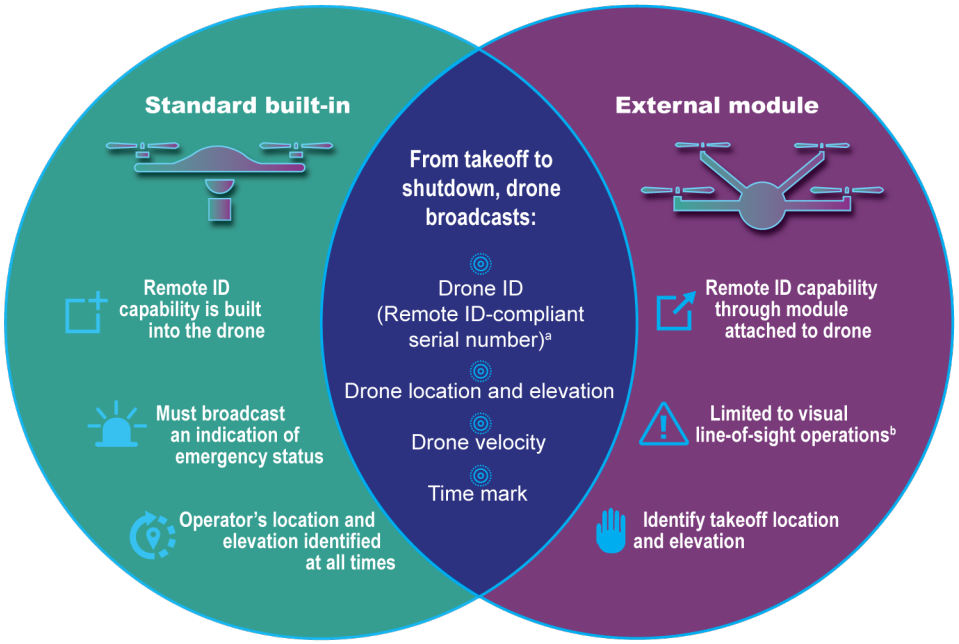
relevant stakeholders.[16] Remote ID using broadcast data transmits radio signals, such as Wi-Fi and Bluetooth, directly from the drone to receivers, such as phones or other devices, in the drone's vicinity. Network-based Remote ID technology, if developed, would rely on drones transmitting information using, for example, cellular networks, to a Remote ID service provider. This method of transmission would make the information available via the internet. However, when FAA published the final rule on January 15, 2021, the agency acknowledged that it had not anticipated many of the difficulties presented by the proposed network requirements. As such, FAA opted for a simplified approach by adopting only the broadcast requirements in the rule.

To comply with the Remote ID rule, drone operators must adhere to one of three options: (1) flying a drone equipped with standard built-in Remote ID capabilities, (2) adding an external broadcast module to a drone for Remote ID transmission, or (3) operating within designated FAA-Recognized Identification Areas for drones without the appropriate broadcast-based technologies.[17] See figure 2 for more information on the two methods using broadcast-based technologies.

[16]Broadcast-based Remote ID technology could use Wi-Fi or Bluetooth to transmit Remote ID information continuously within a limited range of a drone's current location. This allows people on the ground to receive this information, should they be within the range of the radio frequency's transmission. Network-based Remote ID uses a data connection to transmit Remote ID information (typically via cellular network) to a Remote ID network, which collects and disseminates Remote ID information through the internet. This means that anyone with an internet connection can potentially access the Remote ID information.

[17]FAA-Recognized Identification Areas designate specific physical locations, which typically include landscaped grassy areas, paved areas, gravel, forest edges, recreational parks, and agricultural areas, where drones can operate without Remote ID, albeit within prescribed limitations, including that the operator must be in the same area. Only FAA-recognized community-based organizations and educational institutions such as primary and secondary schools, trade schools, colleges, and universities are eligible to request the establishment of a FAA-Recognized Identification Area.

Figure 2: Broadcast-Based Remote ID Methods for Compliance



Source: GAO icons and analysis of broadcast-based methods for meeting Federal Aviation Administration's (FAA) Remote ID compliance standards. | GAO-24-106158

Note: FAA can designate specific physical locations where drones can operate without Remote ID albeit within prescribed limitations, including that the operator must be in the same area. These locations—referred to as FAA-Recognized Identification Areas—typically include landscaped grassy areas, paved areas, gravel, forest edges, recreational parks, and agricultural areas. Only FAA-recognized community-based organizations and educational institutions such as primary and secondary schools, trade schools, colleges, and universities can request that FAA designate a FAA-Recognized Identification Area.

[a]In the future, operators of standard Remote ID drones may be able to choose between broadcasting the drone's serial number ID or a session ID.

