



March 2024

AVIATION SAFETY

Federal Efforts to Address Unauthorized Drone Flights Near Airports

Accessible Version

GAO Highlights

Highlights of [GAO-24-107195](#), a report to congressional committees

Why GAO Did This Study

In recent years, FAA has reported a significant number of drone sightings at or near airports. FAA prohibits drone operations that interfere with airport operations. Whether errant or malicious, unauthorized drone flights around airports present safety and security threats and can result in flight delays.

GAO was asked to review drone detection and mitigation issues at airports. This report examines (1) federal and local roles for responding to a drone incident at an airport, (2) federal legal authorities related to using drone detection and counter-drone technology at airports, and (3) FAA actions to plan for using the technology at airports and its effects on drone integration efforts.

GAO reviewed relevant federal statutes, regulations, agency documents, and reports. GAO interviewed FAA and DHS, and 18 aviation, law enforcement, and other entities to obtain a range of perspectives. GAO also reviewed FAA planning documents to determine how counter-drone technologies were incorporated into FAA's drone integration efforts.

What GAO Recommends

GAO recommends that Congress, as appropriate, amend pertinent statutory authorities related to drone detection and counter-drone operations at airports. GAO also recommends that FAA ensure its drone integration strategy reflects how it will assess the effects of counter-drone technologies. The Department of Transportation agreed with this recommendation.

View [GAO-24-107195](#). For more information, contact Heather Krause at (202) 512-2834 or krauseh@gao.gov.

March 2024

AVIATION SAFETY

Federal Efforts to Address Unauthorized Drone Flights Near Airports

What GAO Found

Tactical and airport response plans and a federal interagency agreement describe the roles for responding to errant or malicious drone operations near airports. As described in these plans, local law enforcement authorities are expected to be the first to respond to a drone sighting. The federal government can assist in responding to an incident at an airport as outlined in the federal interagency agreement.

The Departments of Homeland Security (DHS), Justice (DOJ), Defense, and Energy have express statutory authority to use counter-drone technologies if certain statutory criteria are met. They also have federal statutory exemptions from specified federal criminal laws that are potentially applicable to the use of such technologies. These technologies can be used at an airport by DHS and DOJ if the drone poses, for example, a credible threat to safety or security and the DHS Secretary or the Attorney General designates the airport for an emergency response. GAO concluded that modifications to statutory authorities for drone detection and counter-drone operations could better protect airports against an active drone threat.

The Federal Aviation Administration (FAA) is testing drone detection and counter-drone technologies and is required to develop a plan for their use at airports. FAA is also pursuing several efforts to allow increased and routine drone operations. In various documents, FAA acknowledges the effects counter-drone technologies may have on other integration efforts but does not address how it will assess those effects. Including steps for this assessment in the agency's forthcoming drone integration strategy could help ensure that such technologies will work in harmony with FAA's other efforts, such as developing a drone traffic management system and rules for operating drones beyond operators' visual line of sight.

Unauthorized Drone Flights Near Airports Present Safety and Security Threats



Source: Alexandre Rotenberg/stock.adobe.com. | GAO-24-107195

Accessible Text for Unauthorized Drone Flights Near Airports Present Safety and Security Threats

Drone and airplane in flight.

Source: Alexandre Rotenberg/stock.adobe.com. | GAO-24-107195

This is a public version of a sensitive report that was issued in October 2023 and omits some information that DHS deemed sensitive. In some cases, the omitted information was, in part, the basis for GAO conclusions presented in this report.

Contents

GAO Highlights		ii
	Why GAO Did This Study	ii
	What GAO Recommends	ii
	What GAO Found	ii
Letter		1
	Background	5
	Airport and Federal Planning Documents Define Roles for Responding to Drone Incidents	8
	Federal Statutory Authority and Guidance to Use Counter-Drone Technologies	9
	FAA Is Testing Drone Detection and Counter-Drone Technology at Airports but Has Not Assessed Its Use in Relation to Broader Integration Efforts	14
	Conclusions	20
	Matter for Congressional Consideration	20
	Recommendation for Executive Action	21
	Agency Comments	21
Appendix I: List of Entities Interviewed		22
Appendix II: Comments from the Department of Transportation		23
Appendix III: GAO Contact and Staff Acknowledgments		27
	GAO Contact	27
	Staff Acknowledgments	27
Table		
	Table 1: List of Entities Interviewed	22
Figures		
	Unauthorized Drone Flights Near Airports Present Safety and Security Threats	ii

Abbreviations

2018 Reauthorization Act	FAA Reauthorization Act of 2018
cUAS	counter-UAS systems
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOT	Department of Transportation
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
IG	Inspector General
NAS	national airspace system
NTIA	National Telecommunications and Information Administration
Remote ID	remote identification of drone technology
TSA	Transportation Security Administration
UAS	unmanned aircraft systems

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



March 18, 2024

The Honorable Sam Graves
Chairman
The Honorable Rick Larsen
Ranking Member
Committee on Transportation and Infrastructure
House of Representatives

The Honorable Garret Graves
Chairman
The Honorable Steve Cohen
Ranking Member
Subcommittee on Aviation
Committee on Transportation and Infrastructure
House of Representatives

The number of unmanned aircraft systems (UAS)—often referred to as drones—continues to grow in the U.S.¹ In 2023, the Federal Aviation Administration (FAA) forecasted that the commercial drone fleet (those operated in connection with business, research, or educational purposes) would grow from around 727,000 at the end of 2022 to 955,000 by 2027. For the same period, FAA forecasted that the recreational fleet (those operated for personal interest and enjoyment) would increase from 1.69 million to 1.82 million.² Both commercial and recreational drones have the potential to provide significant social and economic benefits and are already being used in a variety of ways, including for photography, delivering packages, and monitoring crops.

However, drones can also present safety and security threats, including when flown near an airport. In recent years, FAA and the Transportation

¹An unmanned aircraft is defined to mean an aircraft without the possibility of direct human intervention from within or on the aircraft. 14 C.F.R. §§ 1.1, 107.3. 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 on takeoff, including everything that is on board or otherwise attached to the aircraft. 14 C.F.R. § 107.3. A small UAS is defined to consist of an unmanned aircraft and its associated elements—including the aircraft, the control station, and the associated communication links—that are required for safe and efficient operation in the national airspace system. 14 C.F.R. § 107.3.

