



January 2018

HOMELAND DEFENSE

Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft

Accessible Version

GAO Highlights

Highlights of [GAO-18-177](#), a report to congressional committees

Why GAO Did This Study

DOD has until January 1, 2020, to equip its aircraft with ADS-B Out technology that would provide DOD, FAA, and private citizens the ability to track their flights in real-time and track flight patterns over time. This technology is a component of NextGen, a broader FAA initiative that seeks to modernize the current radar-driven, ground-based air transportation system into a satellite-driven space-based system.

Senate Report 114-255 included a provision for GAO to assess the national defense implications of FAA's implementation of ADS-B. This report assesses the extent to which (1) DOD and FAA have identified operations and security risks and approved solutions to address these risks to ADS-B Out -equipped military aircraft; and (2) DOD has implemented key tasks in the 2007 memorandum on implementing NextGen.

GAO analyzed risks identified by DOD and FAA related to ADS-B vulnerabilities, and how they could affect current and future air defense and air traffic missions. GAO also reviewed the tasks in the 2007 NextGen Memorandum and assessed whether the eight tasks specifically related to ADS-B were implemented.

What GAO Recommends

GAO is recommending that DOD and FAA approve one or more solutions to address ADS-B -related security risks; and that DOD implement key tasks to facilitate consistent, long-term planning and implementation of NextGen. DOD and the Department of Transportation generally concurred and described planned actions to implement the recommendations.

View [GAO-18-177](#). For more information, contact Joseph Kirschbaum at (202) 512-9971 or kirschbaumj@gao.gov.

January 2018

HOMELAND DEFENSE

Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft

What GAO Found

Since 2008, the Department of Defense (DOD) and the Department of Transportation's Federal Aviation Administration (FAA) have identified a variety of risks related to Automatic Dependent Surveillance-Broadcast (ADS-B) Out technology that could adversely affect DOD security and missions. However, they have not approved any solutions to address these risks. Compared with other tracking technology, ADS-B Out provides more information, such as an aircraft's precise location, velocity, and airframe dimensions, and better enables real-time and historical flight tracking. Individuals—including adversaries—could track military aircraft equipped with ADS-B Out technology, presenting risks to physical security and operations. This readily available public information allowed GAO to track various kinds of military aircraft. ADS-B Out is also vulnerable to electronic warfare and cyber-attacks. Since FAA is planning to divest radars as part of ADS-B implementation, homeland defense could also be at risk, since the North American Aerospace Defense Command relies on information from FAA radars to monitor air traffic. DOD and FAA have drafted a memorandum of agreement that focuses on equipping aircraft with ADS-B Out but does not address specific security risks. Unless DOD and FAA focus on these risks and approve one or more solutions in a timely manner, they may not have time to plan and execute actions that may be needed before January 1, 2020—when all aircraft are required to be equipped with ADS-B Out technology.

Of the eight tasks associated with the implementation of ADS-B Out technology in the 2007 DOD NextGen memorandum—issued by the Deputy Secretary of Defense to ensure that the NextGen vision for the future national airspace system met DOD's requirements and the appropriate management of DOD's resources—DOD has implemented two, has partially implemented four, and has not implemented two. DOD has established a joint program office and identified a lead service, but it has only partially validated ADS-B Out requirements, developed a directive, issued an implementation plan, and incorporated NextGen into the planning, budgeting, and programming process. DOD has not taken significant action to integrate the needs and requirements of DOD components related to ADS-B into cohesive plans and policies for inclusion in NextGen joint planning and development, and has not provided periodic and recurring NextGen progress reports to the Deputy Secretary of Defense. As a result of DOD not fully implementing the 2007 NextGen memorandum, DOD components have lacked direction and cohesion while trying to address FAA's requirement to equip military aircraft.

This is a public version of a classified report GAO issued in January 2018.

Contents

Letter	1
Background	4
DOD and FAA Have Identified Security and Mission Risks Related to ADS-B Out Technology but Have Not Approved Any Solutions to Mitigate Them	12
DOD Has Achieved Mixed Implementation of Key ADS-B Tasks Directed in 2007	20
Conclusions	26
Recommendations for Executive Action	27
Agency Comments and Our Evaluation	27
<hr/>	
Appendix I: Objectives, Scope, and Methodology	31
Appendix II: Comments from the Department of Defense	35
Appendix III: Comments from the Department of Transportation	38
Appendix IV: GAO Contact and Staff Acknowledgments	39
Appendix V: Accessible Data	40
Agency Comment Letters	40
<hr/>	
Related GAO Products	45
<hr/>	
Tables	
Table 1: Key Data Fields for Aircraft Identification and Tracking in Aircraft Broadcast Systems	7
Table 2: Selected Roles and Responsibilities for Next Generation Air Transportation System (NextGen) Stakeholders	12
Table 3: Organizations and Offices We Visited or Contacted	32

Abbreviations

ADS-B	Automatic Dependent Surveillance-Broadcast
DOD	Department of Defense
FAA	Federal Aviation Administration
GPS	Global Positioning System
ICAO	International Civil Aviation Organization
NextGen	Next Generation Air Transportation System
NORAD	North American Aerospace Defense Command

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.