[b]The person manipulating the drone's flight controls must be able to see the drone throughout the flight. Currently, whether the drone has standard Remote ID or an external module, 14 C.F.R. § 107.31 imposes a separate requirement that the remote pilot in command and person manipulating the flight controls maintain sight of the drone with vision that is unaided by any device other than corrective lenses. The requirement under 14 C.F.R. § 107.31 may also be satisfied by having a designated visual observer.

To implement the Remote ID rule, FAA established compliance dates for both drone manufacturers and operators. FAA generally required that manufacturers of drones meant for operation in U.S. airspace produce and equip such drones with standard Remote ID by September 16, 2022, ensuring that newly manufactured drones complied with the Remote ID

requirements.[18] Subject to some exceptions, FAA required that drone operators comply with the Remote ID rule by September 16, 2023.[19]

Entities with Roles in Responding to Drone Incidents

Federal, tribal, state, and local law enforcement all play a role in responding to drone incidents. State and local law enforcement are often the first to respond to, or receive a report of, a drone incident. Law enforcement can ask for proof of drone registration or ask to see an authorization or waiver if the operator is flying in a restricted airspace such as a no-fly zone. In addition, state and local law enforcement can enforce state and local laws addressing issues such as land use, harassment, privacy, or reckless endangerment.[20]

At the federal level, FAA has Law Enforcement Assistance Program (LEAP) agents, who are responsible for assisting federal, tribal, state, and local law enforcement agencies on a variety of aviation-related public safety issues, including responding to drone incidents. For example, LEAP agents have access to the drone registration database, which contains information about registered drone owners. The *FAA Law Enforcement Assistance Program Handbook*, an internal agency document, describes the authority, responsibilities, policies, guidelines, procedures, and objectives of LEAP. The policies and procedures described in the handbook also explain how FAA generally intends to exercise its statutory and regulatory enforcement responsibilities and provide investigative assistance and training to law enforcement agencies.

[18]FAA issued a notice announcing it would exercise its discretion in deciding whether to take enforcement action for noncompliance by manufacturers occurring on or before December 16, 2022. Enforcement Policy Regarding Production Requirements for Standard Remote Identification Unmanned Aircraft, 87 Fed. Reg. 55685 (Sept. 12, 2022).

[19]In September 2023, FAA issued a notice stating, "[T]he FAA acknowledges that for many operators, compliance with § 89.105 may prove difficult or impossible in the timeframe presented…Accordingly, the FAA will exercise its discretion in determining how to handle any apparent noncompliance, including exercising discretion to not take enforcement action, if appropriate, for any noncompliance that occurs on or before March 16, 2024—the six-month period following the compliance deadline for operators initially published in the Remote Identification of Unmanned Aircraft final rule, RIN 2120–AL31. The exercise of enforcement discretion herein creates no individual right of action and establishes no precedent for future determinations." Enforcement Policy Regarding Operator Compliance Deadline for Remote Identification of Unmanned Aircraft, 88 Fed. Reg. 63518, 63519 (Sept. 15, 2023).

[20]According to FAA, a state or local law will be preempted if it conflicts with FAA regulations. FAA asserts exclusive authority to regulate aviation safety and airspace efficiency regarding drone operations at any altitude.

Other federal law enforcement agencies may also work with tribal, state, and local law enforcement agencies in responding to or investigating a drone incident. For example, at a large sporting event, such as the Super Bowl, state and local law enforcement may engage with Federal Bureau of Investigation (FBI) agents, LEAP agents, and others regarding potential risks of drone flights over the event. Local law enforcement may also call on the FBI to investigate a suspicious drone or a drone carrying a payload.

Additionally, the Transportation Security Administration within DHS works with local officials and officials from FAA and other federal entities authorized to use counter-drone technologies in responding to drone incidents at airports. It also coordinates the federal response, including using counter-drone technology under certain conditions.[21] Further, other DHS components have a role in ensuring the public and the homeland are protected from the criminal misuse of drones and are involved in testing and designing requirements for counter-drone technologies. DHS officials said that Remote ID is a key piece of counter-drone technologies as it enables law enforcement to gain additional threat discrimination around critical infrastructure.

Law Enforcement Can Use Remote ID to Track Drones but Federal Efforts Do Not Fully Support Its Use

Remote ID Technology Can Be Used to Track and Investigate Unauthorized Drone Activity

According to FAA and stakeholders we interviewed, Remote ID could provide new information for law enforcement agencies to track and investigate unauthorized drone activity. According to the preamble accompanying the final rule in the Federal Register, FAA expects Remote ID to support safety and security in the national airspace system as

[21]For more information regarding drone detection and mitigation issues, see GAO, *Aviation Safety: Federal Efforts to Address Unauthorized Drone Flights Near Airports,* GAO-24-107195 (Washington, D.C.: March 2024) and GAO, *Science and Tech Spotlight: Counter-Drone Technologies,* GAO-22-105705 (Washington, D.C.: March 2022).

drones become more prevalent. Potential law enforcement uses of Remote ID are as follows.