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

Security Administration (TSA), a component of the Department of Homeland Security (DHS), have reported a significant number of drone sightings by pilots and local authorities at or near airports. Since 2021, TSA reported over 2,000 drone sightings near U.S. airports, including incidents at major airports nearly every day. From 2021 through 2022, TSA reported that 63 drone incidents caused pilots to take evasive action, including four that involved commercial aircraft.

In addition to potential safety risks to aircraft and others, unauthorized drone operations at airports, whether intentional or not, can cause flight delays and significantly disrupt air traffic control operations. For example, in 2018, authorities in the United Kingdom cancelled hundreds of flights during the holiday season because of unauthorized drone activity near Gatwick International Airport. To help ensure airspace safety, in 2018, legislation was enacted requiring FAA to develop a plan for the certification, permitting, authorizing, or allowing the deployment of drone detection and mitigation technologies.³ The development of the plan is ongoing and drone incidents have continued. In July 2022, flight operations were halted at Reagan Washington National Airport due to a drone sighting. In June 2023, an unauthorized drone caused a 30-minute ground stop at Pittsburgh International Airport, according to TSA officials.

Given the emergence of drones and the potential harm presented by errant or malicious drone activity near airports, you asked us to review issues related to drone detection and mitigation at airports. Our report examined:

- FAA, TSA, and local entity roles for responding to a drone incident at an airport;
- legal authorities held by federal and local entities related to using drone detection and counter-drone technologies at airports; and
- actions FAA has taken to plan for the use of drone detection and counter-drone technologies at airports and in its broader drone integration efforts.

³FAA Reauthorization Act of 2018 (2018 Reauthorization Act), Pub. L. No. 115-254, § 383(a), 132 Stat. 3186, 3320. We also use the term drone detection technology when referring only to technology capable of detecting, identifying, monitoring, or tracking an unmanned aircraft, and the term drone mitigation technology when referring only to technology capable of deterring, preventing, responding to, and minimizing the immediate consequences of safety and security threats posed by drone operations.

This is a public version of a sensitive report that was issued in October 2023.⁴ DHS deemed some of the information to be for official use only and law enforcement sensitive, which must be protected from public disclosure. Therefore, this report omits that sensitive information, including specifics on FAA, TSA, and local entity roles for responding to a drone incident at an airport. In some cases, the information removed was, in part, the basis for GAO conclusions that are presented in this report.

To examine FAA, TSA, and local entity roles for responding to a drone incident, we reviewed FAA and TSA documents related to roles and responsibilities for responding to drone incidents. Additionally, we reviewed relevant federal statutes, regulations, and a federal interagency agreement that details the roles of various federal agencies to a drone incident at a major U.S. airport. We interviewed officials from the Department of Transportation (DOT), including FAA; DHS, including TSA; and other federal agencies involved in the coordination of drone threat responses at airports.

These agencies included the Department of Defense (DOD); Federal Communications Commission (FCC); the Department of Justice (DOJ), including the Federal Bureau of Investigation (FBI); the National Telecommunications and Information Administration (NTIA) within the Department of Commerce; and the Department of Energy (DOE).⁵ We also interviewed local airport operators and law enforcement officials from selected airports about: (1) roles and responsibilities related to drone incident response at their respective airport and (2) coordination with federal officials to plan for and respond to drone threats at or near the airport. We considered a variety of factors when selecting airports, including geographic diversity, presence and absence of drone detection equipment, high and low number of drone incidents reported to TSA from 2019 through 2021, as well as input from relevant stakeholders. The selected airports included: Dallas Fort Worth International Airport, Los Angeles International Airport, San Francisco International Airport, Tampa International Airport, and Washington Dulles International Airport.

⁴GAO, *Aviation Safety: Federal Efforts to Address Unauthorized Drone Flights Near Airports*, GAO-24-105398SU (Washington, D.C.: Oct. 26, 2023).

⁵FCC and NTIA have a regulatory oversight and coordination role in the potential use of counter-drone technologies, also known as counter-UAS systems (cUAS). FCC and NTIA do not have express federal statutory authority to use or test cUAS at airports, but certain federal agencies do have such authority.

To examine the legal authorities held by federal and local entities related to using drone detection and counter-drone technologies at airports, we reviewed and analyzed certain statutory provisions. Specifically, we reviewed and analyzed the express federal statutory provisions that both authorize federal entities to conduct drone detection and counter-drone activities and operate counter-drone technology and exempts certain detection and mitigation efforts by those entities from specified federal criminal laws that are potentially applicable. We also interviewed officials from FAA, TSA, DOD, and DOJ regarding how they view such express authorities and exemptions. Furthermore, we obtained the perspectives of the local airport operators and law enforcement officials from our five selected airports on their authority to use drone detection and counter-drone technology.

To examine actions FAA has taken for the use of the technology at airports and in its broader drone integration efforts, we reviewed legislation that requires FAA to test counter-drone technologies. We reviewed FAA's research plan that documents the testing of various drone detection and counter-drone technologies to evaluate their capabilities for use in the national airspace system. Additionally, we reviewed FAA documents describing FAA's approach to managing drone integration, as well as our previously issued reports on FAA drone integration efforts. FAA documents we reviewed included FAA's Implementation Plan for Integration of UAS into the National Airspace System (NAS) (UAS Implementation Plan);⁶ Integration of Civil UAS in the National Airspace System (NAS) Roadmap, Third Edition (UAS Roadmap);⁷ and the UAS Integration Research Plan 2020–2025 (UAS Research Plan).⁸ We reviewed these documents and information from interviews with officials to determine how drone detection and counter-drone technologies were incorporated into these efforts in line with the

⁶Federal Aviation Administration, *Implementation Plan for Integration of Unmanned Aircraft Systems (UAS) into the National Airspace System (NAS), FY 2020 UAS Implementation Plan* (Washington, D.C.: Feb.18, 2020).

⁷Federal Aviation Administration, *Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap, Third Edition* (2020).