January 18, 2018

Congressional Committees

In 2010, the Federal Aviation Administration (FAA) issued a final rule that requires all aircraft—including military aircraft—flying in specified airspace within the national airspace system as of January 1, 2020, to be equipped with technology that would transmit flight information to an enabled receiver.¹ This technology—known as Automatic Dependent Surveillance-Broadcast (ADS-B) Out—is a key component of the FAA’s Next Generation Air Transportation System (NextGen), which seeks to modernize the current ground-based radar system to a satellite-derived system for automated aircraft position reporting, navigation, and digital communications.² ADS-B Out uses an aircraft’s avionics equipment to broadcast the aircraft’s position, altitude, and velocity to any ground, air, or space-based receiver.

Over the years, the Department of Defense (DOD) has expressed concern about the operations security risk of openly transmitting flight data from military aircraft. For example, in DOD’s 2008 comments about FAA’s draft rule requiring ADS-B Out technology, the department informed FAA that it was possible to identify and potentially compromise DOD aircraft conducting sensitive missions in the United States due to ADS-B Out technology.³ The North American Aerospace Defense Command (NORAD) and DOD have also expressed concerns about the FAA’s plan to decommission FAA legacy radar systems on which NORAD relies to conduct aerospace warning and aerospace control missions, and

¹See 14 C.F.R. §§ 91.225 and 91.227.

²For more information, see GAO, Next Generation Air Transportation System: Information on Expenditures, Schedule, and Cost Estimates, Fiscal Years 2004 — 2030, [GAO-17-241R](#) (Washington, D.C.: Nov. 17, 2016).

³Department of Defense, *DOD Policy Board on Federal Aviation, DOD Comments to Docket No. FAA-2007-29305; Notice No. 07-15, Automatic Dependent Surveillance – Broadcast (ADS-B) Out Performance Requirements to Support ATC Service* (Feb. 29, 2008).

on which DOD relies to conduct its air traffic missions.⁴ In addition, a number of assessments conducted by DOD, FAA, and others have identified security concerns inherent in ADS-B Out technology that could leave aircraft, tactical air traffic control systems, and FAA radars vulnerable to electronic warfare- and cyber-attacks by individuals, groups, or nation-state actors (hereinafter referred to as “adversaries”) and other types of interference.⁵ In addition, according to these assessments, adversaries could create false signals (that is, “spoofing”) or jam signals from ADS-B Out technology to obscure air traffic control and surveillance visibility.⁶

Recognizing the importance of participating in the NextGen interagency partnership, the Deputy Secretary of Defense issued a memorandum in 2007 designating the Air Force as the lead service responsible for representing DOD in the partnership, including leading and coordinating associated efforts across the department.⁷ In addition, the memorandum identified key tasks to help ensure and enhance the department’s ability to operate seamlessly with civil aviation in both national and international airspace.

Senate Report 114-255, accompanying a bill for the National Defense Authorization Act of Fiscal Year 2017, included a provision that we assess the national defense implications of FAA’s implementation of

⁴NORAD is a U.S. and Canadian bi-national organization charged with the missions of aerospace warning, aerospace control, and maritime warning for North America. Aerospace warning includes the detection, validation, and warning of attack against North America, whether by aircraft, missiles, or space vehicles, through mutual support arrangements with other commands and agencies. Aerospace control includes ensuring air sovereignty and air defense of the airspace of Canada and the United States against aircraft and cruise missiles. Maritime warning consists of processing, assessing, and disseminating intelligence and information related to the respective maritime approaches to the United States and Canada.

⁵Cyber-attacks are offensive cyberspace operations, which DOD defines as operations intended to project power by the application of force in or through cyberspace, leveraging platforms such as information technology systems, such as infrastructure, data, networks, computer systems, and the Internet. DOD defines an electronic attack as a division of electronic warfare involving the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability.

⁶Spoofing refers to the generation of ghost tracks of fake aircraft that can confuse air traffic control and compromise safety.

⁷Deputy Secretary of Defense Memorandum, *Implementation of the Next Generation Air Transportation System within the Department of Defense*, (Dec. 28, 2007).

ADS-B as part of the agency's NextGen modernization effort.⁸ This report assesses the extent to which (1) DOD and FAA have identified security and operations risks and approved solutions to address these risks to military aircraft equipped with ADS-B Out technology; and (2) DOD has implemented key tasks in the 2007 Deputy Secretary of Defense memorandum on implementing NextGen (hereinafter referred to as the 2007 NextGen memorandum).⁹ This is a public version of a classified report that we issued in January 2018.¹⁰ This report does not identify specific classified details of DOD assessments, security risks, and other actions DOD is taking to address security risks related to ADS-B Out or the NextGen system that DOD deemed to be sensitive. Although the information provided in this report is less detailed, it addresses the same objectives as our classified report. In addition, the overall methodology used for both reports is the same.