- **Improving situational awareness of drone activity.** According to FAA, Remote ID could provide law enforcement agencies with information about drones operating in a specific area. This could improve their understanding of the drone activity and identify potential risks or threats more effectively. For instance, DOJ officials told us that Remote ID may allow FBI and others to distinguish registered drones with an associated operator from unregistered drones that may be operating with a criminal purpose.
- **Locating operators.** Drones using standard Remote ID with the required technology already incorporated into the drone by the manufacturer could help law enforcement identify the location of the drone's operator during flight. Drones using a dedicated broadcast module could allow law enforcement to identify where the drone took off.[22] This could help law enforcement identify operators unknowingly flying in unauthorized airspace and educate operators about where they are authorized to fly drones.
- **Enforcing laws.** Remote ID could help law enforcement agencies enforce existing drone laws more efficiently.[23] With the ability to identify and track unauthorized drones, authorities could then take appropriate measures against unauthorized takeoffs and landings, stalking or harassing with a drone, or other illegal activities related to drones as designated in federal, state, and local laws. For example, one large city law enforcement agency we spoke to said using Remote ID could help the agency enforce city drone laws limiting where a drone can take off from.[24] In addition, federal law

[22]The required information from a Remote ID broadcast module includes a unique identifier; an indication of the drone's latitude, longitude, and geometric altitude; an indication of the drone's takeoff location latitude, longitude, and geometric altitude; an indication of the drone's velocity; and a time mark.

[23]FAA has stated that it has exclusive authority to regulate aviation safety and airspace efficiency regarding drone operations at any altitude. According to FAA, a state or local law will be preempted if it conflicts with FAA regulations, but FAA advises that state and local laws are not likely to be preempted if such laws focus on other objectives such as addressing land use, harassment, privacy, or reckless endangerment.

[24]Section 10-126(c) of the New York City Administrative Code prohibits any aircraft from taking off or landing, except in an emergency, from any place within the city other than specifically designated areas. FAA has advised that laws regulating the location of drone takeoff and landing areas are not likely to be preempted because states have a valid interest in choosing where aircraft may operate on the ground.

enforcement could use Remote ID to enforce federal laws and regulations restricting drone use, such as at major sporting events.

FAA Has Limited Resources for Law Enforcement on Using Remote ID

In recent years, FAA has consistently developed and provided resources—such as videos and websites—to tribal, state, and local law enforcement on how these entities can use drones for their missions. However, these resources have not included information on using Remote ID technology to support such law enforcement efforts related to drones. FAA provides resources on its website on how tribal, state, and local law enforcement can start and operate their own drone programs as more law enforcement agencies are realizing the potential benefit of drones to enhance their missions. FAA also published a Drone Response Playbook and accompanying supplement for public safety, which includes resources to help respond to drone incidents. These resources include a discussion on law enforcement authority for investigating drone incidents, contact information for LEAP agents, and an example of a remote pilot certificate and drone operator registration card. According to FAA officials, the agency provides these resources to tribal, state, and local law enforcement through FAA's LEAP agents and by engaging with law enforcement at conferences.

FAA guidance states that law enforcement agencies are often in the best position to detect and investigate drone incidents, but FAA has not developed resources to support law enforcement's use of Remote ID in these efforts. FAA officials said they would determine what additional resources they could provide to law enforcement after September 2023—when drone operators are required to comply with the Remote ID rule. Instead, FAA officials said they have focused their Remote ID implementation efforts on drone manufacturer compliance with the Remote ID rule, which required manufacturer compliance starting September 2022.

Tribal, state, and local law enforcement agencies we contacted had little knowledge of Remote ID or how it could be used in their investigations and said they had not received resources from FAA on how they could use it. For example, one local law enforcement agency we contacted said it had not received resources from FAA regarding Remote ID. This agency said that Remote ID could help meet its public safety mission but did not know how to use it in practice. Federal law enforcement officials we contacted generally were knowledgeable of Remote ID and its potential benefits. For example, officials at DOJ and DHS said they were aware of how they could use Remote ID in investigations to track drone

operators at a major sporting event. These officials acknowledged that local law enforcement entities may have less awareness of the technology.

