

September 2012

# UNMANNED AIRCRAFT SYSTEMS

## Measuring Progress and Addressing Potential Privacy Concerns Would Facilitate Integration into the National Airspace System



G A O

Accountability \* Integrity \* Reliability

## Why GAO Did This Study

UAS do not carry a pilot on board, but instead operate on pre-programmed routes and by following commands from pilot-operated ground stations. UAS can be small, generally 55 pounds or less, or large. Current domestic uses include law enforcement, forest fire monitoring, border security, weather research, and scientific data collection. However, current uses are limited. FAA authorizes UAS operations on a case-by-case basis after conducting a safety review. FAA and the other federal agencies that have a role or interest in UAS are working to provide routine access for UAS into the national airspace system.

As requested, this report discusses (1) the status of obstacles identified in GAO's 2008 report to integrate UAS into the national airspace system, (2) FAA's progress in meeting its congressional requirements for UAS, and (3) emerging issues. GAO reviewed and analyzed documents and interviewed relevant government, academic, and private-sector entities, as well as UAS users and civil liberties organizations.

## What GAO Recommends

FAA should incorporate regular monitoring of its efforts to assess progress toward fulfilling its statutory requirements. FAA, DHS, and DOJ should explore whether any actions are needed to guide the collection and use of UAS-acquired data. GAO provided a draft of this report to officials at DOT, DHS, DOJ, and three other agencies. DHS and DOJ concurred with the recommendation; DOT officials agreed to consider the recommendations.

View [GAO-12-981](#). For more information, contact Gerald L. Dillingham at (202) 512-2834 or [dillingham@gao.gov](mailto:dillingham@gao.gov).

# UNMANNED AIRCRAFT SYSTEMS

## Measuring Progress and Addressing Potential Privacy Concerns Would Facilitate Integration into the National Airspace System

### What GAO Found

Progress has been made, but additional work is needed to overcome many of the obstacles to the safe integration of unmanned aircraft systems (UAS) that GAO identified in 2008. GAO reported in 2008 that UAS could not meet the aviation safety requirements developed for manned aircraft and that this posed several obstacles to safe and routine operation in the national airspace system. These obstacles still exist and include the inability for UAS to sense and avoid other aircraft and airborne objects in a manner similar to manned aircraft; vulnerabilities in the command and control of UAS operations; the lack of technological and operational standards needed to guide safe and consistent performance of UAS; and final regulations to accelerate the safe integration of UAS into the national airspace system. The Joint Planning and Development Office of the FAA has provided UAS stakeholders with a framework to collaborate and coordinate their UAS integration efforts.

Congress set forth specific requirements and deadlines in the FAA Modernization and Reform Act of 2012 for FAA to safely accelerate UAS integration. FAA, in coordination with stakeholders, has begun making progress toward completing those requirements, but has missed one deadline and could miss others. Many of the requirements entail significant work, including completing planning efforts and issuing a final rule for small UAS. Most of the requirements are to be achieved by December 2015. While FAA has taken steps to meet them, it is uncertain when the national airspace system will be prepared to accommodate UAS given that these efforts are occurring simultaneously and without monitoring to assess the quality of progress over time toward the deadlines Congress established. Better monitoring can help FAA understand what has been achieved and what remains to be done and can also help keep Congress informed about this significant change to the aviation landscape.

Concerns about national security, privacy, and the interference in Global Positioning-System (GPS) signals have not been resolved and may influence acceptance of routine access for UAS in the national airspace system. The Department of Homeland Security's (DHS) Transportation Security Administration (TSA) has the authority to regulate security of all modes of transportation, including non-military UAS. Working with FAA and other federal agencies, TSA implements security procedures, such as airspace restrictions like those limiting operations into and out of Ronald Reagan National Airport. In 2008, GAO recommended that TSA examine the security implications of non-military UAS. According to a TSA official, it recently reviewed its UAS related advisories and determined that they are still applicable. TSA has not provided information on its efforts to mitigate security implications of UAS, and GAO believes TSA should act on this recommendation. Stakeholder privacy concerns include the potential for increased amounts of government surveillance using technologies placed on UAS, the collection and use of such data, and potential violations of constitutional Fourth Amendment protections against unreasonable search and seizures. Currently, no federal agency has specific statutory responsibility to regulate privacy matters relating to UAS for the entire federal government. Some stakeholders have suggested that DHS or the Department of Justice (DOJ) might be better positioned to address privacy issues since they generally stem from the operational uses of UAS for governmental surveillance and law enforcement purposes. Working proactively to address security and privacy concerns could help prevent further delays in UAS integration. Finally, non-military UAS GPS signals are unencrypted, risking potential interruption of the command and control of UAS.

---

# Contents

---

Letter		1
	Background	4
	Status of Obstacles to Safe and Routine Integration of UAS into the National Airspace System	14
	FAA Progress toward UAS Integration Requirements	23
	Emerging Issues Related to UAS Integration Include Potential Security and Privacy Concerns and GPS Jamming and Spoofing	29
	Conclusions	37
	Recommendations	38
	Agency Comments	38
<hr/>		
Appendix I	Objectives, Scope, and Methodology	41
<hr/>		
Appendix II	Federal Entities with Certificates of Waiver or Authorization Approved from January 1, 2012, to July 13, 2012	43
<hr/>		
Appendix III	GAO Contact and Staff Acknowledgments	44
<hr/>		
Tables		
	Table 1: Key Federal and Industry UAS Stakeholders and Their Roles	12
	Table 2: Selected FAA Modernization and Reform Act of 2012 Requirements for UAS Integration	24
<hr/>		
Figures		
	Figure 1: Conceptual Rendering of Unmanned Aircraft System	2
	Figure 2: Examples of Current Uses for UAS and their Altitudes of Operation	6
	Figure 3: Non-Federal Recipients of Certificates of Waiver or Authorization and Special Airworthiness Certificates in the Experimental Category and the Location, as of July 13, 2012	8
	Figure 4: Illustration of UAS Use for Hurricane Data Collection	10

---

---

**Abbreviations list:**

2012 Act	FAA Modernization and Reform Act of 2012
ADS-B	automatic dependent surveillance-broadcast
ASTM International	formerly known as the American Society for Testing and Materials
CBP	Customs and Border Protection
COA	Certificate of Waiver or Authorization
DHS	Department of Homeland Security
DOD	Department of Defense
DOJ	Department of Justice
DOT	Department of Transportation
EUROCAE	European Organization for Civil Aviation Equipment
FAA	Federal Aviation Administration
GBSAA	ground-based sense and avoid
GPS	Global Positioning-System
GSA	General Services Administration
JPDO	Joint Planning Development Office
MASPS	minimum aviation system performance standards
MOPS	minimum operational performance standards
NASA	National Aeronautics and Space Administration
NDAA	National Defense Authorization Act
NextGen	Next Generation Air Transportation System
NPRM	Notice of Proposed Rule Making
PIA	privacy impact assessment
SC 203	Special Committee 203
RTCA	formerly the Radio Technical Commission for Aeronautics (now RTCA)
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.



**G A O**

Accountability \* Integrity \* Reliability

---

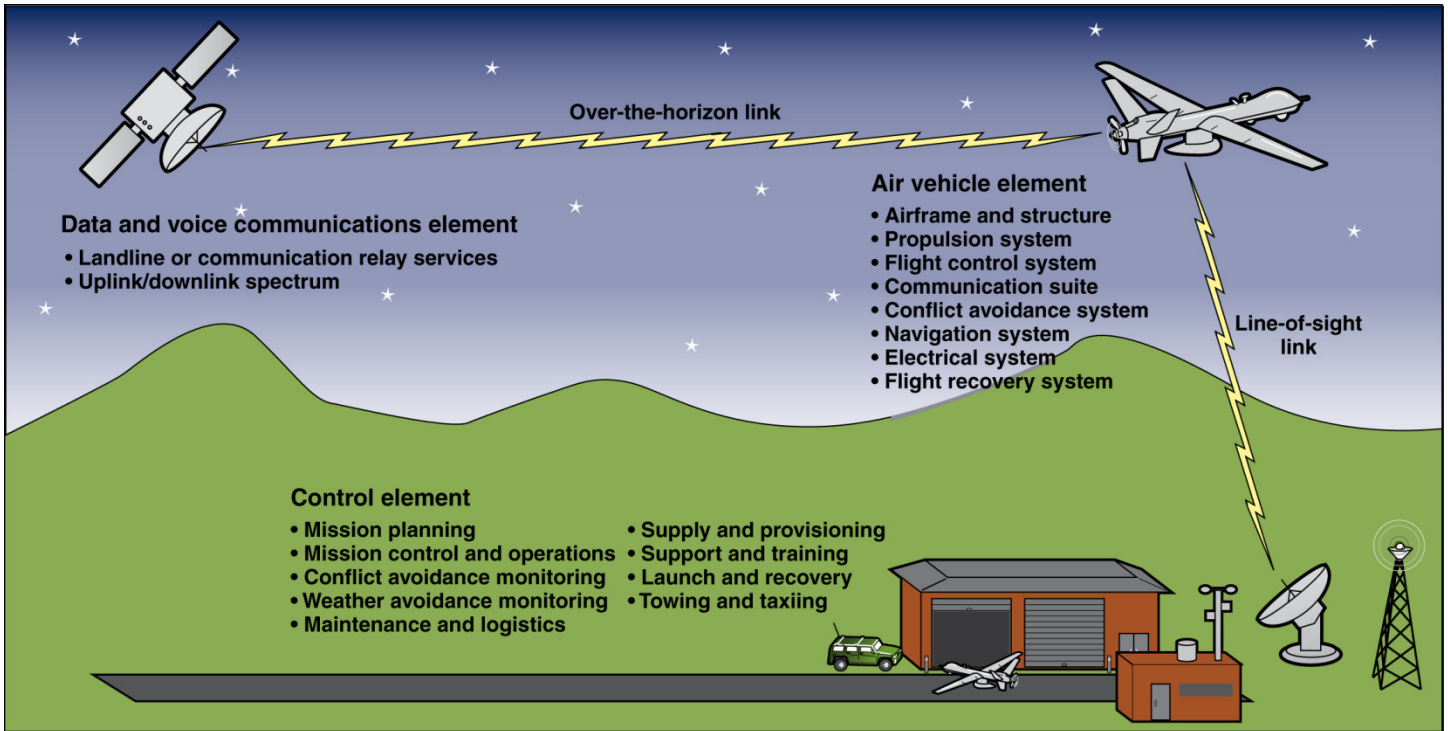
**United States Government Accountability Office**  
Washington, DC 20548

September 14, 2012

Congressional Requesters

Domestic use of unmanned aircraft systems (UAS) is expected to increase as federal, state, and local public safety entities have obtained greater access to the national airspace system and the Federal Aviation Administration (FAA) develops procedures to allow commercial UAS use. UAS aircraft do not carry a pilot onboard but instead operate on pre-programmed routes and by following commands from pilot-operated ground control stations. These aircraft are also referred to as “unmanned aerial vehicles,” “remotely piloted aircraft,” “unmanned aircraft,” or “drones.” The term “unmanned aircraft system” is used to recognize that UAS include not only the airframe and power plant, but also associated elements such as a ground control station and the communications links as shown in figure 1.

**Figure 1: Conceptual Rendering of Unmanned Aircraft System**



Sources: GAO and NASA.

According to an industry forecast, the growth in the market for government and commercial UAS use could result in worldwide expenditures of as much as \$89.1 billion (\$28.5 billion for research and development and \$60.6 billion for procurement) in aggregate over the next decade.<sup>1</sup> While the U.S. military has been a catalyst for growth in the UAS market, the industry forecaster expects the civil UAS market to emerge first based on government use and a commercial non-governmental market to emerge more slowly as the airspace access issues are being resolved. The growth in the market relies in part on regulations that will ensure the safe and routine integration of UAS into the national airspace system. Congress and other stakeholders have

<sup>1</sup>Teal Group Corporation, *World Unmanned Aerial Vehicle Systems* (Fairfax, VA: 2012).