⁸Federal Aviation Administration, *UAS Integration Research Plan 2020–2025, Edition Four* (Feb. 26, 2021).

key elements necessary for a comprehensive strategy.⁹ Lastly, we interviewed relevant FAA officials regarding the agency’s testing and plan to integrate drone detection and counter-drone technologies into its overall drone integration planning efforts.

To inform all three objectives, we conducted semi-structured interviews with representatives from a non-generalizable sample of 18 stakeholders whose work relates to drone detection and mitigation and related issues. These stakeholders were selected based on prior GAO knowledge of their work, a GAO literature search, and recommendations from airports and other stakeholders during interviews for this engagement. Because we selected a non-generalizable sample of stakeholders, their responses should not be used to make inferences about the broader population. However, our sample of stakeholders provides a range of perspectives and opinions related to drone detection and mitigation at airports. See appendix I for a full list of entities we interviewed.

The performance audit upon which this report is based was conducted from September 2021 to October 2023, 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We subsequently worked with DHS from November 2023 to March 2024 to prepare this non-sensitive version of the original sensitive report for public release. This public version was also prepared in accordance with these standards.

Background

Generally, recreational and commercial drone operators can fly in uncontrolled airspace under 400 feet, as long as they meet certain

⁹The “key elements” of a comprehensive strategy include elements we identified in GAO, *Managing for Results: Critical Issues for Improving Federal Agencies’ Strategic Plans*, [GAO/GGD-97-180](#) (Washington, D.C.: Sept. 16, 1997); and *Defense Logistics: A Completed Comprehensive Strategy is Needed to Guide DOD’s In-Transit Visibility Efforts*, [GAO-13-201](#) (Washington, D.C.: Feb. 28, 2013).

requirements.¹⁰ However, they cannot operate drones in most controlled airspace without FAA authorization. According to FAA officials, many airports are located in controlled airspace, meaning that drones require FAA authorization in order to operate in that space. Regardless, operators are expressly prohibited from operating in a manner that interferes with airport operations and traffic patterns.¹¹ According to FAA officials, this prohibition is because of concerns that small drone operations could present a hazard to other aircraft operating at low altitudes.

According to DOJ officials, law enforcement generally describes drone incidents at an airport by the intention of the operator: careless, clueless, or criminal (i.e., those acting with the necessary criminal intent to violate the law). Industry stakeholders reported at the time of our review that the majority of incidents are characterized as errant drone operations, stemming from operators who are characterized as careless or clueless. These operators may either not realize that they had entered controlled airspace or were unaware of restrictions where they were flying. Operators characterized as criminal or malicious operators, on the other hand, are considered to have an intent to cause personal harm, property damage, or economic losses, including by disrupting flights.

Drone detection and counter-drone technologies, also known as counter-UAS systems (cUAS), have been in use for many years in the national defense environment. Elements of such a system might include:

- drone detection technologies, such as radio frequency systems to scan for control signals and acoustic methods to recognize the unique sounds produced by drone motors; and

¹⁰In general, commercial operators may not operate a small drone higher than 400 feet above ground level. 14 C.F.R. § 107.51. For recreational drones, FAA instructs that drones flown at 400 feet and below in uncontrolled airspace do not need to obtain prior authorization from FAA. See FAA, Advisory Circular No. 91-57C (Oct. 20, 2022); see also http://www.faa.gov/uas/recreational_flyers. Examples of airspace restrictions include above stadiums and sporting events, near airports, security sensitive airspace (such as prisons), restricted or special use airspace, the Washington D.C. metropolitan area, and near emergency rescue operations (such as wildfires).

¹¹14 C.F.R. § 107.43. See also 18 U.S.C. § 39B (making it a criminal offense to knowingly operate an unauthorized unmanned aircraft in specified areas in close proximity to airports).

- drone mitigation technologies, which fall into two general categories, kinetic—which generally rely on physical impact to engage a target—and non-kinetic.

DHS, DOJ, DOD, and DOE all currently have express statutory authority to conduct specified drone detection and counter-drone operations, including the use of detection, mitigation, monitoring, and tracking, and the use of reasonable force to damage or destroy a threatening drone.¹² These statutory authorities additionally exempt certain detection and mitigation efforts by these entities from specified federal criminal laws that are potentially applicable.

Although FAA is not expressly authorized to conduct drone detection and counter-drone operations,¹³ FAA's statutory responsibilities include providing for the safety and efficiency of the national airspace system (NAS)¹⁴—a complex network that includes airports, aircraft, and air traffic control facilities. With respect to the NAS, FAA has primary responsibilities to develop a plan to safely integrate drone operations into the NAS while ensuring the safety and efficiency of the airspace.¹⁵ In addition, FAA is charged with coordinating with other relevant federal agencies and departments to ensure that cUAS technologies developed, tested, or deployed by federal agencies do not adversely affect the safe and efficient operation of the NAS.¹⁶

FAA guidance states that local law enforcement agencies are often in the best position to deter, detect, immediately investigate, and take appropriate action to stop unauthorized or unsafe drone operations within their authority.¹⁷ Because these agencies are on the ground in communities, they are generally able to make first contact with drone

¹²See 6 U.S.C. § 124n(a) (DOJ, DHS), 10 U.S.C. § 130i(a) (DOD), and 50 U.S.C. § 2661(a) (DOE).

¹³The 2018 Reauthorization Act does, however, require FAA to deploy detection and mitigation technologies at five airports in order to test and evaluate technologies or systems that detect and mitigate potential aviation safety risks posed by unmanned aircraft. 2018 Reauthorization Act, § 383(a), 132 Stat. at 3321 (codified at 49 U.S.C. § 44810(c)).

¹⁴See e.g., 49 U.S.C. §§ 40101, 40103.

¹⁵49 U.S.C. §§ 44802(a), 40101, 40103.

¹⁶49 U.S.C. § 44810(a).

¹⁷Federal Aviation Administration, *Law Enforcement Guidance for Suspected Unauthorized UAS Operations Version 5* (Aug. 14, 2018).

operators if there is an incident. Local law enforcement could include state and local police, as well as police units on site at an airport. Additionally, some airports have their own law enforcement units and others are served by the police in the locality where the airport is located.