Additional resources for educating law enforcement on the use of Remote ID could better position FAA to support law enforcement's response to drones posing a threat. According to FAA's *Law Enforcement Assistance Program Handbook*, LEAP is responsible for engaging with federal, tribal, state, and local law enforcement agencies on aviation drug smuggling, potential terrorist activities, and other criminal activity detrimental to the national air space and national security including drone incidents. LEAP has a handbook that supports how these agencies are to respond to drone incidents, but FAA lacks resources on how to use Remote ID in those efforts. Developing additional Remote ID resources for tribal, state, and local law enforcement at this stage could also help FAA meet the objectives of its Remote ID rule. FAA has stated that Remote ID will permit FAA and law enforcement to conduct oversight of persons operating unauthorized drones and to determine what actions are necessary to mitigate safety or security risks.

Federal Efforts Do Not Fully Address Access to Remote ID Information for Law Enforcement

FAA officials said that the current information-sharing process in response to drone incidents relies on LEAP agents responding to law enforcement officials' requests on a case-by-case basis. Specifically, FAA officials said that law enforcement officials can request drone information from their LEAP agent using a detected Remote ID number. The LEAP agent would then determine whether the drone is registered and provide information about the owner.[25]

FAA officials said that the LEAP agent is the primary point of contact for law enforcement and that in practice, requests for drone owner registration information cannot be fulfilled in real time. As of January 2024, there were 25 LEAP agents nationwide with responsibilities that also include assisting with and coordinating investigations of drug interdictions or aviation smuggling, identified by federal, tribal, state, and local law enforcement officers. FAA officials said they are in the process

[25]Under the Privacy Act, as amended, agencies may disclose personal information from a system of records without an individual's written consent only in specific situations, such as if disclosing the information under a "routine use" compatible with the purpose for which it was collected. 5 U.S.C. § 552a(b). Agencies identify their routine uses in a Federal Register publication known as a System of Records Notice (SORN). FAA's SORN for aviation registration records includes a routine use to disclose information to other government agencies when necessary or relevant to an investigation of a violation or potential violation of law that the agency is charged with investigating or enforcing.

of providing drone registration database access to aviation safety inspectors and technicians (roughly 6,000 personnel) to help with inquiries. FAA officials said they had not yet provided additional guidance to these personnel on this new means of access, nor had they provided any information to law enforcement on this additional resource. Regardless, this effort would not provide drone owner registration information in real time.

Federal, state, and local law enforcement and agency officials we spoke with expressed concerns about the timeliness and accessibility of drone owner information through Remote ID. All seven law enforcement agencies that we spoke to said that relying on a LEAP agent for drone registration information would significantly delay a response and that this information would need to be available in real time to help an investigation. FAA officials told us that LEAP agents typically respond to requests from law enforcement within 48 hours. Law enforcement and state agency officials we spoke with identified access to real-time information as key to fully using Remote ID. For example, officials of one large metropolitan police department that we spoke to said they thought they would be able to directly access owner registration information once operators are required to comply with the Remote ID rule. However, in practice they do not have access to this information. Additionally, officials from a state transportation agency told us that to address a public safety incident involving drones, they would need to obtain operator information quickly, but do not have access to it in real time. DHS and DOJ officials also expressed concerns about accessing drone owner registration information in real time for investigations until an app connected to FAA's drone owner registration database is operational.

FAA and DHS are also working on technologies to better enable law enforcement access to FAA's drone owner registration information. During the course of our review, DHS officials told us that they began working on an app that could be used by other law enforcement agencies. However, they said this project is in its infancy and there are a number of unknowns such as the availability of sensors to pick up Remote ID signals. Concurrently, FAA informed us that it was developing an application program interface (interface) that would serve as the query system for the app under development by DHS, retrieving drone registration information for authorized law enforcement users.

FAA officials said that to prepare for developing and rolling out the interface, they had to update the policy allowing FAA to share drone registration information with law enforcement through a System of

Records Notice (SORN).[26] Previously, the SORN permitted FAA to share information with law enforcement entities when necessary and relevant to an FAA enforcement activity.[27] FAA updated the SORN, effective September 8, 2023, to additionally allow for sharing information with law enforcement when relevant to an investigation of a violation or potential violation of law.[28]

Once FAA updated the SORN, officials said they proceeded with developing the interface and planning for the interface to connect to the app DHS is developing. (See fig. 3.) As of January 2024, FAA officials said they had made significant progress on the interface. DHS and DOJ officials said they have interagency meetings with FAA officials regarding the interface's development. According to an FAA briefing document on the interface in November 2023, FAA's next steps were testing the capabilities of the interface and developing a memorandum of understanding with DHS and DOJ. In May 2024, FAA stated that its effort to develop the interface is underway.

[26]A SORN is a Federal Register publication that identifies and describes a system used by an agency to maintain personally identifiable information. Among other things, SORNs describe the agency's policies and practices for storing, retaining, and disposing of the information records and routine uses for disclosing such records.