---

expressed concerns that sufficient progress has not been made to allow for UAS to fly in the national airspace system in a manner similar to manned aircraft.<sup>2,3</sup> In 2008, we reported that safe and routine UAS access to the national airspace system poses several obstacles.<sup>4</sup> The FAA Modernization and Reform Act (the 2012 Act), enacted in February 2012, brought greater focus to integrating UAS into the national airspace system, and FAA is working toward implementing the UAS-specific requirements set forth in that act.<sup>5</sup> Concerns have been raised, by members of Congress and a civil liberties organization, about the potential implications of increased UAS use including potential privacy implications.

In this context, you asked us to assess

1. the status of obstacles to the safe and routine integration of UAS into the national airspace system that we identified in our 2008 report,
2. FAA's progress in complying with the 2012 Act UAS requirements, and
3. emerging issues pertaining to UAS.

This report focuses on issues related to non-military UAS and is based on our analysis of the efforts of FAA and other federal agencies to integrate UAS into the national airspace system as well as other emerging issues. To describe and assess the status of obstacles to safe integration that we previously identified in 2008, we reviewed documents provided by and interviewed officials of government, academic, and private-sector entities

---

<sup>2</sup>The Congressional Unmanned Systems Caucus, consisting of 60 members, was formed to educate members of Congress and the public on the strategic, tactical, and scientific value of unmanned systems; actively support further development and acquisition of more systems, and to more effectively engage the civilian aviation community on unmanned system use and safety.

<sup>3</sup> The Congressional Research Service issued a report discussing the evolution of UAS and UAS related considerations for Congress. Congressional Research Service, *Pilotless Drones: Background and Considerations for Congress Regarding Unmanned Aircraft Operations in the National Airspace System, R42718* (Washington, D.C.: September 2012).

<sup>4</sup>GAO, *Unmanned Aircraft Systems: Federal Actions Needed to Ensure Safety and Expand Their Potential Uses within the National Airspace System*, [GAO-08-511](#) (Washington, D.C.: May 15, 2008).

<sup>5</sup>FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, §§ 332 – 334, 126 Stat. 11 (2012).

---

involved with UAS issues. To assess FAA's progress in meeting its statutory requirements for UAS integration, we reviewed relevant portions of the 2012 Act and obtained documents and conducted interviews with the Unmanned Aircraft Systems Integration Office at FAA. We also identified criteria for assessments from *GAO's Standards for Internal Control in the Federal Government*. We spoke with officials from the FAA's Joint Planning Development Office (JPDO) to understand UAS coordination efforts across the federal government and other stakeholders. To identify emerging issues related to UAS, we reviewed documents provided by and interviewed officials from federal, state, and local entities that use UAS as well as representatives from the Electronic Frontier Foundation and the American Civil Liberties Union regarding UAS security and privacy concerns. We also examined pertinent legal requirements to which federal agencies must adhere when collecting and using personal information.

We conducted this performance audit from November 2011 to September 2012 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. Appendix I contains more detailed information on our objectives, scope, and methodology.

---

## Background

The national airspace system encompasses an average of more than 100,000 aviation flights per day, including commercial air carriers, general aviation,<sup>6</sup> and military aircraft. There are approximately 18,000 commercial aircraft and 230,000 active general aviation aircraft in the United States. Most commercial aircraft operate at altitudes between 18,000 and 60,000 feet,<sup>7</sup> while general aviation aircraft can operate at various altitudes, depending on the type of aircraft. For example, the

---

<sup>6</sup>According to the General Aviation Manufacturers Association, general aviation is all aviation other than military and commercial airlines that is not available to the general public for transport. General aviation includes nonscheduled aircraft operations such as air medical-ambulance, corporate aviation, and privately owned aircraft.

<sup>7</sup>Altitudes 18,000 and 60,000 feet are reported as mean sea level, which is the average height of the surface of the sea for all stages of the tide; used as a reference for elevations.



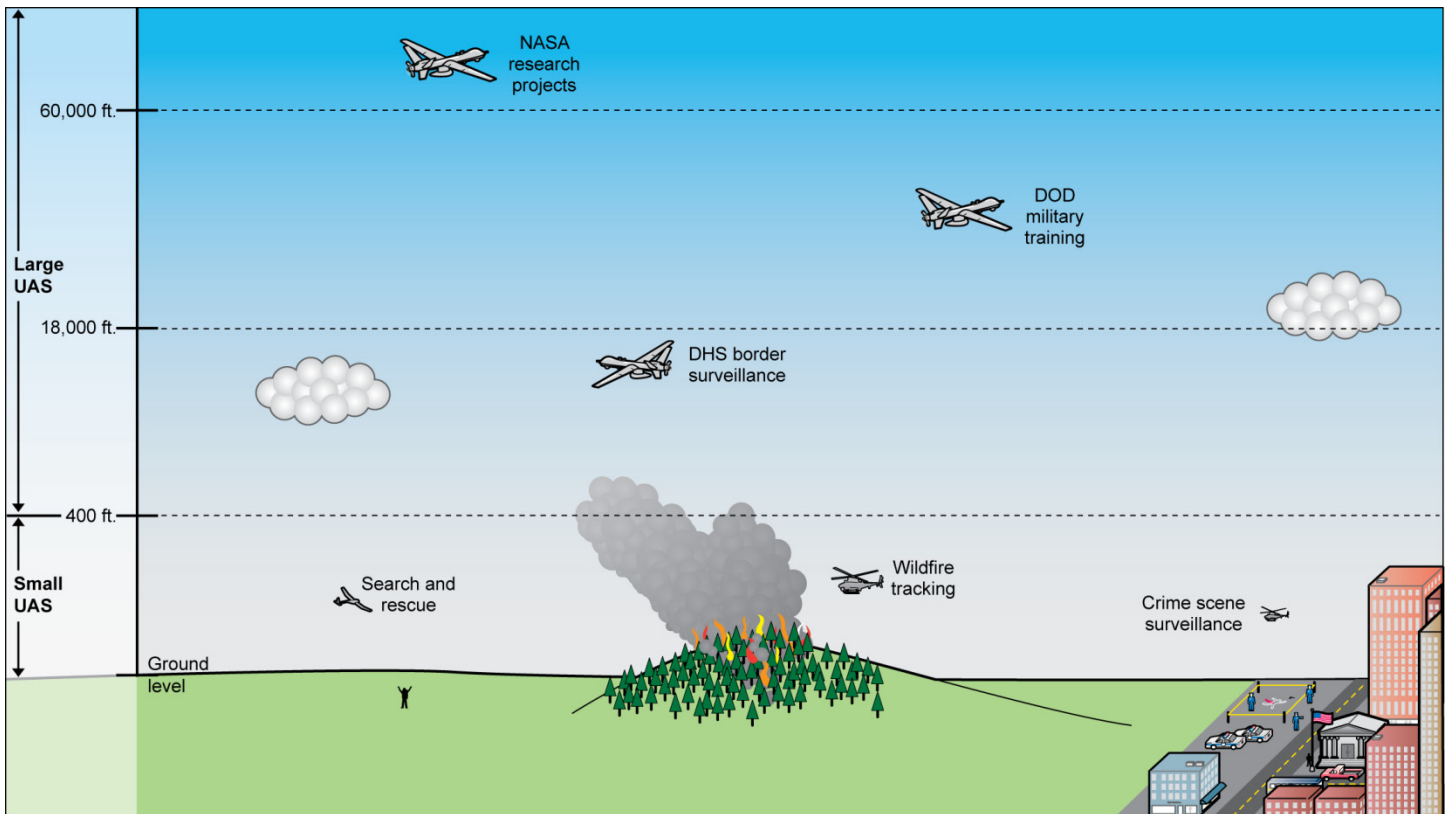
---

majority of single engine aircraft generally operate at altitudes below 10,000 feet, while multi-engine jet aircraft operate at altitudes up to 50,000 feet. UAS also fly at all levels of airspace, generally based on their size. UAS are typically described in terms of weight, endurance, purpose of use, and altitude of operation. For the purposes of this report, we use the broad categories of “large” and “small” UAS. “Small” UAS typically weigh less than 55 pounds, fly below 400 feet above ground level, can stay airborne for several hours, and can be used for reconnaissance, inspection, and surveillance.<sup>8</sup> However, some small UAS can have longer endurance and can operate beyond line-of-sight capability. “Large” UAS, depending on their size and mission, generally fly at altitudes up to or greater than 60,000 feet, some can remain airborne for multiple days, and are generally used for the purposes of surveillance, data gathering, and communications relay. Figure 2 provides examples of UAS and the altitudes at which they operate. Below 18,000 feet, there is a wide variety of types of aircraft, including those taking off and landing, and levels of activity at different altitudes which impacts the integration of UAS into the national airspace system. This variety of flight activity will require coordination with various state and federal agencies, e.g., law enforcement, agricultural, environmental, and emergency response. The activity in this airspace is projected to experience significant growth in small independent UAS utilization because of the potential economic benefits for the users of UAS.

---

<sup>8</sup>According to an industry association, small UAS are expected to comprise the majority of UAS that will operate in the national airspace system.

**Figure 2: Examples of Current Uses for UAS and their Altitudes of Operation**



Source: GAO.

Note: As a technical reference for elevations, altitudes of 18,000 and 60,000 feet are mean sea level and 400 feet is above ground level.

Note: Both NASA and DOD operate at additional flight levels other than those depicted.

Currently, FAA authorizes military and non-military (academic institutions; federal, state, and local governments including law enforcement entities; and private sector entities) UAS operations on a limited basis after conducting a case-by-case safety review. Only federal, state, and local government agencies can apply for and be granted a Certificate of Waiver or Authorization (COA); private sector entities (civil operators) may apply for special airworthiness certificates in the experimental category that