Airport and Federal Planning Documents Define Roles for Responding to Drone Incidents

For this objective, we have omitted sensitive information that is contained in our October 2023 report. The omitted information includes details on how airport and federal planning documents are developed and periodically reviewed, how airports identify and classify threats, and federal roles in responding to drone incidents. In addition, the sensitive version of the report discusses a federal interagency process that identifies federal roles and responsibilities during a drone incident at an airport.

TSA and FAA provide for tactical and airport response plans that address how to respond to certain types of incidents, such as drone incidents. TSA officials told us in April 2023 that all airports they oversee have tactical response plans. According to the tactical response plans we reviewed, if the drone incident causes a persistent disruption at the airport, generally, TSA, in coordination with the federal, tribal, state, local, and territorial entities at an airport, evaluate whether the initial response is sufficient. Similar to the tactical response plans, our review of airport emergency plans for five selected airports shows that local authorities are expected to be the first to respond to a drone sighting.

Pursuant to a federal interagency agreement, if TSA, in coordination with other entities at an airport, determine that the response is insufficient to stop the drone incident, the federal government may provide specified assistance but may only use counter-drone technology to mitigate the threat when all the requirements of the Preventing Emerging Threats Act of 2018 are met.¹⁸

¹⁸Under the Preventing Emerging Threats Act of 2018, the Secretary of Homeland Security or the Attorney General may authorize their respective personnel to take actions authorized in the act (including mitigation actions) after the Secretary or Attorney General designates the facility a “covered facility,” as defined in the act.

Federal Statutory Authority and Guidance to Use Counter-Drone Technologies

Four Departments Have Express Statutory Authority to Detect Drones and Conduct Counter-Drone Operations

For this section, we have omitted sensitive information that is contained in our October 2023 report. Specifically, we omitted details regarding the potential application of federal criminal laws to drone detection and counter-drone technologies.

Various federal statutes provide four federal departments—DHS, DOJ, DOD, and DOE—express statutory authority to conduct drone detection and counter-drone operations. These authorities may be used to help protect covered facilities or assets that meet statutorily specified criteria. A federal interagency process details the use of existing authorities in responding to drone incidents at airports. In particular, this process outlines how counter-drone operations will be conducted by DHS or DOJ at airports and also notes that DHS, DOJ, or DOD may provide counter-drone technology that may integrate or be linked to drone detection systems at airports in accordance with their statutory authorities. It does not cite DOE among the federal agencies supporting drone detection and counter-drone operations at airports.¹⁹ Agency drone detection and counter-drone authorities and situations in which those authorities might be used at airports are summarized below.

The Preventing Emerging Threats Act of 2018 expressly authorizes DHS and DOJ to conduct drone detection and counter-drone operations, including the use of counter-drone technology against a drone that poses

¹⁹DOE was provided express statutory authority to conduct certain specified drone detection and counter-drone operations in 2016. National Defense Authorization Act for Fiscal Year 2017 (NDAA 2017) 2017, Pub. L. No. 114-328, div. C, tit. XXXI, subtit. B, § 3112(a), 130 Stat. 2000, 2756 (2016) (codified at 50 U.S.C. § 2661). DOE is authorized to take such actions to protect certain facilities that are (1) identified by the Secretary of Energy, (2) located in the U.S. including its territories and possessions, and (3) owned by or contracted to the U.S. to store or use special nuclear material.

a credible threat to the safety or security of covered facilities or assets.²⁰ To conduct such drone detection and counter-drone operations under the Act, including the use of counter-drone technologies, the facility or asset must be designated, among other things, a covered facility by the Secretary of Homeland Security or the Attorney General.²¹ A location may be designated as a covered facility or asset if it:

- is identified as high-risk and a potential target for unlawful UAS activity as determined by the Secretary of DHS or the Attorney General in coordination with the Secretary of DOT with respect to potentially impacted airspace through a risk-based assessment;
- is located in the U.S. (including the territories and possessions and the territorial seas and navigable waters of the U.S.); and
- directly relates to certain specified missions authorized to be performed by DHS or DOJ, which includes “an emergency response or security function limited to a specific timeframe and location.”

DOD was provided express statutory authority to conduct certain specified drone detection and counter-drone operations beginning in 2016 in the National Defense Authorization Act.²² Among other things, provisions in the act authorize the detection and mitigation of drones that are determined to be threats to DOD’s specified facilities. Statutorily specified DOD facilities for which DOD may conduct drone detection and counter-drone operations include, for example, facilities located in the U.S. that directly relate to DOD missions pertaining to nuclear deterrence, missile defense, national security space, and assistance in protecting the President or the Vice President. According to TSA officials, as of August 2023, TSA has not requested counter-drone technology from DOD for use at a domestic commercial airport.

²⁰Preventing Emerging Threats Act of 2018, § 1602(a), 132 Stat. at 3522 (codified at 6 U.S.C. § 124n(a)).

²¹The authority provided to DHS and DOJ in the Preventing Emerging Threats Act of 2018 was originally set to expire in September 2022, but legislation has extended the expiration date several times and as of March 2024 was extended through May 10, 2024, terminating on May 11, 2024.

²²NDAA 2017, Pub. L. No. 114-238, div. A, tit. XVI, subtit. F, § 1697(a), 130 Stat. 2000, 2639 (2016) (codified as amended at 10 U.S.C. § 130i). While DOE has also been provided express statutory authority to conduct certain specified drone detection and counter-drone operations, officials told us the technology DOE uses is not portable, and therefore it is unlikely they could provide assistance. For this reason, the DOE authority is not discussed further.

FAA also has responsibilities for helping to better understand and ensure the safety of drone detection and counter-drone technology use at airports.²³ For example, the 2018 Reauthorization Act requires FAA to test and evaluate drone detection and counter-drone technology or systems at five airports and develop a plan for certifying, permitting, authorizing, or allowing the use of this technology, while exempting these testing and evaluation efforts from specified potentially applicable federal criminal laws.²⁴ FAA's work on these efforts is ongoing and is discussed later in the report. With the exception of this limited testing and evaluation, FAA is not expressly authorized by statute to operate drone detection and counter-drone technologies.