[27]Under the Privacy Act, FAA may also disclose registration information to a government agency or instrumentality for a civil or criminal law enforcement activity "if the head of the agency or instrumentality has made a written request… specifying the particular portion desired and the law enforcement activity for which the record is sought." 5 U.S.C. § 552a(b)(7).

[28]Under the revised SORN, FAA may disclose "[t]o government agencies, whether Federal, State, Tribal, local or foreign, information necessary or relevant to an investigation of a violation or potential violation of law, whether civil, criminal, or regulatory, that the agency is charged with investigating or enforcing; as well as, to government agencies, whether Federal, State, or local responsible for threat detection in connection with critical infrastructure protection." Privacy Act of 1974; System of Records, 88 Fed. Reg. 53951, 53954 (Aug. 9, 2023).

Figure 3: Depiction of How Law Enforcement Application Would Access FAA's Interface for Drone Owner Registration Information

Source: GAO illustration and analysis; Federal Aviation Administration (FAA) information. (Phone screen) dhs.gov, (Computer browser) faadronezone-access.faa.gov, (Certificate image) FAA, (Computer rendering) Just Me. Creative/stock.adobe.com. | GAO-24-106158

However, FAA and DHS officials expressed uncertainty on when these efforts might lead to better access to drone operator information for law enforcement. The agencies do not have coordinated plans or timelines for completing their respective efforts. FAA officials said that the next phase for the interface is initial testing, but officials had yet to start the testing due to the lack of an app connecting to the interface. FAA officials also said they have no goals or documentation for what capabilities the interface needs to have to finish testing and have not received a list of law enforcement requirements for the interface from DHS. Further, DHS officials said they do not currently have any planning documents related to the app's development or how it will connect to FAA's interface and that their efforts are in the very early stages.

Without coordinated plans and timelines, federal efforts to better support law enforcement uses for Remote ID could be delayed. The preamble accompanying the Remote ID final rule states that FAA's primary goal in establishing the Remote ID requirements is to enable FAA, law enforcement, and other government officials to identify drones operating in U.S. airspace. FAA's Security and Hazardous Materials Safety Fiscal Year 2023 Business Plan also identifies the need to collaborate with security partners on drone integration, while preserving the safety, efficiency, and public access to the national airspace system.[29] Our previous work has found that developing a plan to communicate outcomes is an important part of maintaining accountability in interagency collaborations.[30]

Law enforcement officials at all levels told us that real-time access to drone operator registration information would help investigations and is a key aspect of Remote ID. FAA and DHS are working on pieces of this information sharing through their respective interface and app. Without a plan on the outcomes and timelines for these projects, law enforcement agencies may continue to experience delays with accessing the real-time information they need to respond to unauthorized drones and will not be able to fully use Remote ID.

FAA and Stakeholders Face Limitations with Using Remote ID to Enable Advanced Operations, and FAA Has Not Identified a Path Forward

In addition to Remote ID's role in public safety, FAA has also recognized Remote ID's potential role in broader drone integration by enabling advanced operations. FAA's Concept of Operations for UAS Traffic Management, issued in March 2020, identified various ways Remote ID will support traffic management. These include (1) identifying and tracking drones operating in the national airspace; (2) assisting with conflict resolution between drones and other aircraft, as well as between drones themselves; and (3) providing real-time data about the location and status of drones for other traffic management functions.

When it issued the Remote ID final rule, FAA stated that Remote ID would support its phased, incremental approach toward full drone integration and enabling advanced operations. In its 2023 UAS Traffic Management Implementation Plan, FAA acknowledged that industry

[29]Individual FAA offices and staff offices (such as FAA's Security and Hazardous Materials Safety Office) develop annual fiscal year business plans that describe activities each office will undertake in support of all FAA initiatives, including FAA drone integration efforts.

[30]GAO, *Managing for Results: Implementation Approaches Used to Enhance Collaboration in Interagency Groups*, GAO-14-220 (Washington, D.C.: Feb. 2014).

envisions network-based Remote ID—which is not part of the current Remote ID requirements—as a foundational piece for enabling more advanced operations.

However, FAA limited the final Remote ID rule to broadcast-based requirements due to a range of concerns, such as cybersecurity, identified during the public comment period of FAA's rulemaking. For example, network-based Remote ID technology, if developed, could rely on drones transmitting information using cellular networks to a Remote ID service provider. This method of transmission would make the information available via the internet and therefore could create cybersecurity vulnerabilities. Conversely, according to FAA officials, with broadcast-based Remote ID technology, a drone transmits information directly to receivers, such as phones and other devices, in the drone's vicinity, typically through Wi-Fi or Bluetooth.