To assess the extent to which DOD and FAA have identified risks and approved solutions to address these risks to military aircraft equipped with ADS-B Out technology, we reviewed policies, procedures, guidance, assessments, and other relevant documents from NORAD, DOD, and FAA. These documents address ADS-B implementation, acquisition, operations, cybersecurity, risk management and mitigation, and any other issues that may be pertinent to identifying and addressing operations and security risks resulting from ADS-B. We also reviewed publicly available literature discussing potential ADS-B cybersecurity vulnerabilities. We interviewed officials from NORAD, DOD, and FAA about potential risks, vulnerabilities, and mitigation strategies. We also reviewed classified intelligence reports that assessed the vulnerabilities of ADS-B technology. While military aircraft and existing radar systems may be equipped with other devices (such as Mode S transponders) that could also pose security risks, this report focused primarily on risks and potential solutions associated with ADS-B Out technology that FAA mandated DOD to install

⁸S. Rep. No. 114-255, at 287-288 (2016).

⁹This report focuses on the ADS-B Out requirement when referencing ADS-B technology unless otherwise noted. As discussed later in the report, ADS-B technology also includes technology related to the enabled receivers.

¹⁰GAO, *Homeland Defense: Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft*, GAO-17-176C (Washington, D.C.: Jan. 18, 2018).

on its aircraft by January 1, 2020.¹¹ To understand DOD and FAA coordination, we reviewed laws, guidance, and directives related to agency cooperation for the NextGen system and implementation of ADS-B technology. This included the 2010 FAA final rule published in the Federal Register that provided guidelines and requirements for coordination between agencies and the 2007 NextGen memorandum on implementing NextGen.

To assess the extent to which DOD has implemented key tasks in the 2007 NextGen memorandum, we compared the actions taken, if any, to implement eight tasks directed by the Deputy Secretary of Defense. We selected these eight from the list of twenty tasks in the memorandum. We selected these eight tasks because, if completed, these eight tasks would be significant to the development of plans and policies related to the implementation of the FAA's ADS-B Out technology requirement. To evaluate completion of the selected tasks, we reviewed documents and interviewed DOD officials to determine the degree to which DOD has implemented the tasks identified by the 2007 NextGen memorandum.¹² Further details on our scope and methodology can be found in appendix I.

We conducted this performance audit from June 2016 to January 2018 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.

Background

FAA Next Generation Air Transportation System

In December 2003 Congress enacted the Century of Aviation Reauthorization Act, laying the foundation for NextGen.¹³ The intent of

¹¹See 14 C.F.R. §§ 91.225 and 91.227, which requires all aircraft operating in certain designated airspace to be equipped with ADS-B Out by Jan. 1, 2020, unless otherwise authorized by air traffic control.

¹²Deputy Secretary of Defense Memorandum, *Implementation of the Next Generation Air Transportation System within the Department of Defense* (Dec. 28, 2007).

¹³Pub. L. No. 108-176, 117 Stat. 2490 (2003).

NextGen is to increase air transportation-system capacity, enhance airspace safety, reduce delays experienced by airlines and passengers, lower fuel consumption, and lessen adverse environmental effects from aviation, among other benefits. This effort is a multi-year, incrementally iterative transformation that will introduce new technologies and leverage existing technologies to affect every part of the national airspace system. These new technologies will use an Internet Protocol-based network to communicate.¹⁴ NextGen consists of components that provide digital communications between controllers and pilots, and that also use satellite-based surveillance to aid in airspace navigation. Because of these new communication methods, NextGen increases reliance on integrated information systems and distribution of information, digital communication methods, and global positioning system (GPS) technology that may put the air traffic control system at greater risk for intentional or unintentional information-system failures and breaches. We have previously reported on progress that FAA has made in implementing NextGen.¹⁵ For example, in 2015 we found that FAA faces cybersecurity challenges in at least three areas: (1) protecting air-traffic control information systems, (2) protecting aircraft avionics used to operate and guide aircraft, and (3) clarifying cybersecurity roles and responsibilities among multiple FAA offices.¹⁶ Among other recommendations, we recommended—and FAA concurred—that the agency should assess developing a cybersecurity threat model.

Evolution of Tracking Military Aircraft in the National Airspace

Historically, FAA and DOD capabilities have allowed both agencies—as well as NORAD—to monitor and track military aircraft flying in the national airspace. For example, FAA maintains two layers of radar—primary surveillance radar and secondary surveillance radar—to track and identify aircraft flying in the national airspace system. Primary surveillance radar

¹⁴Internet Protocol, the principal communication protocol on which the Internet is based, is a networking technology that has been the industry's standard method to network computer systems since the late 1990s.