Federal Guidance Issued to Help Non-Federal Entities Understand Their Authority to Use Drone Detection Technologies

In August 2020, FAA, DOJ, DHS, and FCC jointly issued an advisory to help non-federal public and private entities better understand the federal laws and regulations that may apply to the acquisition and use of technology to detect and mitigate drones.²⁵ The joint 2020 advisory strongly recommends that prior to testing, acquiring, installing, or using drone detection or drone mitigation technology non-federal entities (1) seek legal counsel experienced with both federal and state criminal, surveillance, and communications laws; and (2) conduct their own legal and technical analysis to evaluate these technologies. The advisory states that such analysis should consider whether the use of a technology might impact the public's privacy, civil rights, or civil liberties. According to

²³According to the DOT Office of Inspector General, drone detection and counter-drone operations can also be conducted for high-risk events (e.g., a Presidential Inauguration, Super Bowl, or Daytona 500 NASCAR race), and at other authorized locations, such as federal prisons. DHS, DOJ, DOD, and DOE are responsible for coordinating with FAA to ensure that drone detection and counter-drone technology and the operating guidance for and implementation of such technology will not adversely affect aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, or the use of domestic airspace.

²⁴2018 Reauthorization Act, § 383(a), 132 Stat. at 3321 (codified at 49 U.S.C. § 44810(b), (c), (g)).

²⁵*Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems* (Washington, D.C.: Aug. 2020). The joint federal advisory noted that in addition to implicating federal criminal laws, the acquisition, installation, testing, and use of drone detection or mitigation technologies may implicate laws and regulations administered by FAA and FCC relating to aviation and radio frequency spectrum. The joint advisory also noted that drone response measures may also implicate existing aviation security laws and regulations administered by TSA.

the advisory, a legal analysis is particularly important because potential legal prohibitions are based on how a particular technology functions and the specific ways it operates and is used.²⁶

According to FAA officials, FAA does not have the authority to tell an airport that it may or may not acquire and use drone detection technologies. However, under FAA regulations, entities wanting to construct or alter existing structures near an airport—such as by installing drone detection technology—must notify FAA of their proposal so that FAA can determine if the construction or alteration would constitute a hazard to air navigation.²⁷ The 2020 joint advisory also notes that non-federal entities seeking to install or use technologies for drone detection activities in the vicinity of an airport should evaluate whether they are required to provide this advance notice to FAA. Following FAA’s assessment, the agency is to issue a determination as to whether the proposed construction or alteration poses a hazard to air navigation.

When notifying the entity of a technology posing no hazard, FAA notes that its determination does not constitute an approval or disapproval but is instead a determination of the technology’s effect on the safe and efficient use of the airspace. Nevertheless, FAA also notes in its guidance on air traffic control facility operation and administration that it does not advocate the use of drone detection technologies in the airport environment until appropriate policy and procedures for their use are developed.²⁸ FAA officials told us that as of April 2023, 20 airports had

²⁶For example, according to the advisory, whether a detection or tracking system implicates federal criminal surveillance laws, such as the Pen/Trap Statute and the Wiretap Act, generally depends on whether it captures, records, decodes, or intercepts, in whole or in part, electronic communications transmitted to and from a drone or controller, and the type of communications involved. The advisory states that detection systems that emit electromagnetic waves or pulses of sound or light that are reflected off an object and back to the detection system (e.g., radar) are less likely to pose concerns under federal criminal surveillance statutes. By contrast, detection systems using radio frequency capabilities that monitor the communications passed between a drone and its ground control station may implicate the Pen/Trap Statute and Wiretap Act, according to the advisory.

²⁷See e.g., 14 C.F.R. §§ 77.5, 77.9, 77.11. Supplemental notice to FAA is required for construction or alteration more than 200 feet in height above ground level. 14 C.F.R. § 77.11(a)(1).

²⁸Federal Aviation Administration Order JO 7210.3DD, Facility Operation and Administration, dated April 20, 2023.

submitted notices to FAA for construction or alterations related to drone detection technologies.

Representatives for the five airports we interviewed at the time of our review noted different approaches to drone detection technology, with some having concerns about their authority to use the technology. Representatives from two of the five airports we interviewed told us that they had installed and are using a drone detection technology. However, representatives from one of these airports told us that they remained concerned about using the technology, stating that they believe their legal authority to detect and mitigate unauthorized drone use was unclear. Representatives from a third airport told us they intended to install drone detection technology, and after taking some steps to do so, ultimately decided not to proceed. While we did not assess the extent to which federal laws might affect the airports' testing, acquisition, installation, or use of drone detection technologies, these three airports reported that they notified FAA of their plans to install these technologies in line with FAA regulations.

At the time of our review, representatives from the remaining two airports told us they had not pursued such technologies because they did not think they had the authority to install and use them. Representatives from all five airports told us the ability to use drone detection technologies would be a valuable tool in responding to drone incidents. While representatives from two airports told us they were using drone detection technology, none of the airports we spoke with had installed drone-mitigation technology.

Challenges Related to Federal Statutory Authority to Conduct Counter-Drone Operations

The current administration and others have noted challenges associated with existing legal authorities in responding to drone incidents.²⁹ Changing or clarifying statutory authorities around drone detection and counter-drone operations could help address issues identified by stakeholders, but stakeholders also noted potential ramifications. For example, at the time of our review, representatives from one civil rights

²⁹In this public version of our report, we omitted a more detailed discussion about the identified challenges due to sensitivity concerns.

organization told us they were concerned about law enforcement potentially overusing counter-drone technology.

Ultimately, the decision to grant new or expanded authorities is a policy decision for Congress that could include considering oversight roles, training needs, and privacy issues. The current administration released a legislative proposal regarding DHS's and DOJ's use of drone detection and counter-drone technology that would provide tribal, state, local, and territorial entities as well as airport owners or operators the authority to use certain drone detection technologies subject to specified conditions and safeguards. Some legislation addressing certain identified challenges has been introduced in both the previous and the current sessions of Congress, but as of March 2024, such legislation had not yet been enacted. Legislative action to amend pertinent statutory authorities that exist for federal and non-federal entities could better protect against certain drone threats.

FAA Is Testing Drone Detection and Counter-Drone Technology at Airports but Has Not Assessed Its Use in Relation to Broader Integration Efforts

Five-Phased Research Effort Is Ongoing, but FAA Is Years Away from Completing Its Plan for the Use of Technologies

For this section, we have omitted some sensitive information that is contained in our October 2023 report. FAA developed a five-phased approach to help meet its mandate under the 2018 Reauthorization Act to test drone detection and counter-drone technologies at five airports and to develop a plan for the certification, permitting, authorizing, or allowing the deployment of drone detection and counter-drone technologies or systems.