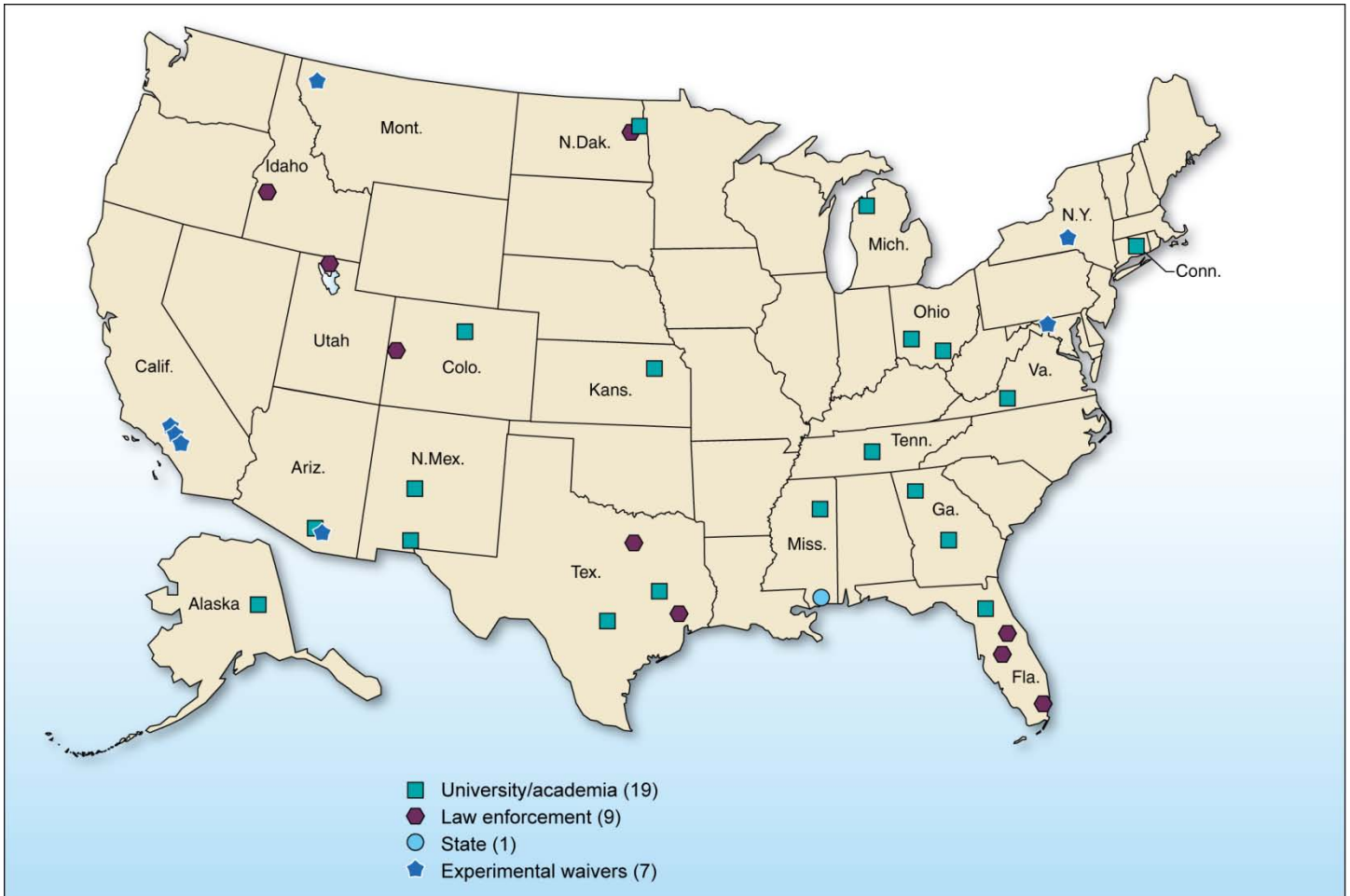
---

allows them to operate UAS.<sup>9</sup> Between January 1, 2012, and July 13, 2012, FAA issued 342 COAs to 106 federal, state, and local government entities across the United States, including law enforcement entities as well as academic institutions. Over the same time period, FAA issued 8 special airworthiness certifications for experimental use to 4 UAS manufacturers. Presently, under COA or special airworthiness certification, UAS operations are permitted for specific time frames (generally 12 to 24 months), locations, and operations and thus the COA holder may fly multiple times under a specific COA. However, it is not uncommon for an entity to receive multiple COAs for various missions and locations. See figure 3 for the locations of COA's and special airworthiness certificates in the experimental category as of July 13, 2012. See appendix II for the list of federal entities with COAs.

---

<sup>9</sup>COAs and special airworthiness certifications in the experimental category represent exceptions to the usual aircraft certification process. FAA examines the facts and circumstances of a proposed UAS to ensure that the prospective pilot has acceptably mitigated the safety risks.

**Figure 3: Non-Federal Recipients of Certificates of Waiver or Authorization and Special Airworthiness Certificates in the Experimental Category and the Location, as of July 13, 2012**



Sources: FAA and Map Resources.

Several federal agencies use UAS to fulfill their mission, including the Department of Homeland Security (DHS), the Department of Defense (DOD), the National Aeronautics and Space Administration (NASA), and the Department of Justice (DOJ). According to DHS officials, Customs and Border Protection (CBP) owns and uses nine UAS that it operates for its own border security missions as well as for missions in conjunction

---

with other agencies, and would like to expand its fleet of UAS.<sup>10</sup> DOD has successfully used UAS for intelligence, surveillance, reconnaissance, and combat missions,<sup>11</sup> and the United States military services expect to conduct more UAS training flights across the contiguous United States, as combat operations in Afghanistan and elsewhere decrease.<sup>12</sup> While many of DOD's UAS operations currently take place outside of the United States, the military services require access to the national airspace system to conduct UAS training. DOD has also assisted DHS in border security missions, including two missions since 2006 where the National Guard provided support in four southwestern Border States. NASA uses UAS primarily for research purposes, such as a large UAS (Predator B) for wildfire mapping and investigations as well as the collection of hurricane data (see fig. 4). Entities within DOJ have used UAS to fulfill its law enforcement missions.

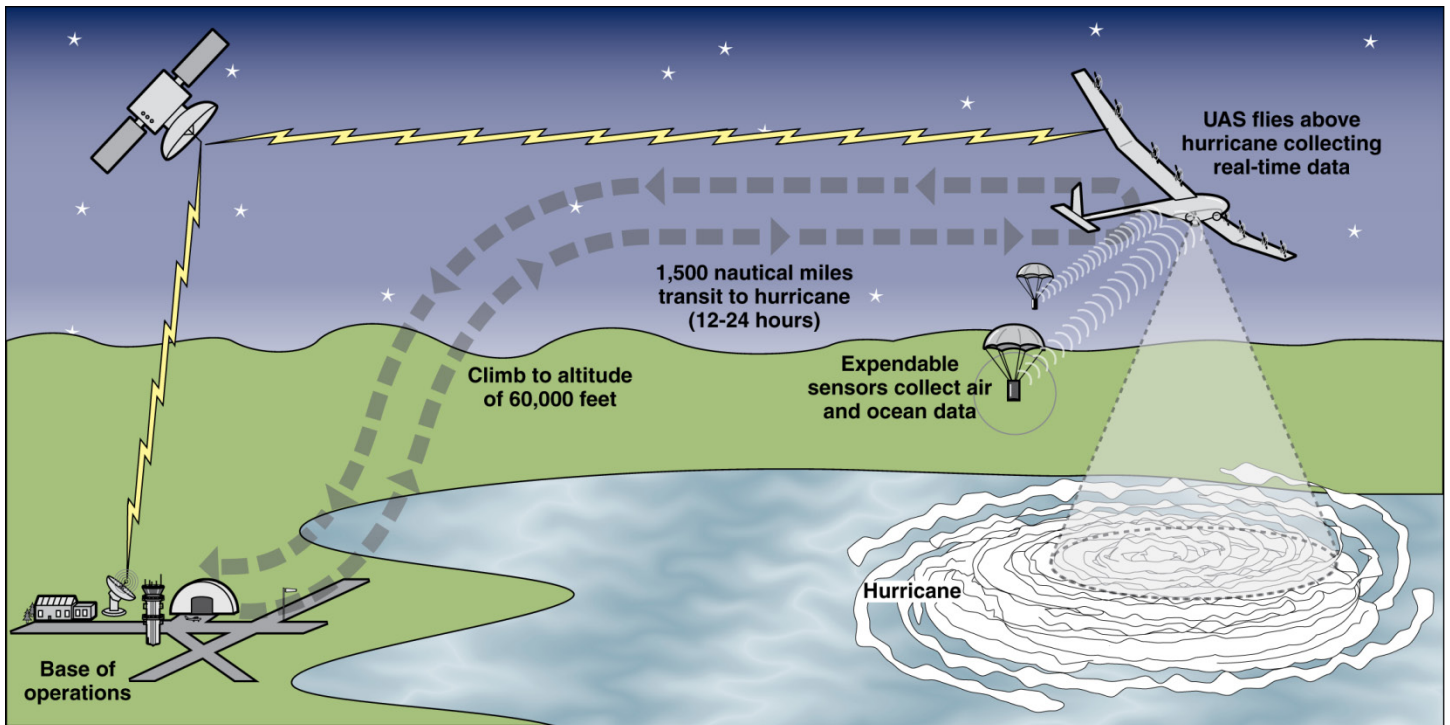
---

<sup>10</sup>The DHS Inspector General reviewed CBP's actions to establish its UAS program, the purpose of which is to provide reconnaissance, surveillance, targeting, and acquisition capabilities across all CBP areas of responsibility. The Inspector General assessed whether CBP has established an adequate operation plan to define, prioritize, and execute its unmanned aircraft mission. The Inspector General's May 2012 report found that CBP had not achieved its scheduled or desired level of flight hours for its UAS. The report estimated that CBP used its UAS less than 40 percent of the time it would have expected. The report made four recommendations intended to improve CBP's planning of its UAS program to address its level of operation, program funding, and resource requirements along with stakeholder needs. Department of Homeland Security, Office of Inspector General, *CBP's Use of Unmanned Aircraft Systems in the Nation's Border Security*, OIG-12-85 (Washington, DC: May 30, 2012).

<sup>11</sup>GAO, *Unmanned Aircraft Systems: Comprehensive Planning and a Results-Oriented Training Strategy Are Needed to Support Growing Inventories*, [GAO-10-331](#) (Washington, D.C.: Mar. 26, 2010).

<sup>12</sup>House Permanent Select Committee on Intelligence, *Performance Audit of the Department of Defense Intelligence, Surveillance, and Reconnaissance* (Washington, DC: Apr. 2012).

Figure 4: Illustration of UAS Use for Hurricane Data Collection



Sources: GAO and AeroVironment.

Although current domestic uses of UAS are limited to include activities such as law enforcement, search and rescue, forensic photography, monitoring or fighting forest fires, border security, weather research, and scientific data collection, UAS also have a wide range of other potential uses. These include commercial uses such as pipeline, utility, and farm fence inspections; vehicular traffic monitoring; real-estate and construction-site photography; relaying telecommunication signals; fishery protection and monitoring; and crop dusting. FAA's goal is to eventually permit, to the greatest extent possible, routine UAS operations in the national airspace system while ensuring safety. As the list of potential uses for UAS grows, so do the concerns about how they might affect existing military and non-military aviation as well as concerns about how they might be used.

---

According to an industry forecast, the market for government and commercial use of UAS is expected to grow, with small UAS having the greatest growth potential.<sup>13</sup> As previously stated, this forecast states that the worldwide expenditures on UAS and related research could be potentially as much as \$89.1 billion in aggregate over the next decade. The associated worldwide research and development for production is estimated to be \$28.5 billion of the \$89.1 billion.<sup>14</sup> The United States could account for 62 percent of this research and development investment. A 2008 forecast noted that while civil and commercial UAS markets will eventually emerge, a likely scenario would be for a UAS-leasing industry to emerge first to serve the needs of businesses that do not want to invest in UAS ownership.

Domestically, state and local law enforcement entities represent the greatest potential users of small UAS in the near term because they can offer a simple and cost effective solution for airborne law enforcement activities. For example, federal officials and one airborne law enforcement official said that a small UAS costing between \$30,000 and \$50,000 is more likely to be purchased by state and local law enforcement entities because the cost is nearly equivalent to that of a patrol car and much less than a manned aircraft. According to an industry trade group, local law enforcement can potentially choose from about 146 different types of small UAS being manufactured by about 69 different companies in the U.S.

In addition to FAA, many federal and private sector entities have roles in the effort to integrate UAS into the national airspace system. For example, DHS's Transportation Security Administration (TSA) has authority to regulate the security of all transportation modes to ensure that appropriate safeguards are in place. According to TSA, its aviation security efforts include addressing risks, threats, and vulnerabilities related to non-military UAS. Table 1 provides an overview of key federal and industry UAS stakeholders' roles in the integration effort.

---

<sup>13</sup>Teal Group Corporation, *World Unmanned Aerial Vehicle Systems* (Fairfax, VA: 2012).

<sup>14</sup>The other portion of the estimate, \$60.6 billion, is for the procurement of UAS.

**Table 1: Key Federal and Industry UAS Stakeholders and Their Roles**

	<b>Key stakeholders</b>	<b>UAS integration role</b>
Federal entity	FAA	FAA’s UAS Integration Office is responsible for ensuring that UAS operate safely in the national airspace system.
	DOD	DOD provides FAA with UAS operational and safety data, as well as research and development support.
	NASA	NASA provides research and development and testing on UAS integration efforts.
	JPDO	FAA’s JPDO provides a framework for UAS stakeholders to collaborate and coordinate on their UAS integration efforts.
	DHS	DHS’s CBP has provided flight demonstrations to FAA’s Next Generation Air Transportation System (NextGen) Office.
	GSA	The General Services Administration (GSA) is responsible for tracking the federal government’s UAS inventory. Federal agencies that own or lease UAS report their UAS inventory, cost and utilization data to GSA.
	DOJ	DOJ’s National Institute of Justice is responsible, in part, for addressing the technology needs—including UAS—of local, state, and tribal law enforcement agencies.
	UAS Executive Committee <sup>a</sup>	The UAS Executive Committee is composed of senior executives from federal agencies including FAA, DOD, NASA, and DHS and is responsible for identifying solutions to the range of technical, procedural, and policy concerns arising from UAS integration.
	UAS Aviation Rulemaking Committee <sup>b</sup>	The UAS Aviation Rulemaking Committee was chartered in 2011 to provide a mechanism for industry and academic stakeholders as well as other federal, state, and local government entities to provide recommendations and standards to FAA on issues related to UAS integration.
Standards making bodies	RTCA SC-203 <sup>c</sup>	RTCA is a private, not-for-profit organization consisting of industry experts. SC 203 is responsible for developing consensus-based recommendations and standards regarding UAS communications, navigation, surveillance, and air traffic management system issues.
	ASTM International Committee F38 <sup>d</sup>	ASTM International Committee F38 is a private organization consisting of industry experts that is responsible for developing standards and consensus based recommendations for small UAS integration into the national airspace system and worldwide.