In its Notice of Proposed Rulemaking, FAA had proposed requiring drones with Remote ID equipment to incorporate cybersecurity protections for the transmission and broadcast of data. However, some comments to the rule expressed concern that drones transmitting information via the internet (i.e., network-based Remote ID) would create cybersecurity vulnerabilities. In its final rule, FAA determined it would remove the internet connectivity requirement associated with network-based Remote ID and, as a result, eliminated the proposed cybersecurity requirements for Remote ID.

Multiple drone industry stakeholders we spoke with said there are limitations with using broadcast-based Remote ID technology to enable advanced operations. These limitations include the signal's limited range, such that others can only detect a drone when it passes nearby in flight, and its unreliability. In contrast, these stakeholders said that network-based Remote ID technology could provide information more robustly. While FAA decided not to require network-based Remote ID because of cybersecurity and other concerns, FAA has indicated it will rely on industry to continue developing network-based technologies that may allow for integrating advanced drone operations. For example, according to FAA's UAS Traffic Management Implementation Plan, "FAA is optimistic that industry will continue to voluntarily develop and adopt solutions that use network Remote ID to enable other UAS traffic management capabilities, in addition to adding broadcast Remote ID capabilities to meet the requirements of the new rule."

However, stakeholders representing a commercial drone group said that there is a general lack of willingness on the part of industry to develop network-based Remote ID alongside the required broadcast-based approach. These same stakeholders told us that requiring a broadcast-based approach to comply with the Remote ID rule while incorporating a network-based approach poses practical limitations. For example, they said that incorporating broadcast technology into the flight controls of a network-based drone could interfere with other operations of the drone. They also expressed concern about interference with Remote ID broadcast modules used in conjunction with network-based transmissions. For example, stakeholders emphasized the complexity involved in integrating signal transmission systems into drones, citing the need for significant engineering analysis and related resources. Moreover, these stakeholders pointed to the adverse effects of the additional weight from both broadcast-based and network-based technology on drone safety and performance. For instance, stakeholders told us that any increase in weight, such as the need for incorporating a broadcast-based system alongside a network-based system, could alter the performance of the drone and decrease the drone's payload capacity.

FAA has not determined whether Remote ID or some other means of providing networked data would help enable advanced operations. FAA and stakeholders said that real-time, networked data for traffic management functions are important to drone integration. However, some industry stakeholders said that FAA's path forward on this issue is unclear—such as related roles and responsibilities among federal agencies and industry stakeholders for progressing toward advanced drone operations. This has led to uncertainty across industry on how to identify real-time, networked data about the location and status of drones. FAA officials told us that at a future date, FAA may begin assessing short and long-term options for providing real-time data that could enable advanced operations, but there are currently no plans to do so. Further, as enacted in May 2024, the FAA Reauthorization Act of 2024 requires FAA to determine whether alternative means of compliance, such as network-based Remote ID, would satisfy the intent of the Remote ID final rule.[31]

By not acting on this within the scope of its roles and responsibilities, FAA's progress toward fully integrating drones into the airspace may be

[31]Pub. L. No. 118-63, § 907, 138 Stat. 1025. The act directs FAA to submit a report to Congress on the results of this evaluation by May 16, 2025.

at risk. *Standards for Internal Control in the Federal Government* state that managing risk is a critical component of management control, and management should identify, analyze, and respond to risks related to achieving defined objectives.[32] In FAA's case, the agency risks not being able to achieve a key aspect of its stated objectives related to drone integration. As previously noted, FAA has acknowledged that industry envisions network-based Remote ID as a foundational piece for enabling more advanced operations. Without FAA determining a path forward on real-time, networked data about the location and status of drone flights, through Remote ID or another method, there will be continued uncertainty about how to develop the technology and whether further drone integration will be delayed.

Conclusions

FAA is charged with ensuring the safety and security of the national airspace system, a responsibility that has become increasingly challenging due to expanded drone operations. FAA has taken steps, such as issuing its Remote ID rule for drones, to help law enforcement ensure public safety. Despite these steps, law enforcement agencies we spoke with raised concerns with using Remote ID and understanding how associated drone information can help them accomplish their safety mission. By developing additional resources about Remote ID, FAA could better support the efforts of law enforcement at all levels to detect and respond to drones carrying out potentially unsafe or illegal activities. In addition, by developing a plan and timeline for its Remote ID interface, FAA would be better positioned to support timely access for law enforcement to drone operator information. This information could better inform the Remote ID app DHS is developing. In turn, DHS could better assist law enforcement in accessing FAA drone owner registration information by developing a plan and timeline for its law enforcement app and how it will connect to FAA's interface.