According to FAA officials at the time of our review, Phases 1 and 2 of FAA's research effort are ongoing. For Phase 1, FAA developed a research program plan to guide its testing program in November 2020

and updated the plan in April 2022.³⁰ FAA intends to use the testing program to inform the other follow-on phases of its approach, including the required plan for certifying, permitting, authorizing, or allowing the use of detection and mitigation systems, as well as any standards that may need to be developed with respect to such technologies.³¹ According to the research program plan, FAA will use the results to provide information on the performance of a range of drone detection and counter-drone technologies (e.g., any impacts to navigational aids and other airport equipment) and best practices for airports to follow when considering future installations of such technologies.

As part of Phase 1, FAA began testing and evaluating drone detection and counter-drone technologies in 2021. FAA conducted an initial phase of testing at its William J. Hughes Technical Center at the Atlantic City International Airport to determine whether the technologies are safe for further testing. FAA selected four additional airports to provide a diverse representation of airport environments for additional technology testing and evaluation to validate performance data collected at the technical center.³² According to its research program plan, FAA plans to use testing data to determine how other airport variables (e.g., geography, noise, proximity to metropolitan areas, airport infrastructure) may affect the performance of each technology.

According to the research program plan, FAA planned to test and evaluate at least 10 technologies. Officials told us that they anticipate testing at least 15 technologies before the testing program ends.³³ The officials told us that as of June 1, 2023:

³⁰Federal Aviation Administration, *Airport Unmanned Aircraft System(s) (UAS) Detection and Mitigation Research Program* (April 2022).

³¹Among other things, section 383 of the 2018 Reauthorization Act requires FAA test and evaluate technologies or systems that detect and mitigate potential safety risks posed by drones at five airports. 2018 Reauthorization Act, § 383(a), 132 Stat. at 3321 (codified at 49 U.S.C. § 44810).

³²In addition to FAA's technical center co-located with the Atlantic City International Airport, FAA chose the following airports as test sites: Rickenbacker International Airport in Columbus, Ohio; Hancock International Airport in Syracuse, New York; Seattle-Tacoma International Airport, in Washington; and Huntsville International Airport in Alabama.

³³FAA's statutory authority to carry out its program to test and evaluate technologies or systems that detect and mitigate potential aviation safety risks posed by unmanned aircraft was originally set to expire at the end of September 2023 and is now extended through May 9, 2024, sunseting on May 10, 2024. 49 U.S.C. § 44810(h).

- eight technologies (seven detection and one mitigation) passed initial testing at the technical center and were subsequently tested at airport test sites;
- six technologies (one detection and five mitigation) were undergoing testing at the technical center, and FAA anticipated testing at airport test sites during summer 2023; and
- four technologies were scheduled for testing at the technical center during summer 2023.

Concurrent with the ongoing Phase 1 testing, FAA moved forward with Phase 2 of its approach by establishing a UAS Detection and Mitigation Systems Aviation Rulemaking Committee in March 2023 and first convening the committee in May 2023. The committee's charter states that it is tasked with making recommendations for a plan and standards to ensure the use of counter-drone technologies does not adversely impact or interfere with safe airport operations, navigation, air traffic services or with the safe and efficient operation of the NAS. The committee is also to make recommendations for a certification framework and standards in order to minimize risk to the NAS when drone detection and counter-drone technologies are used.³⁴ The committee is to submit a recommendation report to FAA within 3 months of the group's last meeting. At the time of our review, FAA officials told us that they anticipated receiving this report by the end of 2023.³⁵

FAA officials told us in May 2023 they do not currently have a timeline for completing Phases 3 through 5, which include developing and implementing the mandated plan. In March 2022, the DOT Inspector General (IG) reported that FAA's Phase 1 initial testing was delayed due to COVID-19 related impacts.³⁶ The DOT IG found that the testing delays could have a cascading effect on future phases of the program, including delaying the implementation of drone detection and counter-drone technologies and their potential to make airports safer. The report concluded that as a result of the delayed testing, FAA will not be able to

³⁴Federal Aviation Administration, *UAS Detection and Mitigation Systems Aviation Rulemaking Committee*, (Washington D.C.: Mar. 16, 2023).

³⁵In January 2024, after the issuance of the sensitive version of this report, the UAS Detection and Mitigation Systems Aviation Rulemaking Committee issued its final report. As this report was issued after our audit work had finished, we did not assess the findings of that report for this review.

³⁶Department of Transportation Inspector General, *FAA: While FAA Is Coordinating With Other Agencies on Counter-UAS, Delays in Testing Detection and Mitigation Systems Could Impact Aviation Safety*, AV2022026 (Washington, D.C.: Mar. 30, 2022).

assess safety risks and benefits until 2024 at the earliest, which will delay FAA's use of testing data to inform industry standards and its plan to authorize cUAS technology in the airport environment. FAA officials acknowledged these delays and said they plan to continue testing until their authority to do so expires. Given the status of testing and the sequential steps that FAA has identified will inform the plan, FAA is likely several years away from completing the mandated plan for using counter-drone technology. Moreover, full implementation of the plan may depend on additional legislation from Congress, according to FAA officials.

FAA Has Not Developed Plans for Assessing How Counter-Drone Technology Will Affect Other Drone Integration Efforts

FAA is pursuing a number of efforts aimed at allowing increased and routine drone operations. FAA's drone integration efforts include developing traffic management systems and requirements for remote identification of drone technology (Remote ID), and considering exemptions for operating drones beyond the operator's visual line of sight.³⁷ FAA officials told us that integrating counter-drone technologies with these efforts could be challenging because FAA does not yet fully understand all the counter-drone technologies and the effects that these technologies will have on the integration capabilities being developed by these other efforts. FAA officials also told us that counter-drone technology is intrinsically intertwined with FAA's broad responsibilities to ensure the safety of the national airspace. In testimony before Congress in July 2022, FAA stated that integrating drones is a national priority and discussed the agency's role in supporting the safe integration of counter-drone technologies into the NAS.³⁸

³⁷Remote ID is the ability of a drone in flight to provide identification and location information that can be received by other parties. It also lays the foundation of the safety and security groundwork needed for more complex drone operations, according to FAA.