¹⁵For example, see GAO, *Air Traffic Control: FAA Needs a More Comprehensive Approach to Address Cybersecurity as Agency Transitions to NextGen*, [GAO-15-370](#) (Washington, D.C.: Apr. 14, 2015). The Related GAO Products page includes other reports about NextGen.

¹⁶[GAO-15-370](#).

identifies the location of aircraft flying in the national airspace by transmitting a signal and calculating the amount of time that passes until that signal bounces off the aircraft and returns to the radar. FAA also uses secondary surveillance radar that transmits an interrogation signal to aircraft flying in the national airspace. A receiver on the aircraft receives the interrogation signal and then transmits a broadcast back to this radar with flight information.¹⁷ Table 1 shows the evolution and capabilities of different transponders that broadcast aircraft information to receivers.¹⁸ The fields identified in the table are critical for identifying and tracking aircraft. Of the different transponder modes and technology, ADS-B Out provides the most precise and comprehensive data. ADS-B Out makes it easier for third parties to identify and track aircraft, as ADS-B Out broadcasts include registration number, precise location, aircraft dimensions, and other information. This additional information reduces the need to identify aircraft using private databases and to determine aircraft location by comparing time difference of arrival among receivers.

¹⁷Some Mode S transponders provide information autonomously even if they do not receive an interrogation signal from secondary-surveillance radar.

¹⁸Mode S and ADS-B Out broadcast could also include additional information about the aircraft, such as its emergency status.

Table 1: Key Data Fields for Aircraft Identification and Tracking in Aircraft Broadcast Systems

Key Data Fields for Aircraft Identification and Tracking in Aircraft Broadcast Systems			
System	Modes 3/A ^a and Mode C	Mode S ^b	ADS-B Out
Era used	1963 to present	1984 to present	Mandated by Jan 1, 2020
Squawk code ^c	Information Available	Information Available	Information Available
Barometric altitude	Mode C only	Information Available	Information Available
File information Not Available address	INFORMATION NOT AVAILABLE	Information Available	Information Available
Registration number	INFORMATION NOT AVAILABLE	INFORMATION NOT AVAILABLE	Information Available
Latitude / longitude	INFORMATION NOT AVAILABLE	INFORMATION NOT AVAILABLE	Information Available
Geometric altitude	INFORMATION NOT AVAILABLE	INFORMATION NOT AVAILABLE	Information Available
Aircraft dimensions	INFORMATION NOT AVAILABLE	INFORMATION NOT AVAILABLE	Information Available

Legend:

ADS-B Out = Automatic Dependent Surveillance-Broadcast Out technology

✓ = Information that is made publicly available by the aircraft broadcast system

x = Information that either is not transmitted or is not made publicly available by the aircraft broadcast system

Source: Federal Aviation Administration. | GAO-18-177

^aMode 3/A is a combined reference to both Mode A (civilian mode) and Mode 3 (military-defined mode). According to DOD and FAA officials, both of these modes are the same and provide the same type of information – the squawk code.

^bIn addition, Mode S can provide additional data that may be valuable for identifying and tracking aircraft, such as the aircraft registration number. While Mode S broadcasts do not always include an aircraft’s registration number, according to FAA officials, some FAA Mode S systems query aircraft registration numbers and some Mode S transponders provide registration numbers.

^cSquawk code: A temporary four-digit transmit code assigned by air traffic control that facilitates aircraft tracking during a single flight.

Mode 3/A and Mode C Transponders

The content of these aircraft broadcasts varies depending on the type of transmitter providing the information from the aircraft. For example, earlier broadcast systems, including the Mode 3/A and Mode C systems, transmit a temporary four-digit transmit code (commonly referred to as a squawk code) assigned by air traffic control that facilitates aircraft tracking

during a single flight.¹⁹ Since FAA was the sole source of flight data for systems preceding Mode S, the agency could filter out military aircraft flight information for security reasons before providing information to the public about other aircraft flying in the national airspace.

Mode S Transponder

Mode S transponders provide more information than do the Mode 3/A and Mode C transponders. For example, the Mode S transponder broadcast identifies an aircraft-specific, 24-bit fixed address (commonly known as the ICAO address) assigned under International Civil Aviation Organization (ICAO) standards. An aircraft retains this fixed address based on its registration, and thereby facilitates aircraft identification until the aircraft is reregistered and receives a new ICAO address.

FAA and aviation groups have reported that with the proliferation of commercial and amateur receivers, the public can now track individual aircraft by receiving the aircraft's ICAO address, squawk code, and altitude. In addition, these entities have reported that since aviation groups and hobbyists have connected the receivers, the networked receivers can calculate and identify the latitude and longitude of the aircraft they are tracking. In addition, according to these reports, some groups maintain aircraft information databases and receiver networks that can identify aircraft by ICAO address and can locate aircraft by comparing the time difference of arrival of Mode S signals between three or more receivers.²⁰ Using data derived from this work, interested parties—including adversaries (for example, foreign intelligence entities, terrorists, and criminals)—can identify military aircraft by type and registration number, and can track the aircraft while in flight through Mode S fixed address broadcasts. Using this readily available public information, we were able to track various kinds of military aircraft that were equipped with Mode S transponders.