Source: GAO analysis of FAA data.

<sup>a</sup>The UAS Executive Committee was formed as a result of the National Defense Authorization Act (NDAA) for Fiscal Year 2010 (Pub. L. No. 111-84, 123 Stat. 2190 (2009)). Section 935 of 2010 NDAA states that “The Secretary of Defense and the Secretary of Transportation shall, after consultation with the Secretary of Homeland Security, jointly develop a plan for providing expanded access to the national airspace system for unmanned aircraft systems of the Department of Defense” and requires the Executive Committee members to provide Congress with, among other things, a communication plan, specific milestones for expanded access to the national airspace system, and report on their efforts.

<sup>b</sup>FAA also chartered a small UAS Aviation Rulemaking Committee in 2008, which made recommendations for the standards and regulations for the operation of small UAS in the national airspace system.



---

<sup>c</sup>RTCA, formerly the Radio Technical Commission for Aeronautics, serves as a federal advisory committee, and its recommendations are the basis for a number of FAA's policy, program, and regulatory decisions.

<sup>d</sup>ASTM International, formerly known as the American Society for Testing and Materials, works to deliver the test methods, specifications, guides, and practices that support industries and governments worldwide.

FAA has also historically partnered with a range of industry, federal research entities, universities, and international organizations for research on UAS. These types of research and development agreements are categorized as Federally Funded Research and Development Centers,<sup>15</sup> Cooperative Research and Development Agreements,<sup>16</sup> and International Agreements.<sup>17</sup> These agreements typically require the agency, organization, or company to perform types of research and provide FAA with the data in exchange for funding. For example, FAA established an agreement with the European Union to initiate, coordinate, and prioritize the activities necessary for supporting the development of provisions required for the evolution of UAS to full recognition as a legitimate category-of-airspace user.

In 2008, we reported that federal actions were needed to ensure safety and expand the potential uses of UAS within the national airspace system.<sup>18</sup> We stated that Congress should consider creating an overarching body within FAA to address obstacles for routine access. While such a body has not been created, as discussed in this report, FAA is combining its UAS safety and air traffic staff under one executive, and JPDO has provided UAS stakeholders with a framework to collaborate and coordinate their UAS integration efforts. FAA implemented our recommendations that it (1) finalize and issue a UAS program plan to

---

<sup>15</sup>FAA's Federally Funded Research and Development Centers are located at MITRE, MIT's Lincoln Lab, and the Air Force Research Lab.

<sup>16</sup>FAA has Cooperative Research and Development Agreements with academic institutions such as New Mexico State University, Rutgers University, Auburn University, University of North Dakota, Stanford University, University of Alaska Fairbanks, Colorado University, Wichita State University, and Embry Riddle University. FAA also has Cooperative Research and Development Agreements with General Atomics, AAI Corporation, GE Aviation Systems LLC, Boeing Inc, and Georgia Tech Research Corporation.

<sup>17</sup>FAA's international agreements include the Netherlands, the German Aerospace Center, and the European Union.

<sup>18</sup> [GAO-08-511](#)

---

address the future of UAS and (2) analyze the data FAA collects on UAS operations under its COAs and establish a process to analyze DOD's data on its UAS research, development, and operations. In addition, to ensure that appropriate UAS security controls are in place when civil-use UAS have routine access to the national airspace system, we recommended that the Secretary of Homeland Security direct the TSA Administrator to examine the security implications of future, non-military UAS operations in the national airspace system and take any actions deemed appropriate. As discussed later in this report, TSA has taken some steps but we have not yet closed this recommendation.

---

## Status of Obstacles to Safe and Routine Integration of UAS into the National Airspace System

In 2008, we reported that UAS could not meet the aviation safety requirements developed for manned aircraft and that UAS posed several obstacles to operating safely and routinely in the national airspace system. FAA and others have continued their efforts to address these obstacles, but many still remain, including

1. the inability for UAS to detect, sense, and avoid other aircraft and airborne objects in a manner similar to "see and avoid" by a pilot in a manned aircraft;
2. vulnerabilities in the command and control of UAS operations;
3. the limited human factors engineering incorporated into UAS technologies;
4. unreliable UAS performance;
5. the lack of technological and operational standards needed to guide the safe and consistent performance of UAS;
6. the lack of final regulations to guide the safe integration of UAS into the national airspace system; and
7. the transition to NextGen.<sup>19</sup>

---

## Sense and Avoid Technologies

To date, no suitable technology has been deployed that would provide UAS with the capability to sense and avoid other aircraft and airborne objects and to comply completely with FAA regulatory requirements of the

---

<sup>19</sup>NextGen is a new satellite-based air traffic management system that will replace the current radar-based system

---

national airspace system.<sup>20</sup> However, research and development efforts by FAA, DOD, NASA, and MITRE<sup>21</sup>, among others, suggests that potential solutions to the sense and avoid obstacle may be available in the near term. With no pilot to scan the sky, most UAS do not have an on-board capability to directly “see” other aircraft. Consequently, UAS must possess the capability to sense and avoid an object using on-board equipment, or within the line-of-sight of a human on the ground or in a chase aircraft,<sup>22</sup> or by other means, such as ground-based sense and avoid (GBSAA).<sup>23</sup> Many UAS, particularly smaller models, will likely operate at altitudes below 18,000 feet, sharing airspace with other aircraft or flight objects. Sensing and avoiding other vehicles or objects through the use of technology represents a particular challenge for small UAS because aircraft, obstructions, or flight objects at low altitude often do not transmit an electronic signal to identify themselves, and even if they did, many small UAS do not have equipment to detect such signals and may be too small to carry such equipment. Since 2008, FAA and other federal agencies have managed several research activities to support meeting the sense and avoid requirements. DOD officials told us that the Department of the Army is working on a GBSAA system that will detect other airborne objects and allow the pilot to direct the UAS to maneuver to a safe location. The Army has successfully tested one GBSAA system, but this system may not be useable on all types of UAS. Another potential system to address this obstacle is an airborne sense and avoid system, which could equip UAS with the same Global Positioning System (GPS)-based transponder system that will be used in FAA’s NextGen air-traffic-management system and with which some manned aircraft are starting to be equipped. UAS could also be equipped with other systems comprised of sensors for detecting airborne aircraft or other objects, computer software to track and potentially resolve collision threats and displays to

---

<sup>20</sup> The FAA regulations include 14 C.F.R. § 91.111, “Operating near other aircraft,” with reference to “create a collision hazard,” and 14 C.F.R. § 91.113, “Right-of-way rules.”

<sup>21</sup> MITRE is a public interest company that works in partnership with the federal government applying systems engineering and advanced technology to address issues of national importance.

<sup>22</sup> A chase aircraft is a manned aircraft that is used to follow a UAS and serves as the see-and-avoid function for total flight safety. The pilot of the chase aircraft monitors for conflicting aircraft and is in constant radio contact with the pilot in command of the UAS who is on the ground.

<sup>23</sup> GBSAA is an air surveillance radar that provides positional information via a display of traffic information to the UAS flight crew.

---

provide maneuvering advice and/or information to the pilot. In 2012, NASA researchers at Dryden Flight Research Center successfully tested an automatic dependent surveillance-broadcast (ADS-B) transponder system on its Ikhana UAS.<sup>24 25</sup> An airborne sense and avoid system could include ADS-B, along with other sensors such as optical / infrared cameras and radar. However, not all aircraft will be required to be equipped with ADS-B. Until technical solutions for UAS to sense and avoid are tested and validated, both small and large UAS will continue to mitigate the “see and avoid” obstacle by operating within line-of-sight, using a chase aircraft, or operating in segregated airspace.

---

## Command and Control Communications

Similar to what we reported in 2008, ensuring uninterrupted command and control for both small and large UAS remains a key obstacle for safe and routine integration into the national airspace system. Since UAS fly based on pre-programmed flight paths and by commands from a pilot-operated ground control station, the ability to maintain the integrity of command and control signals are critically important to ensure that the UAS operates as expected and as intended.

## “Lost Link” Scenarios

FAA and MITRE have been researching solutions to lost link, but the standardization of lost link procedures, for both small and large UAS, has not been finalized. In a “lost link” scenario, the command and control link between the UAS and the ground control station is broken because of either environmental or technological issues, which could lead to loss of control of the UAS. To address this type of situation, UAS generally have pre-programmed maneuvers that may direct the UAS to first hover or circle in the airspace for a certain period of time to reestablish its radio link. If the link is not reestablished, then the UAS will return to “home” or the location from which it was launched, or execute an unintentional flight termination at its current location. It is important that air traffic controllers know where and how all aircraft are operating so they can ensure the

---

<sup>24</sup>ADS-B transponder system uses GPS signals along with aircraft avionics to transmit the aircraft’s location to ground receivers. The ground receivers then transmit that information to controller screens and cockpit displays on aircraft equipped with automatic dependent surveillance-broadcast transponder system avionics.

<sup>25</sup>Ikhana is a large UAS that NASA has used for a number of research activities, such as monitoring and tracking wildfires and expects to use for an arctic mission to assess the surface sea ice next year.

---

## Dedicated Radio-Frequency Spectrum

safe separation of aircraft in their airspace.<sup>26</sup> Currently, according to FAA, each COA has a specific lost link procedure unique to that particular operation and air traffic controllers should have a copy for reference at all times. Until procedures for a lost link scenario have been standardized across all types of UAS, air traffic controllers must rely on the lost link procedures established in each COA to know what a particular UAS will do in such a scenario.

Progress has been made in obtaining additional dedicated radio-frequency spectrum for UAS operations, but additional dedicated spectrum, including satellite spectrum, is still needed to ensure secure and continuous communications for both small and large UAS operations. In 2008, we reported that the lack of protected radio-frequency spectrum for UAS operations heightens the possibility that a pilot could lose command and control of a UAS. Unlike manned aircraft—which use dedicated, protected radio frequencies—UAS currently use unprotected radio spectrum and, like any other wireless technology, remain vulnerable to unintentional or intentional interference. This remains a key security and safety vulnerability because, in contrast to a manned aircraft in which the pilot has direct physical control of the aircraft, interruption of radio transmissions can sever the UAS’s only means of control. At the 2011 World Radio Conference, additional aviation protected spectrum was allocated for line of sight control of for both public and civil UAS operations.

UAS stakeholders are working to develop and validate hardware and standards for communications operating in allocated spectrum. Specifically, according to NASA, it is developing, in conjunction with Rockwell Collins, a radio for control and a non-payload communications data link that would provide secure communications. In addition, FAA’s UAS Research Management Plan identified 13 activities designed to mitigate command, control, and communication obstacles. One effort focused on characterizing the capacity and performance impact of UAS operations on air-traffic-control communications systems. In addition, a demonstration led by Embry-Riddle Aeronautical University in 2010

---

<sup>26</sup>Air traffic controllers monitor and coordinate the movement of air traffic. They communicate with pilots of aircraft, including UAS, but do not directly control the operations of aircraft.

---

simulated a national airspace communications system<sup>27</sup> to demonstrate the process and ability of a UAS pilot to establish alternate voice communications with air traffic control if the primary radio communications link were lost. NASA is also performing additional command and control research. As part of its 5-year UAS Integration in the National Airspace System Project, NASA is working to develop and verify a communications system prototype to support the allocation of spectrum for safe UAS operations.