³⁸Tonya Coultas, Deputy Associate Administrator for Security and Hazardous Materials Safety, Federal Aviation Administration, *Administration Counter-UAS National Action Plan Legislative Proposal*, testimony before the Senate Committee on Homeland Security and Governmental Affairs, July 14, 2022.

FAA has developed various planning documents to manage its efforts to integrate drones into the NAS.³⁹ These documents identify and describe a wide range of drone integration efforts and include various activities, timelines, and milestones that FAA is pursuing. The documents also recognize the importance of counter-drone technologies and state that these technologies could have a broader effect on the integration of drones into the national airspace. One of these documents—the UAS Implementation Plan—identifies major steps planned to enable drone traffic management systems and expected completion dates. The UAS Implementation Plan states that drone detection and mitigation technologies need to be appropriately integrated based on risk-based assessments to review any negative effects that could be introduced by such technologies.

Another FAA document, the Integration of Civil UAS in the NAS Roadmap, states that some counter-drone technologies pose a potential risk to “safety of life systems,” including air navigation services and onboard navigation. The roadmap further states that the use of counter-drone technology poses an indirect risk to persons and property on the ground or other aircraft in flight, depending on how the drone responds to the technology. Lastly, the roadmap notes that some counter-drone technologies can interfere with authorized or compliant drone activity that may be occurring near the unauthorized drone.

Overall, while these planning documents acknowledge the potential effects that counter-drone technologies could have, including on other integration efforts, they stop short of articulating how FAA will proceed with assessing them. Representatives from an organization representing the drone industry told us that assessing the effects of counter-drone technology could be a critical component of integrating drones into the national airspace. They also noted that FAA planning efforts have yet to focus on this issue. In particular, they noted that companies using or planning to use drones as part of their commercial distribution networks emphasized that it will be important for FAA and others to be able to identify drones authorized to operate at airports. Such identification would

³⁹Federal Aviation Administration, *Implementation Plan for Integration of Unmanned Aircraft Systems (UAS) into the National Airspace System (NAS), FY 2020 UAS Implementation Plan* (Washington, D.C.: Feb. 18, 2020); *Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap, Third Edition* (2020); and *UAS Integration Research Plan 2020-2025, Edition Four* (Feb. 26, 2021). In addition to these documents, individual FAA offices and staff offices develop annual fiscal year business plans that describe activities each FAA office will undertake in support of all FAA initiatives, including FAA drone integration efforts.

help ensure that authorized drone operations are not impeded by detection or mitigation technology. The organization's representatives also said that there are many unknowns regarding how all the technologies, including Remote ID, as well as FAA's traffic management and counter-drone efforts will work in harmony in the same airspace.

Questions about how drone detection and mitigation technology will affect ongoing integration activities, particularly at airports, come at a time when FAA is working to consolidate its drone planning efforts. FAA is working to replace its existing drone integration planning documents—published in 2020—with a single overarching strategy intended to guide the direction and priorities of its drone integration efforts. In doing so, FAA intends to provide greater clarity on its overall vision for drone integration by capturing all of its efforts in one document. In January 2023, we recommended that FAA develop such a strategy and that it includes all the key elements of a comprehensive strategy.⁴⁰ These key elements are based on leading practices we identified in past work and include identifying activities, milestones, performance measures, resources, and investments.⁴¹ FAA initially anticipated publishing the overarching strategy by February 2022 but now expects to complete it by June 30, 2024. While FAA has not disclosed details about what will be included in the strategy, in July 2023, it stated that it is developing the strategy collaboratively across FAA, with the intent of focusing, coordinating, and fulfilling efforts for full drone integration.

Given FAA's intentions for the strategy and consensus across FAA and industry that counter-drone technologies will affect integration, ensuring that the strategy reflects how FAA will assess potential effects is a critical next step. Without doing so, FAA will be less equipped to ensure the

⁴⁰GAO, *Drones: FAA Should Improve Its Approach to Integrating Drones into the National Airspace System*, [GAO-23-105189](#) (Washington, DC: Jan. 26, 2023). DOT agreed with our recommendation.

⁴¹The "key elements" of a comprehensive strategy include elements we identified in GAO, *Managing for Results: Critical Issues for Improving Federal Agencies' Strategic Plans*, [GAO/GGD-97-180](#) (Washington, D.C.: Sept. 16, 1997); and GAO, *Defense Logistics: A Completed Comprehensive Strategy is Needed to Guide DOD's In-Transit Visibility Efforts*, [GAO-13-201](#) (Washington, D.C.: Feb. 28, 2013). Key elements of a comprehensive strategy are: (1) mission statement; (2) problem definition, scope, and methodology; (3) goals and objectives; (4) activities, milestones, and performance measures; (5) resources and investments; (6) organizational roles and responsibilities, and coordination; and (7) key external factors that could affect goals.

safety of the NAS as advancements toward greater integration proceed, particularly at airports.

Conclusions

Unauthorized drone operations near airports can present safety and security risks as well as cause flight delays and disruptions cascading through the national airspace. As the number of drone incidents rises, it is increasingly likely that these drone incidents, whether accidental or intentional, could overwhelm local authorities' ability to respond and cause major disruptions to operations, damage infrastructure, and harm people. If local authorities cannot mitigate a drone incident, federal law enforcement may be called upon to use drone detection and counter-drone technologies at airports to address the threat. Given the current statutory authority to conduct counter-drone operations, legislative action would be needed to address some or all of these issues. Any changes to statutory authority could also involve policy considerations related to oversight roles, training needs, and privacy issues.

FAA is testing drone detection and counter-drone technology at airports to, among other things, determine how well the technologies work to mitigate potential aviation safety risks posed by drones and to inform the mandated plan for use of detection and counter-drone technologies. However, FAA's existing drone integration planning documents are a few years old and do not specify how FAA will ensure the technologies will work in harmony with other drone integration efforts. FAA is in the process of developing a comprehensive drone integration strategy. It will be important for FAA to include in this strategy a plan to assess the effects of drone detection and mitigation technologies on these other efforts. Doing so will better enable FAA to ensure the safety of the NAS as drone integration efforts expand.