¹⁹Mode 3/A is a combined reference to both Mode A (civilian mode) and Mode 3 (military-defined mode). According to DOD and FAA officials, both of these modes are the same and provide the same type of information – the squawk code. Consequently, throughout the report, we refer to both of these modes as Mode 3/A.

²⁰Measuring the timing of broadcasts received at multiple locations and, thereby, measuring position is referred to as multilateration.

ADS-B Technology

ADS-B consists of two distinct aircraft information services, ADS-B Out and ADS-B In. As previously stated, ADS-B Out technology is one of the main components of FAA's NextGen effort. It is a performance-based surveillance technology using GPS-enabled satellites to produce flight information, such as an aircraft's location and velocity, and according to FAA, it is more precise than radar.²¹ These precise data provide air traffic controllers and pilots with more accurate information to keep aircraft safely separated in the national airspace. This technology combines aircraft avionics, a positioning capability, and ground infrastructure to enable accurate transmission of information from aircraft to the air traffic control system. This technology periodically transmits information without a pilot or operator involved (that is, Automatic); collects information from GPS or other suitable navigation systems (that is, Dependent); provides a method of determining 3-dimensional position and identification of aircraft, vehicles, or other assets (that is, Surveillance); and transmits the information available to anyone with the appropriate receiving equipment (that is, Broadcast). Using this readily available public information, we were able to track various kinds of military aircraft that were equipped with ADS-B transponders. ADS-B In is the technology that enables receivers to have direct access to information broadcasted through ADS-B Out transponders.

FAA's final rule requiring all aircraft that fly in certain categories of airspace to equip with ADS-B by January 1, 2020, applies to the ADS-B Out technology.²² FAA has not issued a rule or requirement for aircraft to equip with the ADS-B In technology, as of July 2017. However, according to representatives from Airlines for America, an airline industry advocacy organization, airlines have begun to install the ADS-B In capability on commercial aircraft due to the benefits they anticipate from the capability (for example, the ability of passenger airliners to reduce separation standards to save time and reduce fuel consumption). In addition, according to Air Force officials, the Air Force plans to install ADS-B In on future KC-46 transport/tanker aircraft. This report focuses on the ADS-B Out requirement when referencing ADS-B technology unless otherwise noted.

²¹See Federal Register, Vol. 75, No. 103, at 30161 (May 28, 2010).

²²See 14 C.F.R. §§ 91.225 and 91.227.

According to DOD and FAA documents and officials, FAA has identified ADS-B implementation as providing an opportunity to save costs by divesting a number of secondary-surveillance radars. According to FAA officials, as of April 2017 the agency was re-evaluating its original ADS-B backup strategy and the need for retaining additional secondary-surveillance radars. According to these officials, FAA plans to maintain all high-altitude secondary-surveillance radars and the low-altitude secondary-surveillance radars around 30 or more of the busiest airports.²³

Relationship between FAA and DOD in Managing National Airspace

The FAA and DOD are to cooperate in order to regulate airspace use. Specifically, the FAA is responsible for providing air navigation services, including air traffic control across most of the United States, and is leading the overall NextGen efforts in the United States. The FAA's air traffic control system works to prevent collisions involving aircraft operating in the national airspace system, while also facilitating the flow of air traffic and supporting national security and homeland defense missions. In addition, in accordance with International Civil Aviation Organization guidelines, the FAA has categorized airspace as controlled, uncontrolled, or not used in the United States. According to the ADS-B Out rule, after January 1, 2020, no person may operate an aircraft in certain categories of airspace defined by the rule unless otherwise authorized by air traffic control authorities.²⁴

DOD conducts its missions within the national airspace system as both an aircraft operator and, as delegated by the FAA, as provider of air traffic control and other air navigation services. DOD has the authority to certify its own aircraft, manage airspace, and provide air traffic control-related services in accordance with FAA requirements.²⁵ DOD also provides guidance to FAA concerning security matters pertaining to the national airspace system. DOD is responsible for ensuring that DOD components,

²³En route secondary-surveillance radars are used to track aircraft between airports, whereas terminal secondary-surveillance radars are used for aircraft landing and taking off from airports.

²⁴Each person operating an aircraft equipped with ADS-B Out must operate this equipment in the transmit mode at all times. See 14 C.F.R. §§ 91.225(f).

²⁵Deputy Secretary of Defense Memorandum, *Implementation of the Next Generation Air Transportation System within the Department of Defense* (Dec. 28, 2007).

such as the military services, have sufficient access to airspace to meet security requirements, and that civilian and military aircraft can operate safely both domestically and abroad. DOD also releases airspace to the FAA when it does not need the space for military purposes.