---

## Human Factors

UAS stakeholders have been developing solutions to human factor issues for both small and large UAS. According to FAA, human factors are defined as a broad field that examines the interaction between people, machines, and the environment for the purpose of improving performance and reducing errors. Human factors are important for UAS operations as the pilot and aircraft are not collocated. The separation of pilot and aircraft creates a number of issues, including loss of sensory cues valuable for flight control, delays in control and communications loops, and difficulty in scanning the visual environment surrounding the unmanned aircraft. In 2008, we reported that UAS developers had not fully incorporated human factors engineering in their products. Such engineering incorporates what is known about people, their abilities, characteristics, and limitations into the design of the equipment they use, the environments in which they function, and the jobs they perform. Several human factors issues have not yet been resolved. Specifically, how pilots or air traffic controllers respond to the lag in communication of information from the UAS, the skill set and medical qualifications required for UAS pilots, and UAS pilot-training requirements. As part of NASA's UAS Integration in the National Airspace System Project, NASA is working to develop human factor guidelines for ground control stations. NASA plans to share the results with RTCA SC-203 to inform the recommended guidelines. In addition, the U.S. Army is working to develop universal ground control stations, which would allow UAS pilots to fly different types of UAS without having to be trained on multiple configurations of a ground control station.

---

<sup>27</sup>A National Airspace System Voice System is a new flexible networkable voice communications system with flexible networking capabilities that will be required for future air traffic operations, as envisioned by NextGen. The National Airspace System Voice System is the key voice communication component for NextGen, as many of the seventeen different switches currently used in the national airspace are already experiencing severe obsolescence issues.

---

## Reliability

FAA and NASA are taking steps to ensure the reliability of both small and large UAS by developing a certification process specific to UAS. Currently, FAA has a process and regulations in place for certifying any new aircraft type and allowing it access to the national airspace system. UAS stakeholders we interviewed stated that this process is costly and manpower intensive, and does not assure certification. One manufacturer that tried certifying a UAS through this process noted that it took one year and cost \$1 million to permit a single airframe to have access to the national airspace system. According to FAA, another manufacturer recently started this process. FAA's Research and Development office is working to identify the substantive differences in how to meet the certification standards for manned and unmanned aircraft. According to its Research Management Plan, the office has six activities under way that support the development of UAS-specific certification and airworthiness standards. One such activity brought subject matter experts together to examine how the varied requirements of certification<sup>28</sup> relate to operations of UAS in the national airspace system. A 2007 study examined the relevant federal regulations, statutes, orders, and policies applicable to UAS operating in the national airspace. It found that 30 percent of the certification regulations would apply to UAS, 16 percent would not apply, and it was unclear whether the remaining 54 percent would apply.

---

## Standards

Standards-making bodies are working to develop safety, reliability, and performance standards for UAS. The complexities of the issues to be addressed and the lack of operational and safety data have hindered the standards development process. Minimum aviation system performance standards (MASPS) and minimum operational performance standards (MOPS) are needed in the areas of: operational and navigational performance; command and control communications; and sense and avoid capabilities. RTCA, a standards-making body chartered by FAA, established a federal advisory committee called the Special Committee 203 (or SC 203), to establish MASPS and MOPS for FAA to use in developing UAS regulations. Individuals from academia and the private sector serve on the committee, along with FAA, NASA, and DOD officials. According to an RTCA official, both DOD and NASA are sharing the

---

<sup>28</sup>Title 14, Code of Federal Regulations (14 C.F.R.) part 91, titled "General Operating and Flight Rules."

---

results of their UAS flight experience and research and development efforts to assist RTCA in the standards development process. In addition, an international voluntary consensus standards-making body known as ASTM International Committee F38 on UAS, is working with FAA to develop standards to support the integration of small UAS into the national airspace system. An official from RTCA suggested that the standards-making process might be accelerated if RTCA SC 203 could start by producing an initial set of standards for a specific UAS with a clearly defined mission. RTCA SC 203 could then utilize those initial standards, along with the subsequent safety and performance data from those operations, to develop additional standards for increasingly complex UAS functions and missions.

While FAA officials stated that the agency's efforts to develop standards have been slowed by the lack of operational data, FAA has not utilized the operational data it does possess. In 2008, we recommended that FAA expedite efforts to ensure that UAS have routine access to the national airspace system by analyzing the data FAA collects on UAS operations as part of its COA process and establish a process to analyze DOD data on its UAS research, development, and operations.<sup>29</sup> Safety and operational data can directly support the development of UAS technology. For example, in the development and validation of UAS technology, GBSAA for example, the FAA requires data to demonstrate that cooperative and non-cooperative aircraft can be consistently identified at all operational altitudes and ranges, and the proposed system can effectively avoid a potential collision. To date, FAA has not utilized the operational data available to the agency as part of the COA process for the development of standards. According to a DOD official, it started providing, FAA with 7 years of operational and safety data in September 2011.<sup>30</sup> However, according to FAA officials, the agency has been unable to use the data to support its standards development because the data was not in a usable format. As of June 2012, FAA was still defining the data fields it needed and how the data will be used to support the development of performance or certification standards and the regulatory process for UAS. FAA officials have since communicated their data requirements to DOD and also provided us with a list of general data

---

<sup>29</sup>GAO-08-511.

<sup>30</sup> In June 2011, FAA and DOD signed a memorandum of agreement that specified the data that would be provided.



---

requirements. Furthermore, FAA officials also noted that the agency currently has a contract with MITRE to address these data challenges in fiscal year 2013.

---

## Regulations

According to FAA, its draft Notice of Proposed Rule Making (NPRM) that would define and govern how small UAS would potentially operate in the national airspace system will be issued at the end of 2012. Concerns relating to the process and potential timeline for publishing the final small UAS rule will be discussed later in this report. FAA regulations govern the routine operation of most aircraft in the national airspace system.<sup>31</sup> However, these regulations do not contain provisions that explicitly address issues relating to UAS. As we highlighted in our 2008 report, existing regulations may need to be modified to address the unique characteristics of UAS to prevent “undue harm to manned aircraft.” Today, UAS continue to operate as exceptions to the regulatory framework rather than being governed by it. Without specific and permanent regulations for safe operation of UAS, federal stakeholders, including DOD, continue to face challenges and limitations on their UAS operations. The lack of final regulations could hinder the acceleration of safe and routine integration of UAS into the national airspace system. In addition, as we stated earlier, the market for government and commercial use of UAS is expected to grow with small UAS having the greatest potential and a market forecast indicates that the United States could account for 62 percent of the world’s research and development investment for UAS technology over the coming decade.

---

## Transition to NextGen

As FAA and others continue to address the challenges to UAS integration, they must do so with the expected changes to the operations of the national airspace system as a result of NextGen in mind. As UAS operations are expected to proliferate, it is important that they are able to safely operate in the NextGen environment. Both FAA’s NextGen Integration Office and JPDO are working to coordinate UAS and NextGen research and development. NextGen is a new satellite-based air traffic management system that will replace the current radar-based system for a variety of aircraft types, including UAS. NextGen is expected to enhance the safety and capacity of the air transport system and will provide a number of operational, technical, economic, and environmental

---

<sup>31</sup>Title 14 of Code of Federal Regulations.

---

opportunities and challenges for all national airspace system users. NextGen will use technological advancements to identify the location of aircraft as they travel in the national airspace system and develop efficient flight paths. The transition to NextGen and the integration of UAS into the national airspace system entail many of the same technological issues. We have previously reported on research gaps,<sup>32</sup> and the Department of Transportation's Office of Inspector General recently reported that significant research and development issues remain unresolved, including developing cross-agency requirements, standards, procedures, and avionics for introducing UAS into the NextGen environment, among others.<sup>33</sup> According to a JPDO official, UAS and NextGen stakeholders should focus on critical and cross-cutting long-term research and development issues. These include UAS technologies, human factors, ground-control stations, communications, and sense and avoid, all associated with UAS flying with manned aircraft in a future NextGen airspace.

In addition, the NextGen Integration Office recently published its NextGen Implementation Plan. The Implementation Plan identified a number of NextGen-related efforts that could benefit UAS integration. For example, in July 2011, FAA achieved initial operating capability with ADS-B transponder-system data integrated into the air traffic control's automations system at the New York Terminal Radar Approach Control facility. As we stated earlier in this report, developing and testing ADS-B transponder-system technology may be a key aspect of an airborne sense and avoid system, which will allow for pilots of UAS to see and avoid other aircraft. Furthermore, the Office of Management and Budget recently tasked the NextGen partner agencies to develop a strategic, multiagency, NextGen UAS road map with assistance from the JPDO.<sup>34</sup> This road map would identify the most critical technology issues involved in establishing a plan for UAS operations as a part of NextGen.

---

<sup>32</sup>GAO, *Transportation: Integration of Current Implementation Efforts with Long-term Planning for the Next Generation Air Transportation System*, [GAO-11-132R](#) (Washington, D.C.: Nov. 22, 2010).

<sup>33</sup>Department of Transportation, Office of Inspector General, *Timely Actions Needed to Advance the Next Generation Air Transportation System*, Report Number AV-2010-068 (Washington, D.C.: June 16, 2010).

<sup>34</sup>The NextGen partner agencies include the Departments of Transportation, Commerce, Defense, and Homeland Security, FAA, NASA, White House Office of Science and Technology Policy, and the Office of the Director of National Intelligence.

---

Coordinating UAS integration and NextGen implementation efforts could lead to opportunities to cost-share demonstrations, eliminate duplicate investments and efforts, and accelerate the FAA's use of data and requirements to develop standards and regulations.

Similar to FAA's NextGen efforts, other countries are also looking to modernize their air traffic control systems and develop standards for UAS. FAA has worked with the international community and Europe in particular on harmonization of their systems to ensure that airplanes can seamlessly fly and transfer between different air traffic control systems. As other countries work toward integrating UAS in their respective airspaces, similar harmonization efforts will be critical to developing standards and operational procedures that could enable UAS to seamlessly cross international borders and U.S. manufacturers to sell their products in the global marketplace. International bodies and individual countries face challenges similar to those that the United States faces in integrating UAS into their respective airspaces and have similar efforts underway to develop UAS standards. The European Organization for Civil Aviation Equipment (EUROCAE) working group 73 is developing standards for large UAS (above 150 kilograms) that would be adopted by the European Union as a whole; and working group 93 is developing standards for small UAS (under 150 kilograms) that would be approved on a country-by-country basis. Both EUROCAE working groups are coordinating with RTCA SC 203 and ASTM F38 to try to ensure harmonized standards. In addition, as of April 2012, the International Civil Aviation Organization amended its International Standards, Rules of the Air to identify high level requirements related to UAS while noting that certification and licensing standards have not yet been developed.

---

## FAA Progress toward UAS Integration Requirements

Concerned with the pace of progress of UAS integration, Congress set forth specific requirements and deadlines for FAA to safely accelerate UAS integration in the 2012 Act. FAA—with its federal and other stakeholders—has begun making progress toward completing those requirements, but has missed one deadline and could miss others. Many of the requirements will require significant work on the part of FAA and its stakeholders to complete. This work involves developing detailed steps for achieving safe and routine access to the national airspace system, including defining the characteristics of safe integration, identifying needed research and development to achieve integration, and identifying the information needed to issue regulations, among other tasks. By meeting these requirements, FAA will be better positioned not only to address the obstacles cited earlier, but to achieve UAS integration.

The requirements in the 2012 Act include streamlining the existing COA process for public safety entities, developing test ranges for developing and validating UAS technologies and potential standards to completing planning efforts and issuing a final rule for small UAS. Most of the requirements must be achieved between May 2012 and December 2015 (see table 2), and FAA is working to identify the actions and resources needed to meet those requirements. The 2012 Act sets an aggressive time frame for FAA to integrate UAS into the national airspace system. In our 2008 report, we recommended that FAA expedite efforts to ensure that UAS have routine access to the national airspace system by finalizing and issuing a program plan to address future issues. In 2010, FAA implemented our recommendation by issuing a 2-page road map highlighting steps towards UAS integration, which included the goal of UAS having routine access to the national airspace system after 2020.