FAA and industry stakeholders believe that real-time, networked data about the location and status of drones in flight are needed to enable advanced operations. However, industry stakeholders said that industry faces practical limitations with developing and incorporating network-based Remote ID while meeting the broadcast-based requirement in the Remote ID rule. FAA has nonetheless encouraged industry to develop a network-based solution and has said that it may begin assessing these issues in the future. Without identifying a path forward on this issue in the near-term by assessing these issues and determining how to respond,

[32]GAO-14-704G.

FAA's progress toward fully integrating drones into the airspace may be at risk.

Recommendations for Executive Action

We are making four recommendations, including three to FAA and one to DHS. Specifically:

The Administrator of FAA should develop resources to help tribal, state, and local law enforcement use Remote ID. (Recommendation 1)

The Administrator of FAA should develop a plan and timeline for deploying FAA's interface in collaboration with DHS and DOJ. (Recommendation 2)

The Secretary of Homeland Security should develop a plan and timeline for deploying its Remote ID app in collaboration with FAA and DOJ. (Recommendation 3)

The Administrator of FAA should identify a path forward for how to provide real-time, networked data about the location and status of drones. This could include identifying and assessing short-term and long-term options and clarifying roles and responsibilities. (Recommendation 4)

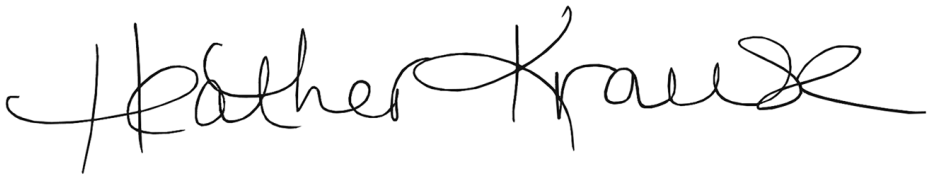
Agency Comments

We provided a draft of this report to FAA, DHS, DOJ, the Federal Communications Commission, and the National Telecommunications and Information Administration for review and comment. In its written comments, which are reprinted in appendix II and III, FAA and DHS concurred with our recommendations. DHS also provided technical comments, which we incorporated, as appropriate. DOJ, the Federal Communications Commission, and the National Telecommunications and Information Administration did not have any comments on the report.

We are sending copies of this report to the appropriate congressional committees, the Secretaries of Transportation, Homeland Security, and Commerce; the Administrator of the FAA; the Attorney General; the Chairwoman of the Federal Communications Commission; and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-2834 or krauseh@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last

page of this report. GAO staff who made key contributions to this report are listed in appendix IV.



Heather Krause
Managing Director, Physical Infrastructure

Appendix I: Stakeholders Interviewed

We interviewed representatives from a nongeneralizable sample of 23 law enforcement and drone stakeholder groups. We selected these representatives based on their participation in the Federal Aviation Administration's (FAA) aviation rulemaking committees, such as the Unmanned Aircraft Systems (UAS) Identification and Tracking rulemaking committee and the UAS Beyond Visual Line-of-Sight rulemaking committee, their participation in FAA's Advanced Aviation Advisory committee, and recommendations from other drone stakeholders.[1] We selected stakeholders to achieve a range of perspectives.

In addition to interviews with individual stakeholders, we also met with a broad range of leading stakeholders convened by a drone stakeholder group. This drone stakeholder group ensured that a broad range of leading stakeholders participated in interviews we held with this drone stakeholder group. Not all stakeholders we interviewed over the course of our review had opinions on all topics discussed. Instead, we analyzed the responses and reported on common themes that arose during the stakeholder interviews. Because we selected a nongeneralizable sample of stakeholders, their responses should not be used to make inferences about a population. See table 1 for tribal, state, and local entities, as well as drone stakeholder groups we interviewed.

Table 1: List of Stakeholders Interviewed

Tribal and State Entities
Choctaw Nation of Oklahoma
Virginia Department of Aviation
Local Law Enforcement
Houston Police Department
Miami Dade Police Department
New York Police Department
Philadelphia Police Department
Wood County Sheriff's Office
Drone Stakeholders
Academy of Model Aeronautics
Aerial Armor
Aerospace Industries Association

[1]Although a stakeholder group may not be identified as a law enforcement organization, several of these groups work with or have law enforcement membership and shared their perspective on law enforcement matters related to Remote ID.

Airborne International Response Team
Amazon
ANRA Technologies
Association for Uncrewed Vehicle Systems International
Commercial Drone Alliance
Hidden Level
MITRE Center for Advanced Aviation System Development
National Council of State Legislatures
National League of Cities
Pierce Aerospace
Skysafe
uAvionix
WhiteFox Defense Technologies, Inc.