The FAA also works with DOD to ensure aviation safety between civil and military aircraft. The FAA designates airspace over certain parts of the United States as Special Use Airspace, because the areas may have prohibited airspace, restricted airspace, warning areas, or alert areas. It might be hazardous for civil aircraft to operate in that restricted airspace due to these designations. Special Use Airspace allows military aircraft to operate safely in separate, clearly defined airspace in order to conduct missions in support of the National Security Strategy and the National Military Strategy.²⁶ The FAA also issues safety briefings that could identify military-protected, temporarily flight-restricted areas, to prevent civil pilots from flying into the airspace. These briefings also include information such as flight safety advice and information on air traffic technology, such as ADS-B. The FAA also shares radar information with NORAD to support the defense of North America over areas such as the National Capital Region surrounding Washington, D.C.

Roles and Responsibilities

The FAA is responsible for providing airspace navigation services within the United States and has a particular entity—the FAA Office of NextGen—that directs its NextGen requirements. In 2007 the Deputy Secretary of Defense designated the Air Force as the lead service for representing DOD and for leading and coordinating efforts across DOD.²⁷ To accomplish this responsibility, the Air Force established a Lead Service Office, hereinafter referred to as the DOD Lead Service Office. These and numerous other entities have a role in implementing NextGen and ADS-B, as shown in table 2 below.

²⁶The White House, *National Security Strategy* (Washington, D.C.: February 2015); and The Joint Chiefs of Staff, *The National Military Strategy of the United States of America: The United States Military's Contribution to National Security* (June 2015).

²⁷Deputy Secretary of Defense Memorandum, *Implementation of the Next Generation Air Transportation System within the Department of Defense* (Dec. 28, 2007).

Table 2: Selected Roles and Responsibilities for Next Generation Air Transportation System (NextGen) Stakeholders

Organization or Agency	Component	Responsibility
North American Aerospace Defense Command		A bi-national security organization chaired by both the United States and Canada and responsible for aerospace warning and aerospace control of North America. Provides representatives to the Policy Board on Federal Aviation.
Department of Defense (DOD)	Under Secretary of Defense for Acquisition, Technology, and Logistics	Provides policy guidance and oversight of DOD interactions with the Federal Aviation Administration (FAA) on all national airspace system matters for the Secretary of Defense except for those specifically assigned to the Secretary of the Air Force in the 2007 Next Generation Air Transportation System (NextGen) memorandum.
	Air Force	Acts as lead service for DOD's implementation of NextGen, including the requirements to install Automatic Dependent Surveillance-Broadcast (ADS-B) technology on DOD aircraft. Established a DOD Lead Service Office to execute the role of the Secretary of Air Force as the lead service.
	Military Services	Coordinate with the lead service on NextGen programs they agree to support and fund procurement of these programs through services' annual program objective memorandum process.
	Policy Board on Federal Aviation	Senior Advisory Group to the DOD Lead Service Office and DOD to synchronize DOD-wide policies and decisions concerning NextGen.
Transportation	FAA	Manages the control and use of navigable airspace within the United States.
	FAA Office of NextGen	Coordinates NextGen initiatives, programs and policy developments for the FAA.
	FAA Interagency Planning Office	Leads interagency and international collaboration to resolve complex challenges critical to NextGen. Additionally, the Interagency Planning Office leverages stakeholder expertise to identify, research, coordinate, and prioritize shared issues, and bring the appropriate resources together to advance NextGen.
	NextGen Advisory Committee	Facilitates and coordinates the exchange of information on NextGen between the government and non-governmental (e.g., private-sector companies and airport authorities) stakeholders.

Source: Department of Defense and Department of Transportation. | GAO-18-177

DOD and FAA Have Identified Security and Mission Risks Related to ADS-B Out Technology but Have Not Approved Any Solutions to Mitigate Them

Since 2008, DOD and FAA have identified a variety of ADS-B- related risks that could adversely affect military security and missions. While DOD and FAA have identified some potential mitigations for these risks, the departments have not approved any solutions.

DOD and FAA Have Identified Risks to DOD Security and Missions Related to ADS-B Technology

Documents we reviewed and officials we met with identified a variety of operations and physical security risks that could adversely affect DOD missions. These risks arise from information broadcast by ADS-B itself, as well as from potential ADS-B vulnerabilities to electronic warfare- and cyber-attacks, and from the potential divestment of secondary-surveillance radars.²⁸

ADS-B Information Presents Operations and Physical Security Risks

Information broadcasted from ADS-B transponders poses an operations security risk for military aircraft.²⁹ For example, a 2015 assessment that RAND conducted on behalf of the U.S. Air Force stated that the broadcasting of detailed and unencrypted position data for fighter aircraft, in particular for a stealth aircraft such as the F-22, may present an operations security risk.³⁰ The report noted that information about the F-22's precise position is classified Secret, which means that unauthorized disclosure of this information could reasonably be expected to cause serious damage to the national security. Similarly, in 2012 MITRE issued a report on behalf of the DOD Lead Service Office that identified a number of risks—including the ability to track movement in and out of restricted airspaces and changes in operations—to ADS-B-equipped aircraft.