**Table 2: Selected FAA Modernization and Reform Act of 2012 Requirements for UAS Integration**

<b>Approximate deadline<sup>a</sup></b>	<b>FAA Modernization and Reform Act of 2012 requirement</b>	<b>Status of action</b>
05/14/2012	Enter into agreements with appropriate government agencies to simplify the process for issuing COAs or waivers for public UAS.	In process
08/12/2012	Establish a program to integrate UAS into the national airspace system at 6 test ranges. This program is to terminate 5 years after date of enactment.	In process
08/12/2012	Develop an Arctic UAS operation plan and initiate a process to work with relevant federal agencies and national and international communities to designate permanent areas in the Arctic where small unmanned aircraft may operate 24 hours per day for research and commercial purposes.	In process
08/12/2012	Determine whether certain UAS can fly safely in the national airspace system before the completion of the Act's requirements for a comprehensive plan and rulemaking to safely accelerate the integration of civil UAS into the national airspace system or the Act's requirement for issuance of guidance regarding the operation of public UAS including operating a UAS with a COA or waiver.	In process
11/10/2012	Expedite the issuance of a COA for public safety entities.	Completed
11/10/2012	Develop a comprehensive plan to safely accelerate integration of civil UAS into national airspace system.	In process
11/10/2012	Issue guidance regarding operation of civil UAS to expedite COA process; provide collaborative process with public agencies to allow an incremental expansion of access into the national airspace system as technology matures and the necessary safety analysis and data become available and until standards are completed and technology issues are resolved; facilitate capability of public entities to develop and use test ranges; provide guidance on public entities' responsibility for operation.	In process
02/14/2013	Approve and make publically available a 5-year road map for the introduction of civil UAS into national airspace system, to be updated annually.	In process
02/14/2013	Submit to Congress a copy of the comprehensive plan.	In process
02/12/2013	Make operational at least one project at a test range.	None to date

Approximate deadline <sup>a</sup>	FAA Modernization and Reform Act of 2012 requirement	Status of action
08/14/2014	Publish in the <i>Federal Register</i> the Final Rule on small UAS.	In process
08/14/2014	Publish in the <i>Federal Register</i> a Notice of Proposed Rulemaking to implement recommendations of the comprehensive plan.	None to date
08/14/2014	Publish in the <i>Federal Register</i> an update to the Administration's policy statement on UAS in Docket No. FAA-2006-25714.	None to date
09/30/2015	Achieve safe integration of civil UAS into the national airspace system.	In process
12/14/2015	Publish in the <i>Federal Register</i> a Final Rule to implement the recommendations of the comprehensive plan.	None to date
12/31/2015	Develop and implement operational and certification requirements for public UAS in national airspace system.	In process
02/14/2017	Report to Congress on the test ranges.	None to date

Source: GAO analysis of FAA Modernization and Reform Act as well as FAA progress.

<sup>a</sup>Some of these deadlines are approximate. For example, while the 2012 Act requires that a program to integrate UAS at 6 test ranges is to be established no later than 08/12/2012, such test ranges could conceivably be established prior to that date. The date such a program is actually established triggers a deadline for an additional requirement.

FAA has several efforts under way to satisfy its statutory requirements for safe integration of UAS. These include four broad categories of requirements, including: (1) developing plans for the integration of UAS into the national airspace system; (2) changes to the COA process; (3) efforts to develop UAS test ranges; and (4) developing, revising, or finalizing regulations and policies related to UAS.

- *Comprehensive plan and road map.* FAA, with the assistance of JPDO, is developing several planning documents required by the 2012 Act, including a 5-year roadmap and comprehensive plan to outline the steps toward safe integration. The road map, which FAA must complete and make publicly available by February 2013, is intended to help facilitate UAS integration into the national airspace system. Given its unique role in managing partnerships among federal agencies for NextGen, JPDO is leading the development of a comprehensive plan for UAS on behalf of FAA. As required by law, this plan shall contain, among other elements, recommendations on the small UAS rulemaking, a phased-in approach to and timeline for the integration of civil UAS into the national airspace system, and the establishment of a process to develop certification, flight standards, and air traffic requirements at UAS test ranges. To assist in the development of the comprehensive plan, FAA is developing a Concept of Operations to guide efficient federal resources planning for UAS integration. To date, FAA has not developed measures for assessing the various efforts to achieve safe integration by

---

September 2015. The 2012 Act specifies content for a more comprehensive plan than what was laid out in the 2-page road map, but it does not set forth any expectation for monitoring to assess the quality of progress over time toward meeting the range of activities to be outlined in the plan. Our *Standards for Internal Control in the Federal Government* provide the overall framework for establishing and maintaining internal control and for identifying and addressing major performance and management challenges and areas at greatest risk of fraud, waste, abuse, and mismanagement.<sup>35</sup> One of those standards is monitoring, which is an internal control designed to assess the quality of performance over time. This internal control should generally be designed to assure that ongoing monitoring occurs in the course of normal operations and that it is performed continually and is ingrained in the agency's operations. In light of the time frames and complicated tasks ahead, the absence of regular monitoring precludes the agency and Congress from assessing progress toward completion of the 2012 Act requirements.

- *Changes to the COA process.* FAA has changed the existing COA process in response to the 2012 Act, including taking steps to expedite COAs for public safety entities and finalizing agreements with government agencies to expedite the COA or waiver process for UAS. First, FAA extended the length of UAS authorization from a 12-month period to a 24-month period so that those entities receiving COAs do not have to reapply as frequently. Second, FAA worked with DOJ's National Institute of Justice to develop a process through a memorandum of understanding to meet the operational requirements of law enforcement entities, which are expected to be early adopters of small UAS. According to FAA, two law enforcement entities currently use small UAS on a consistent basis for their missions and operations. Officials from both FAA and DOJ have reached agreement on a draft version of the memorandum of understanding establishing this process; the memorandum of understanding is still under legal review. The process would allow law enforcement entities to receive a COA for training and performance evaluation. When the entity has shown proficiency in operating its UAS, it would then receive an operational COA allowing it to operate small UAS for a range of missions. While this process adds an additional step for

---

<sup>35</sup>GAO, *Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: November 1999).

---

entities applying to operate a UAS, once an entity receives the operational COA, it has more latitude for where and when it can operate its UAS. According to FAA data, as of July 2012, 12 state and local law enforcement entities have a COA. An official at the DOJ said that approximately 100 law enforcement entities have expressed interest in using UAS for some of their missions. According to law enforcement officials with whom we spoke, small UAS are ideal for certain types of law enforcement activities. Officials anticipate that small UAS could provide support for tactical teams, post-event crime scene analysis, and critical infrastructure photography. Officials do not anticipate using small UAS for routine patrols or missions that would require flights over extended distances or time periods.

- *Test ranges.* FAA has taken steps to develop, but has not yet established, a program to integrate UAS at six test ranges, as required by the 2012 Act. FAA must establish six test ranges, and as part of these ranges, FAA must safely designate airspace for integrated manned and unmanned flight operations, develop certification standards and air traffic requirements for UAS, ensure the program is coordinated with NextGen, and verify the safety of UAS and related navigation procedures before integrating them into the national airspace system. FAA expects data obtained from these test ranges will contribute to the continued development of standards for the safe and routine integration of UAS. In March 2012, FAA issued a Request for Comments in the *Federal Register* and subsequently received 227 comments from congressional members, state and local governments, industry firms, academic and other entities, and individuals. The comments addressed questions such as what certification requirements should be set for aircraft as part of the test ranges, who should manage the airspace and what restrictions should be placed on those using the test ranges, and where test ranges should be located. For example, FAA has proposed outsourcing the management of the test ranges; however, some commenters preferred FAA or another public entity to maintain oversight responsibility. Some commenters also said that test ranges should be selected based on locations with existing facilities and infrastructure, given the absence of any funding available for the set-up, management, or oversight of the test ranges. FAA officials told us they are still working to meet all of the specified requirements for the test ranges and had expected to issue a Request for Proposals in July 2012. However, because of privacy concerns regarding the collection and use of UAS-acquired data expressed by commenters, the internal review process was delayed, and FAA officials do not know when they will issue the Request for Proposals. The 2012 Act requires the FAA

---

to have at least one project at a test range operational 180 days after the date the project is established.

- *Rulemaking.* While FAA has efforts under way supporting a rulemaking for small UAS, as required by the 2012 Act, it is uncertain whether FAA will be able to meet the established deadline. The agency's rulemaking efforts for UAS date back more than 5 years, when it established the small UAS Aviation Rulemaking Committee in 2008. In August 2011, FAA provided the Secretary of Transportation with its draft NPRM for the first time. Since then, the Office of the Secretary has provided several rounds of comments to FAA to further refine the NPRM. FAA expected to publish the NPRM in late 2011, but FAA officials told us in August 2012 that the Office of the Secretary of Transportation was still reviewing the draft and that FAA does not expect to publish it in the *Federal Register* before the end of the year.<sup>36</sup> FAA is required by the 2012 Act to publish a final rule governing small UAS in the *Federal Register* by August 2014.

While FAA has made some progress to meet the requirements from the 2012 Act to date, those requirements that remain will require significant work from the agency to meet the established deadlines. FAA has reorganized to provide more focus on its UAS integration efforts; however, because the reorganization has not yet been fully implemented, it remains unclear whether it will provide the support needed to complete the work. FAA's UAS efforts rely on expertise and resources from several offices within FAA, such as the Aviation Safety Organization, the Air Traffic Organization, the Research and Development Integration Office, JPDO, and the NextGen Office. FAA has reorganized its office that oversees UAS activities several times over the past few years, but had not previously assigned a single and visible leader to this effort. We have previously reported the need for stable leadership at FAA for major aviation efforts.<sup>37</sup> More recently, FAA has taken steps to provide the organizational leadership needed to facilitate progress to safely

---

<sup>36</sup>In general, after OMB reviews a proposed rule, the proposed rule is issued and the public provides comments generally within a 60-day period. This is followed by the agency's preparation and OMB's review of the final rule, concluding with the agency publishing the final rule in the *Federal Register*.

<sup>37</sup>GAO, *Joint Planning and Development Office: Progress and Key Issues in Planning the Transition to the Next Generation Air Transportation System*, [GAO-07-693T](#) (Washington, D.C.: Mar. 29, 2007).



---

accelerate UAS integration into the national airspace system. In March 2012, FAA assigned an Executive Manager for its newly created UAS Integration Office, which is expected to combine UAS-related activities from the agency's Air Traffic Organization and Aviation Safety Organization. However, as of July 2012, the UAS Integration Office had not yet been finalized within FAA and no employees had been officially assigned to the UAS Integration Office. FAA officials told us that they expect approximately 50 federal employees and contractors eventually will be assigned to the office; however, the officials are still evaluating the number of personnel needed.<sup>38</sup>

While FAA has taken steps to meet the requirements set forth in the 2012 Act, it is uncertain when the national airspace system will be prepared to accommodate UAS. FAA's efforts and activities are occurring simultaneously and without monitoring to assess the quality of progress over time toward the deadlines Congress established as well as the activities to occur over the next 5 years, as outlined in FAA's road map.

---

## Emerging Issues Related to UAS Integration Include Potential Security and Privacy Concerns and GPS Jamming and Spoofing

Although not new, concerns about national security, privacy issues, and GPS jamming and spoofing related to UAS have not been resolved and may influence the acceptance of routine access for UAS in the current national airspace system or the forthcoming transition to NextGen.

---

## Security of Domestic UAS Use

In 2008, we reported that TSA had not examined the security implications of routine UAS access in the national airspace system, an assessment that remains unchanged. Within DHS, TSA has authority to regulate security of all transportation modes to ensure that appropriate security safeguards are in place. According to TSA, its aviation security efforts

---

<sup>38</sup>Presently, the Air Traffic Organization and the Flight Standards Organization are developing a Service Level Agreement (SLA) that will define the reporting protocols for Air Traffic Organization employees who would be reporting to the Aviation Safety Organization, which structurally houses the UAS Integration Office.

---

include addressing risks, threats, and vulnerabilities related to non-military UAS. Working with FAA and other federal agencies, TSA implements security procedures, such as allowing some flights into restricted airspace (e.g., allowing certain operations into and out of Ronald Reagan National Airport).<sup>39</sup> TSA also coordinates and provides notice about threats to transportation in addition to carrying out other security-related responsibilities.