Source: GAO. | GAO-24-106158

Appendix II: Comments from the Department of Transportation

U.S. Department of Transportation
Office of the Secretary of Transportation

Assistant Secretary for Administration

1200 New Jersey Avenue, SE
Washington, DC 20590

May 13, 2024

Heather Krause
Director, Physical Infrastructure Issues
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

The Federal Aviation Administration (FAA) is committed to promoting safe and responsible drone operation and ensuring that drones do not pose a threat to other aircraft and the National Airspace System (NAS). FAA has taken an incremental approach to integrating drones into the NAS to balance the gradually increasing risk and complexity of drone operations. Currently, FAA regulations require all Unmanned Aircraft Systems (UAS) operators to broadcast Remote Identification (ID) unless otherwise authorized by the FAA Administrator.

FAA has several efforts underway to support the integration of drones in the national airspace, including:

- Developing specific resources for tribal, state, and local law enforcement and disseminating this information through various channels, such as webinars, the International Association of Chiefs of Police Aviation Section meetings, state public safety UAS working groups, and conferences and presentations conducted by various stakeholders throughout the year.
- Developing the Application Programming Interface through a well-defined plan and timeline for deployment. FAA's timeline largely depends on our security partner's development of software, successful integration of their technology with FAA database applications, and finalization of information technology sharing agreements with partner agencies. FAA will work to ensure that Law Enforcement Assistance Program Agents and Aviation Safety Inspectors are able to receive Remote ID broadcast signals on government-issued mobile devices, as necessary.

Upon review of the draft report, the Department concurs with GAO's three recommendations to (1) develop resources to help tribal, state, and local enforcement use of Remote ID, (2) develop a plan and timeline for deploying FAA's interface in collaboration with DHS and DOJ, and (3) identify a path forward for how to provide real-time, networked data about the location and status of drones. We will provide a detailed response to the recommendations within 180 days of final report issuance.

We appreciate the opportunity to respond to the GAO draft report. Please contact Gary Middleton, Office of Audit Relations and Program Improvement, at (202) 366-6512 with any questions or if GAO would like to obtain additional details about these comments.

Sincerely,

Philip A. McNamara
Assistant Secretary for Administration

Appendix III: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

May 13, 2024

Heather Krause
Director, Physical Infrastructure
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to Draft Report GAO-24-106158, "DRONES: Actions Needed to Better Support Remote Identification in the National Airspace"

Dear Ms. Krause:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS, or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

DHS leadership is pleased to note GAO's positive recognition of the Department's efforts to develop an application (app) for law enforcement that would link to the Federal Aviation Administration (FAA) interface to provide drone registration information from Remote ID to law enforcement. DHS remains committed to working with the FAA to ensure the safe and secure use of drones in the national airspace system, and enabling more advanced drone operations by using Remote ID information to identify compliant and authorized drone activity.

The draft report contained four recommendations, including one for DHS with which the Department concurs. Enclosed find our detailed response to the recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, sensitivity, and other issues under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H CRUMPACKER Digitally signed by JIM H CRUMPACKER Date: 2024.05.13 16:56:16 -04'00'

JIM H. CRUMPACKER
Director
Departmental GAO-OIG Liaison Office

Enclosure

Enclosure: Management Response to Recommendations Contained in GAO-24-106158

GAO recommended that the Secretary of Homeland Security:

Recommendation 3: Develop a plan and timeline for deploying its Remote ID app in collaboration with FAA and DOJ [United States Department of Justice].

Response: Concur. The DHS Countering Unmanned Aerial Systems (C-UAS) Program Management Office, located within the Office of Strategy, Policy, and Plans (PLCY) is currently coordinating with the DHS Science and Technology Directorate to develop the app to link to FAA's Remote ID interface. As part of this effort, C-UAS is in the process of developing a plan of action, milestones, and required resources, and will collaborate with the FAA and DOJ, as appropriate, with regard to progress, obstacles, and timelines. However, it is important to note that this activity is currently in the planning phase and will likely be impacted by future budgeting actions for all departments and agencies involved. Further, the ability to effectively utilize this app is highly dependent upon the deployment of a Remote ID sensor infrastructure either by the FAA, DHS, or industry, which is also early in the planning and fact-finding stage. Even following successful development of this app establishing a link to drone registration and waiver databases, full benefits cannot be realized without an extensive Remote ID sensor infrastructure. Estimated Completion Date: April 30, 2025.

2

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Heather Krause, (202) 512-2834 or KrauseH@gao.gov

Staff Acknowledgments

In addition to the contact named above, the following individuals made important contributions to this report: David Sausville (Assistant Director), Ray Griffith (Analyst in Charge), Melanie Diemel, Alexandra Jeszeck, Delwen Jones, Alicia Loucks, Chi L. Mai, Kelly Rubin, Jasmine Sammons, Mike Soressi, and Alicia Wilson.