In addition to these documents, DOD officials identified a number of increased operations and physical security risks associated with aircraft

²⁸DOD defines an electronic attack as a division of electronic warfare involving the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability.

²⁹An operations security (commonly referred to as "OPSEC") risk includes actions that can be observed by adversary intelligence systems or indicators and vulnerabilities that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

³⁰RAND, *Ensuring Readiness in NextGen: Assessment of ADS-B Out Surveillance Modernization for Trainers and Fighters*, (Santa Monica, CA: May 2015).

equipped with ADS-B technology.³¹ In DOD's 2008 comments about FAA's draft rule requiring ADS-B Out technology, the department informed FAA that DOD aircraft could be identified conducting special flights for sensitive missions in the United States and potentially compromised due to ADS-B technology.³² Such sensitive missions could include low-observable surveillance, combat air patrol, counter-drug, counter-terrorism, and key personnel transport. While some military aircraft are currently equipped with Mode S transponders that provide individuals who have tracking technology the altitude of the aircraft, ADS-B poses an increased risk. Specifically, according to documents we reviewed and officials we met with, a confluence of the following three issues has led to ADS-B technology presenting more risks to DOD aircraft, personnel, equipment, and operations:

- **Additional information.** The additional information provided through ADS-B technology—including the aircraft's precise location, velocity, and airframe dimensions—increases both direct physical risks to DOD aircraft, personnel, and equipment, and long-term risks to DOD air operations.
- **Accessibility of information.** ADS-B technology also introduces risks to aircraft, personnel, equipment, and operations, because it provides information to the public that was not previously accessible. FAA filters information about DOD's flights so that the information is not available to the public via any FAA data feed. According to FAA officials, this filtering was effective for protecting such information for Mode-S equipped DOD aircraft until the 2012 timeframe, when the capability of third-party networked receivers started to allow position determination for such aircraft. With ADS-B, aircraft location and other information is broadcast from the aircraft, where FAA cannot filter it. While individuals and groups could obtain additional information about DOD flights operating with Mode S, such as an aircraft's fixed address, information such as geographic location and velocity was not

³¹DOD defines physical security as "that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, materiel, and documents; and to safeguard them against espionage, sabotage, damage, and theft." See *DOD Dictionary of Military and Associated Terms* (as of June 2017).

³²Department of Defense, DOD Policy Board on Federal Aviation, DOD Comments to Docket No. FAA-2007-29305; Notice No. 07-15, "Automatic Dependent Surveillance – Broadcast (ADS-B) Out Performance Requirements to Support ATC Service" (Feb. 29, 2008).

included in broadcasts. Individuals could estimate location and velocity of DOD flights by locating the signal through privately owned receiver networks. By equipping military aircraft with ADS-B technology, individuals and groups would receive additional identifiers, location information, and airframe information through aircraft broadcasts and, as a result, could identify and track aircraft without the use of fixed address databases and with less receiver infrastructure.

- **Historical data.** ADS-B technology better enables individuals and groups to track flights in real time and use computer programs to log ADS-B transmissions over time. Therefore, individuals or groups could observe flight paths in detail, identify patterns-of-life, or counter or exploit DOD operations.

ADS-B Could Affect Current and Future Air Defense and Air Traffic Missions

While NORAD and DOD officials told us that they will benefit from information provided by ADS-B technology, NORAD, DOD, and professional organizations' documents and officials also noted that electronic warfare- and cyber-attacks—and the potential divestment of secondary-surveillance radars as a result of reliance on ADS-B—could adversely affect current and future air operations.³³

For example, a 2015 Institute of Electrical and Electronics Engineers article about ADS-B stated that ADS-B is vulnerable to an electronic-warfare attack—such as a jamming attack—whereby an adversary can effectively disable the sending and receiving of messages between an ADS-B transmitter and receiver by transmitting a higher power signal on the ADS-B frequencies.³⁴ The article notes that while jamming is a problem common to all wireless communication, the effect is severe in

³³NORAD and DOD entities that make use of ADS-B data will have more accurate information about aircraft positions, speed, velocity, and other information to make more informed decisions. FAA is providing NORAD and 10 DOD sites with information collected from ADS-B transponders. According to FAA, DOD has not requested information for additional sites.

³⁴Martin Strohmeier, Vincent Lenders, and Ivan Martinovic, "On the Security of the Automatic Dependent Surveillance-Broadcast Protocol," *IEEE Communications Surveys & Tutorials* 17, no. 2 (2015): 1066-1087. According to the Institute of Electrical and Electronics Engineers internet site, the institute is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity. GAO did not independently validate the details and conclusions in the article.

aviation due to the system's inherently wide-open spaces, which are impossible to control, as well as to the importance and criticality of the transmitted data. As a stand-alone method, jamming could create problems within the national airspace. Jamming can also be used to initiate a cyber-attack on aircraft or ADS-B systems. According to the article in the 2015 Institute of Electrical and Electronics Engineers publication, adversaries could use a cyber-attack to inject false ADS-B messages (that is, create "ghost" aircraft on the ground or air); delete ADS-B messages (that is, make an aircraft disappear from the air traffic controller screens); and modify messages (that is, change the reported path of the aircraft). The article states that jamming attacks against ADS-B systems would be simple, and that ADS-B data do not include verification measures to filter out false messages, such as those used in spoofing attacks.