In 2008, we recommended that TSA examine the security implications of future, non-military UAS operations in the national airspace system and take any actions deemed appropriate. At the time, TSA indicated that it used a risk management approach to identify and address security threats, but had not completed a UAS risk assessment. In response to our recommendation, DHS referenced the 2007 National Strategy for Aviation Security, which requires regular reviews of national aviation security programs as a whole to identify conflicting procedures, changes to threats, vulnerabilities, and resulting consequences, and coordinate mitigation measures but does not specifically address UAS. Since 2008, TSA has identified and documented the potential threat posed by UAS and remote controlled aircraft on several occasions. In its 2004 advisory, TSA noted the potential for UAS to carry explosives or biological weapons and advised individuals to report any suspicious activities to local law enforcement and the TSA General Aviation Hotline.<sup>40</sup> According to a TSA official, it recently reviewed its UAS related advisories and determined that they are still applicable. However, TSA has not provided information on specific steps it has taken to mitigate the potential threats, but believes its current practices are sufficient to address UAS security. A recent incident in which a man pled guilty to plotting to use a large remote-controlled model aircraft filled with plastic explosives to attack the

---

<sup>39</sup>After the attacks of September 11, 2001, the FAA maintained flight restrictions over certain cities and sensitive sites, including Washington D.C., Ronald Reagan National Airport. While commercial aircraft operators with full TSA security programs were permitted to resume at Ronald Reagan National Airport, commercial operators without full programs and general aviation operators were largely prohibited from operating into and out of the airport. In order to fly into these restricted airspace areas, certain aircraft operators must seek a waiver from TSA, which provides an analysis of the security aspects of requests for waivers.

<sup>40</sup>Department of Homeland Security, *TSA Advisory: Security Information Regarding Remote Controlled Aircraft and Unmanned Aerial Vehicles* (Washington, DC: Nov. 22, 2004).

---

Pentagon and U.S. Capitol highlights the potential for UAS being used as weapons.

Security remains a significant issue that could be exacerbated with an increase in the number of UAS. TSA's practices might be sufficient in the current UAS environment of limited operations taking place under closely controlled conditions, but these controlled conditions will change as FAA and others continue to work toward allowing routine UAS operations in the national airspace system. Without an assessment of TSA's current security practices, TSA is not equipped to know whether any changes to its practices are needed. As a partner agency of JPDO, DHS—and specifically TSA—have an opportunity to shape the security requirements for UAS from the outset. For example, TSA has not yet taken steps to develop security requirements for UAS ground control stations, which are the UAS equivalent of cockpits.

Another emerging issue is the operation of model aircraft—aircraft flown for hobby or recreation. Congress defined the term “model aircraft” in the 2012 Act as an unmanned aircraft that is capable of sustained flight in the atmosphere, flown within visual line of sight of the person operating the aircraft, and flown for hobby or recreational purposes. Model aircraft and small UAS—the latter for which FAA is currently developing rules—may essentially be the same aircraft with the critical difference being that the operator of the model aircraft is a hobbyist and the small UAS is being operated for an authorized purpose such as a search and rescue mission. According to FAA officials, model aircraft, which are subject to special statutory conditions outlined in the 2012 Act, can be larger and faster and fly at higher altitudes than UAS that are expected to operate under the proposed rule for small UAS. FAA provided guidance on voluntary safety standards to model aircraft operators in 1981 in its *Advisory Circular 91-57*. A model aircraft association has also published voluntary guidance documents for its members.<sup>41</sup> Voluntary guidance, however, is not enforceable and, according to FAA officials, does not address the increased size and performance capability of model aircraft. Owners of model aircraft do not require a COA to operate their aircraft. Pursuant to the 2012 Act, FAA is prohibited from developing any rule or regulation for

---

<sup>41</sup>FAA's *Advisory Circular 91-57* sets out model aircraft operating standards that encourage voluntary compliance with specified safety standards for model aircraft operators.

---

model aircraft that fly under a specified set of conditions.<sup>42</sup> Regardless of the statutory prohibition against promulgating a rule or regulation for model aircraft, FAA maintains the authority to take enforcement action against the operator of a model aircraft who endangers the safety of the national airspace system or persons and property on the ground. For example, in April 2012, FAA took such action against a person who operated a small remote controlled model aircraft on the campus of the University of Virginia in close proximity of pedestrians. FAA fined the operator \$10,000, citing public safety concerns based on video footage of the aircraft flying close to pedestrians, cyclists, and property.

We continue to believe that our 2008 recommendation—that TSA examine the security implications of future, non-military UAS operations in the national airspace system and take any actions deemed appropriate—remains relevant and that TSA should take steps to implement the recommendation.

---

### Privacy Concerns over the Collection and Use of UAS-Acquired Data

Recently, members of Congress, a civil liberties organization, and others expressed concern that the potential increased use of small UAS for surveillance and other purposes in the national airspace system has potential privacy implications. Concerns include the potential for increased amounts of government surveillance using technologies placed on UAS, the collection and use of such data, and potential violations of constitutional Fourth Amendment protections against unreasonable search and seizure.<sup>43</sup> Additionally, a June 2012 poll conducted by Monmouth University reported that 42 percent of those sampled were very concerned about their own privacy if U.S. law enforcement started

---

<sup>42</sup>This prohibition on FAA model aircraft rules or regulations only applies where the aircraft is: (1) flown strictly for hobby or recreational use; (2) operated in accordance with a community-based set of safety guidelines and within the programming of a nationwide community-based organization; (3) limited to not more than 55 pounds (unless otherwise certified through a design, construction, inspection, flight test, and operational safety program administered by a community-based organization); (4) operated in a manner that does not interfere with and gives way to any manned aircraft; and (5) when flown within 5 miles of an airport, operated under prior notice to the airport operator and the air traffic control tower.

<sup>43</sup> The Congressional Research Service has issued a report assessing the use of UAS under the Fourth Amendment. Congressional Research Service, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses*, R42701 (Washington, D.C.: September 2012).

---

using UAS with high tech cameras, while 15 percent said they were not at all concerned. However, the poll reported that of those sampled, 80 percent said they supported the use of UAS for search and rescue missions while 67 percent said they oppose the use of UAS to issue speeding tickets.<sup>44</sup> While the 2012 Act contains provisions designed to accelerate the safe integration of UAS into the national airspace system, proposed legislation in the 112th session of Congress seeks to limit or serve as a check on government use of UAS by, for example, limiting the ability of the federal government to use UAS to gather information pertaining to criminal conduct without a warrant.<sup>45</sup>

Many stakeholders we interviewed projected how past Supreme Court cases that address privacy issues related to government surveillance might apply to UAS. While the Supreme Court has not addressed privacy issues related to governmental UAS surveillance, the Court has, however, upheld several instances involving government aerial surveillance from manned aircraft.<sup>46</sup> Several other Supreme Court governmental surveillance cases, while not aerial surveillance cases, specifically relate to technology (one involving a GPS tracking device and the other a thermal imaging device) and have included some general discussion of the interplay between evolving technology and privacy.<sup>47</sup> In the 2012 GPS case, for example, one Justice observed, in part, that with respect to privacy expectations, “technology can change those expectations” and that “dramatic technological changes may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may

---

<sup>44</sup>The Monmouth University Polling Institute reported that it conducted the poll on June 4 to 6, 2012 with a national random sample of 1,708 adults age 18 and older, including 607 via live interview on a landline telephone, 675 via interactive voice response on a landline, and 426 via live interview on a cell phone. Monmouth University Poll, “U.S. Supports Some Domestic Drone Use, But Public Registers Concern About Own Privacy” (June 12, 2012).

<sup>45</sup>Preserving Freedom from Unwarranted Surveillance Act of 2012, S. 3287, 112<sup>th</sup> Cong. (2012) and Farmer’s Privacy Act of 2012, H.R. 5961, 112<sup>th</sup> Cong. (2012).

<sup>46</sup>See, e.g., *California v. Ciraolo*, 476 U.S. 207 (1986); *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986); and *Florida v. Riley*, 488 U.S. 445 (1989).

<sup>47</sup>See, *Kyllo v. United States*, 533 U.S. 27 (2001); *United States v. Jones*, 132 S. Ct. 945 (2012).

---

find the tradeoff worthwhile.”<sup>48</sup> These manned aircraft and advanced surveillance technology cases may present some issues similar to those that may be raised as governmental use of UAS becomes more widespread.

At the individual agency level, there are multiple federal laws designed to provide protections for personal information collected and used by federal agencies. As we have previously reported,<sup>49</sup> privacy protections for personal information collected or used by federal agencies is governed primarily by two laws: the Privacy Act of 1974<sup>50</sup> and the privacy provisions of the E-Government Act of 2002.<sup>51</sup> The Privacy Act, as amended, places limitations on agencies’ collection, disclosure, and use of personal information maintained in systems of records. The E-Government Act of 2002 was passed, among other reasons, to enhance the protection for personal information in government information systems or information collections by requiring that agencies conduct privacy impact assessments (PIA). PIAs are analyses of how personal information is collected, stored, shared, and managed in a federal system. In addition, a number of federal agencies including the Department of Transportation (DOT), DHS, and DOJ, are statutorily required to establish a privacy office and/or Chief Privacy Officers to assess their agency programs, including proposed programs, systems, technologies, or rule-makings for privacy risks. DHS reports that its associated privacy office also provides policy and programmatic oversight across the agency. DHS was the first federal agency to be statutorily required to establish a privacy officer. With respect to the individual agencies, both DOT’s and DHS’s privacy officers responsibilities include “assuring that the use of technologies

---

<sup>48</sup>*United States v. Jones*, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring). In *Kyllo*, a justice stated, in part, that “it would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology. For example, the technology enabling human flight has exposed to public view (and hence, we have said, to official observation) uncovered portions of the house and its curtilage that once were private.” *Kyllo v. United States*, 533 U.S. 27, 33-34 (2001)

<sup>49</sup>See, GAO, *Privacy: OPM Should Better Monitor Implementation of Privacy-Related Policies and Procedures for Background Investigations* [GAO-10-849](#) (Washington, D.C.: Sep. 7, 2010).

<sup>50</sup>Pub. L. No. 93-579, 88 Stat. 1896 (1974).

<sup>51</sup>Pub. L. No. 107-347, 116 Stat. 2899 (2002).

---

sustain, and do not erode, privacy protections relating to the use, collection, and disclosure” of personal information.

We recently testified that while laws and guidance set minimum requirements for agencies, they may not protect personal information in all circumstances in which it is collected and used throughout the government and may not fully adhere to key privacy principles.<sup>52</sup> We have previously suggested that Congress consider amending applicable privacy laws to address identified issues in three major areas: applying privacy protections consistently to all federal collection and use of personal information, ensuring that use of personally identifiable information is limited to a stated purpose, and establishing effective mechanisms for informing the public about privacy protections. We have also made numerous recommendations to agencies over the last several years to address weaknesses in policies and procedures related to privacy and to strengthen their information security programs.<sup>53</sup> In addition, at a July 2012 testimony before the Senate Homeland Security and Governmental Affairs committee, a law professor testified that the Congress should create a Chief Privacy Officer to coordinate privacy policy across federal agencies.<sup>54</sup>

Currently, no single federal agency has been statutorily designated with specific responsibility to regulate privacy matters relating to UAS for the entire federal government. UAS stakeholders with whom we spoke disagreed as to whether the regulation of UAS privacy-related issues should be centralized within one federal agency and, if centralized, which agency would be best positioned to handle such a responsibility. Representatives from a civil liberties organization told us that since FAA

---

<sup>52</sup>Federal agency collection or use of personal information is governed primarily by two laws: the Privacy Act of 1974 and the privacy provisions of the E-Government Act of 2002. The Privacy Act places limitations on agencies’ collection, disclosure, and use of personal information maintained in systems of records. The E-Government Act of 2002 was passed, among other reasons, to enhance the protection for personal information in government information systems or information collections by requiring that agencies conduct PIAs. PIAs are analyses of how personal information is collected, stored, shared, and managed in a federal system.

<sup>53</sup>[GAO-12-961T](#)

<sup>54</sup>Statement of Peter Swire, “*State of Federal Privacy and Data Security Law: Lagging Behind the Times?*,” Subcommittee on Oversight of Government Management, the Federal Workforce and the District of Columbia, July 31, 2012.