Matter for Congressional Consideration

To help ensure the safety and security of the national airspace system, Congress should act to amend pertinent statutory authorities that exist for federal and non-federal entities, as it deems appropriate, with respect to drone detection and counter-drone operations at airports. (Matter for Congressional Consideration 1)

Recommendation for Executive Action

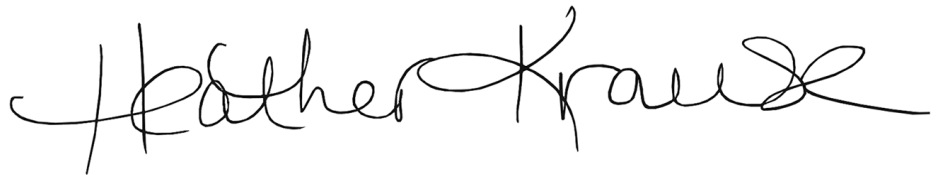
As part of ongoing efforts to develop an overarching strategy for drone integration, the Administrator of FAA should ensure that the strategy reflects plans for assessing how drone detection and mitigation technology will affect technologies aimed at allowing increased and routine drone traffic, particularly at airports. (Recommendation 1)

Agency Comments

For the performance audit upon which this report is based, we sent a draft of that report to DOT, DHS, DOJ, DOD, DOE, NTIA, and FCC. In its written comments, reproduced in appendix II, DOT agreed with our recommendation. DOT also provided technical comments, which we incorporated as appropriate. DHS, DOJ, DOD, and FCC officials provided technical comments, which we incorporated as appropriate.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the appropriate congressional committees, the Secretaries of Transportation, Homeland Security, Defense, Energy, and Commerce; the Administrator of the FAA; the Attorney General; the Chairwoman of FCC, and other interested parties. In addition, the report will be available at no charge on the GAO website at <http://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 III.



Heather Krause
Managing Director, Physical Infrastructure

Appendix I: List of Entities Interviewed

Table 1: List of Entities Interviewed

Category	Category member
Airports and Airport Police	Dallas Fort Worth International Airport
Airports and Airport Police	Los Angeles International Airport
Airports and Airport Police	San Francisco International Airport
Airports and Airport Police	San Francisco Police Department
Airports and Airport Police	Tampa International Airport
Airports and Airport Police	Washington Dulles International Airport
Aviation	Aerial Armor
Aviation	Airports Council International-North America
Aviation	Association for Uncrewed Vehicle Systems International
Aviation	Commercial Drone Alliance
Research and Standards	European Union Aviation Safety Agency
Research and Standards	MITRE Center for Advanced Aviation System Development
Research and Standards	RTCA
Research and Standards	Dr. Ryan Wallace, Embry-Riddle Aeronautical University
Research and Standards	WhiteFox Defense Technologies, Inc.
Civil Liberties	American Civil Liberties Union
Civil Liberties	Electronic Frontier Foundation
Civil Liberties	Electronic Privacy Information Center

Source: GAO. | GAO-24-107195

Appendix II: Comments from the Department of Transportation

**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

DATE: September 20th, 2023

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

The Federal Aviation Administration (FAA) continues to conduct comprehensive testing and evaluation to assess the impact of Unmanned Aircraft System (UAS) mitigation and detection technologies on the National Airspace System (NAS). FAA's analysis to date suggests that some Counter-Unmanned Aircraft Systems (cUAS) methods may interfere with certain navigation, communication, and radar systems essential to NAS operations. Additionally, adjacent off-airport critical infrastructure may be impacted as well. By the end of Fiscal Year (FY) 2023, the FAA will have completed the mitigation and detection testing as specified by Congress in Section 383 of the FAA Reauthorization Act of 2018, and the data collected will continue to be analyzed in FY 2024. These analyses along with stakeholder input from the UAS Detection and Mitigation Systems Aviation Rulemaking Committee will inform FAA's plan to certify, authorize, or allow such systems for use in the NAS and support broader UAS integration efforts.

Upon review of the draft report, the Department concurs with GAO's recommendation to ensure FAA's integration strategy reflects plans for assessing how detection and mitigation technologies will affect other technologies aimed at allowing increased and routine drone traffic, particularly at airports. We will provide a detailed response to the recommendation 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,

A handwritten signature in black ink, appearing to read "Philip A. McNamara".

Philip A. McNamara
Assistant Secretary for Administration

Accessible Text for Appendix II: Comments from the Department of Transportation

DATE: September 20th, 2023

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

The Federal Aviation Administration (FAA) continues to conduct comprehensive testing and evaluation to assess the impact of Unmanned Aircraft System (UAS) mitigation and detection technologies on the National Airspace System (NAS). FAA's analysis to date suggests that some Counter-Unmanned Aircraft Systems (cUAS) methods may interfere with certain navigation, communication, and radar systems essential to NAS operations. Additionally, adjacent off-airport critical infrastructure may be impacted as well. By the end of Fiscal Year (FY) 2023, the FAA will have completed the mitigation and detection testing as specified by Congress in Section 383 of the FAA Reauthorization Act of 2018, and the data collected will continue to be analyzed in FY 2024. These analyses along with stakeholder input from the UAS Detection and Mitigation Systems Aviation Rulemaking Committee will inform FAA's plan to certify, authorize, or allow such systems for use in the NAS and support broader UAS integration efforts.

Upon review of the draft report, the Department concurs with GAO's recommendation to ensure FAA's integration strategy reflects plans for assessing how detection and mitigation technologies will affect other technologies aimed at allowing increased and routine drone traffic, particularly at airports. We will provide a detailed response to the recommendation 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,

**Accessible Text for Appendix II: Comments
from the Department of Transportation**

Philip A. McNamara
Assistant Secretary for Administration

Appendix III: 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 the performance audit upon which this report was based: David Sausville, Assistant Director; Alexandra Jeszeck and Aaron Kaminsky, Analysts-In-Charge; Dwayne Curry; Geoffrey Hamilton; Delwen Jones; Malika Rice; Kelly Rubin; Raymond Weyandt; and Alicia Wilson.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548



Please Print on Recycled Paper.