---

has responsibility to regulate the national airspace system, it could be positioned to handle responsibility for incorporating rules that govern UAS use and data collection. However, FAA officials and others have suggested that regulating privacy issues in connection with equipment carried on UAS, such as surveillance sensors that do not affect safety, is outside FAA's mission, which is primarily focused on aviation safety. DHS or DOJ might be better positioned to address UAS privacy issues since they generally stem from the operational uses of UAS for surveillance and law enforcement purposes. While it is not clear what entity should be responsible for addressing privacy concerns across the federal government, many stakeholders believe that there should be federal regulations for the types of allowable uses of UAS to specifically protect the privacy of individuals as well as rules for the conditions and types of data that UAS can collect. As government use of UAS is expected to increase with FAA's development of standards and rules to allow routine access to the national airspace system, the safety of personal information collected by federal agencies using UAS is an emerging issue and the government can take a number of steps to potentially address some of these privacy issues. Some stakeholders have suggested that FAA has the opportunity and responsibility to incorporate such privacy issues into the small UAS NPRM that is currently under development and in future rulemaking procedures. In addition, stakeholders we interviewed stated that developing guidelines for technology use on UAS ahead of widespread adoption by law enforcement entities could preclude abuses of the technology that could lead to a negative public perception of UAS and possibly affect their acceptance and use.

---

## GPS Jamming and Spoofing

The jamming of the GPS signal being transmitted to the UAS could also interrupt the command and control of UAS operations. In a GPS jamming scenario, the UAS could potentially lose its ability to determine its location, altitude, and the direction in which it is traveling. Low cost devices that jam GPS signals are prevalent. According to one industry expert, GPS jamming would become a larger problem if GPS is the only method for navigating a UAS. This problem can be mitigated by having a second or redundant navigation system onboard the UAS that is not reliant on GPS, which is the case with larger UAS typically operated by DOD and DHS. In addition, a number of federal UAS stakeholders we interviewed stated that GPS jamming is not an issue for the larger, military-type UAS, as they have redundant inertial navigation systems on the aircraft. A stakeholder noted that GPS jamming can be mitigated for small UAS by encrypting its communications, but the costs and weight associated with encryption may make it infeasible.



---

GPS spoofing has also been identified as an emerging issue. Encrypting civil GPS signals could make it more difficult to “spoof” or counterfeit a GPS signal that could interfere with the navigation of a UAS. Non-military GPS signals, unlike military GPS signals, are not encrypted and transparency and predictability make them vulnerable to being counterfeited, or spoofed. In a GPS-spoofing scenario, the GPS signal going from the ground control station to the UAS is first counterfeited and then overpowered. Once the authentic (original) GPS signal is overpowered, the UAS is under the control of the “spoofer.” This type of scenario was recently demonstrated by researchers at the University of Texas at Austin at the behest of DHS. During the demonstration at the White Sands Missile Range, researchers spoofed one element of the unencrypted GPS signal of a fairly sophisticated small UAS (mini-helicopter) and induced it to plummet toward the desert floor. The research team found that it was straightforward to mount an intermediate-level spoofing attack, such as controlling the altitude of the UAS, but difficult and expensive to mount a more sophisticated attack. The research team recommended that spoof-resistant navigation systems be required on UAS exceeding 18 pounds.<sup>55</sup>

---

## Conclusions

By establishing statutory requirements for FAA, Congress highlighted the importance of accelerating the safe integration of UAS into the national airspace system. However, FAA faces the daunting task of ensuring that all of the various efforts within its own agency, as well as across agencies and other entities, will align and converge in a timely fashion. The pace of progress toward UAS integration that occurred prior to the 2012 Act and questions about the agency’s ability to meet deadline requirements raise concerns about when UAS integration in the national airspace system will be achieved. Incorporating regular monitoring will help to assess progress toward goals identified in the comprehensive plan and 5-year road map that can help FAA understand what has been achieved and what remains to be done. Monitoring can also help keep Congress informed about this significant change to the domestic aviation landscape.

---

<sup>55</sup>The presentation “Assessing the Civil GPS Spoofing Threat” by Todd Humphreys, Jahshan Bhatti, Brent Ledvina, Mark Psiaki, Brady O’Hanlon, Paul Kintner, and Paul Montgomery sought to assess the spoofing threat of a small civil UAS. The team built a civilian GPS spoofer and tested some countermeasures. They concluded that GPS spoofing is a threat to communications security and civil spoofing has not been the focus of research in open literature.

---

Concerns regarding the potential security and privacy implications of UAS are growing. As the number of UAS operating in the national airspace system increases, questions about how the security of the national airspace system will be protected and how data captured by UAS will be used by governmental or commercial entities will continue to arise. Federal agencies have not yet stepped forward to proactively address these issues. This lack of activity may result from agency officials' belief that they do not have direct authority to regulate privacy issues for UAS or the current level of UAS activity in the national airspace system. However, not working to proactively address security and privacy concerns could lead to further delays in the integration of UAS into the national airspace system.

---

## Recommendations

We recommend that the Secretary of Transportation direct the FAA Administrator to incorporate, in FAA's comprehensive plan (to be completed in November 2012) and the 5-year road map for UAS integration (to be completed in February 2013), mechanisms that allow for regular monitoring to assess progress toward safe and routine access of UAS into the national airspace system.

We recommend that the Secretaries of Transportation and Homeland Security and the Attorney General initiate discussions, prior to the integration of UAS into the national airspace system, to explore whether any actions should be taken to guide the collection and use of UAS-acquired data.

---

## Agency Comments

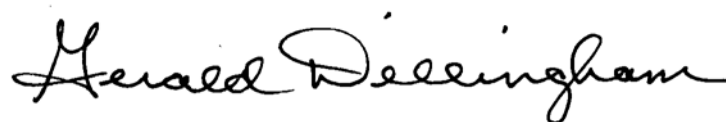
We provided a draft of this report to officials at Commerce, DHS, DOD, DOJ, DOT, and NASA. DHS and DOJ concurred with our recommendation. DOT officials agreed to consider our recommendations. DHS, DOJ, DOD and DOT provided comments that were technical or clarifying in nature, which were incorporated into the report as appropriate. NASA and Commerce had no comments on the draft report.

---

We are sending copies of this report to interested congressional committees, the Secretary of the Department of Transportation, Secretary of the Department of Homeland Security, Secretary of the Department of Commerce, Secretary of the Department of Defense, the Attorney General, and the Administrator of the National Aeronautics and Space Administration. In addition, this report will be available at no charge on GAO's Web site at <http://www.gao.gov>.

---

If you or your staff have any questions about this report, please contact me at (202) 512-2834 or [dillinghamg@gao.gov](mailto:dillinghamg@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.

A handwritten signature in black ink that reads "Gerald Dillingham". The signature is written in a cursive style with a large, prominent initial "G".

Gerald L. Dillingham, Ph.D.  
Director  
Physical Infrastructure Issues

---

*List of Congressional Committees*

The Honorable John D. Rockefeller IV  
Chairman  
The Honorable Kay Bailey Hutchison  
Ranking Member  
Committee on Commerce, Science and Transportation  
United States Senate

The Honorable John L. Mica  
Chairman  
The Honorable Nick J. Rahall II  
Ranking Member  
Committee on Transportation and Infrastructure  
House of Representatives

The Honorable Thomas E. Petri  
Chairman  
The Honorable Jerry F. Costello  
Ranking Member  
Subcommittee on Aviation  
Committee on Transportation and Infrastructure  
House of Representatives

The Honorable Michael T. McCaul  
Chairman  
Subcommittee on Oversight, Investigations, and Management  
House of Representatives

---

# Appendix I: Objectives, Scope, and Methodology

---

This report describes (1) the status of obstacles we identified in our previous report to the safe and routine integration of UAS into the national airspace system, (2) FAA's progress in complying with FAA Modernization and Reform Act of 2012 requirements, and (3) emerging issues pertaining to UAS.

To describe and assess the status of obstacles to safe integration that we previously identified, we reviewed documents provided by and interviewed officials of government, academic, and private-sector entities involved with UAS issues. We reviewed relevant GAO reports and interviewed internal stakeholders working on related engagements. We also interviewed officials at federal agencies, including the FAA's Unmanned Aircraft Systems Integration and Research and Development Offices, DOD, NASA, Department of Commerce's International Trade Administration, DHS, and the Department of Justice. We interviewed representatives from related federal advisory groups including FAA's JPDO, RTCA Special Committee 203, the Interagency Taskforce on Unmanned Systems, and the DOD's Air Force Research Lab as well as independent standards setting organizations RTCA and ASTM F38. Additionally, we interviewed representatives from universities with centers of research on UAS technology and issues, including the University of North Dakota and New Mexico State University, as well as a representative from the Mesa County, Colorado Sherriff's Office. We interviewed private sector representatives from MITRE, Rockwell Collins, and Raytheon. We interviewed representatives from the Association for Unmanned Vehicle Systems International, Aircraft Owners and Pilots Association, General Aviation Manufacturers Association, and the Airborne Law Enforcement Association. To obtain information on current civil UAS use, we obtained information from the FAA on the certificates of authority and special airworthiness certificates issued from January 2012 to July 2012.

To assess FAA's progress in meeting its reauthorization requirements and to understand UAS coordination efforts across and federal government and private stakeholder, we reviewed relevant portions of the FAA Modernization and Reform Act of 2012 and the *Federal Register*. We identified criteria for assessments from GAO's *Standards for Internal Control in the Federal Government*. We also reviewed documents provided by and conducted interviews with FAA's Unmanned Aircraft Systems Integration Office and JPDO. Additionally, we participated in several public webinars that addressed privacy concerns over non-military UAS use and FAA's request for comment on the UAS test range program.

To assess issues regarding privacy concerns over the use of UAS acquired data, we reviewed documents provided by and interviewed UAS federal, state, and local stakeholders as well as representatives from the Electronic Frontier Foundation and the American Civil Liberties Union. To obtain information about UAS security considerations, we reviewed documents from the Academy of Model Aeronautics and the Federal Law Enforcement Training Center and spoke with officials from FAA, DHS, and the Association for Unmanned Vehicles Systems International. We also examined legal requirements to which federal agencies should adhere when collecting and using personal information.

We conducted this performance audit from November 2011 through September 2012 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.

# Appendix II: Federal Entities with Certificates of Waiver or Authorization Approved from January 1, 2012, to July 13, 2012.

<b>Federal Entities with Approved COAs</b>	<b>Number of Groups within Federal Entities with COAs</b>	<b>Number of approved COAs</b>
DARPA	1	3
Department of State	1	1
Department of Homeland Security	2	17
DOD – U.S. Special Operations Command	1	32
DOD – Navy-USMC	12	18
DOD – U.S. Air Force	16	56
DOD – U.S. Army	33	54
Department of Energy – National Laboratories	2	6
Department of Justice – Federal Bureau of Investigation	1	3
Department of Interior	1	7
NASA	5	30
<b>Total Federal Entities with approved COAs between January 1, 2012 and July 13, 2012</b>	<b>75</b>	<b>227</b>

Source: GAO analysis of FAA data.

Note: Federal agencies have COAs in multiple locations across the U.S.

---

# Appendix III: GAO Contact and Staff Acknowledgments

---

## GAO Contact

Gerald L. Dillingham, Ph.D., (202) 512-2834 or [dillinghamg@gao.gov](mailto:dillinghamg@gao.gov).

---

## Staff Acknowledgments

Individuals making key contributions to this report include Maria Edelstein, Assistant Director; Amy Abramowitz; Gary Bianchi; Cristina Chaplain; Erin Cohen; Elizabeth Curda; John de Ferrari; Colin Fallon; Rebecca Gambler; Geoffrey Hamilton; David Hooper; Daniel Hoy; Joe Kirschbaum; Patricia Lentini; Brian Lepore; SaraAnn Moessbauer; Faye Morrison; Brian Mullins; Madhav Panwar; David Plocher; and Tina Won Sherman.



---

## 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 GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

---

## 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, <http://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 [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at [www.gao.gov](http://www.gao.gov).

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Katherine Siggerud, Managing Director, [siggerudk@gao.gov](mailto:siggerudk@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](mailto:youngc1@gao.gov), (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