FAA officials stated that the agency is aware of these possible attacks, and that it addresses such vulnerabilities by validating ADS-B data against primary- and secondary-surveillance radar tracks. Both FAA and DOD have identified a potential solution to address this vulnerability. However, this solution has not been tested and as of November 2017, no testing has been scheduled.

In addition to electronic warfare- and cyber-attacks, both NORAD and DOD officials expressed concerns that the air defense and military air traffic control missions would be affected if FAA were to divest secondary-surveillance radars following ADS-B implementation. According to DOD and FAA documents and officials, FAA has identified ADS-B implementation as an opportunity to save costs by divesting a number of secondary-surveillance radars. However, according to NORAD and DOD officials, in those locations where FAA divests of radars, the missions would be at higher risk if an aircraft operator were to turn off the aircraft's ADS-B technology; if an adversary were to conduct an electronic or cyber-attack on the ADS-B system; or if the ADS-B system were to experience a technical failure.

According to NORAD command officials, the command relies on information from FAA radars to monitor air traffic in the national airspace system. If an aircraft is operating without ADS-B, if a GPS or ADS-B system fails, or if an adversary has jammed an aircraft's GPS signal or ADS-B transmissions, then the command will have to rely on primary- and secondary-surveillance radar to track the aircraft's location.

FAA officials stated that FAA is chiefly responsible for air safety, while NORAD and DOD are chiefly responsible for air defense, and that they believe there will be sufficient radar coverage for DOD to conduct its missions. FAA officials stated that they will maintain sufficient backup systems to ensure air traffic safety for all flights, and will maintain radar in excess of their needs to support NORAD's missions. FAA officials stated that they will maintain all primary-surveillance radar, all high-altitude secondary-surveillance radar, and low-altitude secondary-surveillance radar near at least thirty major flight terminals. However, according to NORAD and DOD officials, FAA has not proposed an updated legacy primary- and secondary-surveillance radar divestment plan since 2012 for use by NORAD and DOD in assessing potential effects on the mission. NORAD is a bi-national command that requires support from U.S. federal agencies—not just DOD—and relies on FAA radar to support its mission, and it will need to ensure that sufficient air surveillance resources are in place.

DOD and FAA Have Not Approved Any Solutions to Address ADS-B Risks

Although DOD, FAA, and other organizations have identified risks to military security and missions since 2008, DOD and FAA have not approved any solutions to address these risks. This is because DOD and FAA have focused on equipping military aircraft with ADS-B technology and have not focused on solving or mitigating security risks from ADS-B. The approach being taken by FAA and DOD will not address key security risks that have been identified, and delays in producing an interagency agreement have significantly reduced the time available to implement any agreed-upon solutions before January 1, 2020, when the full deployment of ADS-B Out is required. Federal internal control standards state that federal agencies should make risk-based decisions in a timely manner. Specifically, OMB Circular A-123 states that management should evaluate and document internal control issues and determine appropriate corrective actions for internal control deficiencies on a timely basis.³⁵ In the case of equipping military aircraft with ADS-B technology and addressing any risks associated with it, DOD and FAA have shared responsibility.

³⁵Office of Management and Budget, Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (Washington, D.C.: July 15, 2016).

In 2008 DOD informed FAA that military aircraft would need special accommodations to the ADS-B Out rule due to national security concerns, such as sensitive missions and electronic warfare vulnerabilities.³⁶ In 2010 FAA responded to DOD's comments to the draft ADS-B Out rule stating that the agency would collaborate with departments or agencies, including DOD and the Department of Homeland Security, to develop memorandums of agreement to accommodate their national defense mission requirements while supporting the needs of all other national airspace system users.³⁷ Since that time, DOD components have identified actions that could mitigate some of the risks. For example, DOD and others have identified such mitigations as masking DOD aircraft identifiers, maintaining current inventory of primary-surveillance radars, allowing pilots to turn off ADS-B broadcasts, and seeking an exemption from installing ADS-B technology on select military aircraft (for example, fighter and bomber aircraft). However, as of June 2017—almost 7 years after FAA acknowledged that it would address DOD's concerns (and less than 3 years before full deployment of ADS-B Out is required)—DOD and FAA have not approved any solutions to these risks. The DOD's Lead Service Office and FAA have focused on developing a memorandum of agreement that they hope will create a framework for future collaboration at the local level. However, our work and that of NORAD and other DOD components identified a number of limitations to DOD's Lead Service Office and FAA's dependence on this draft memorandum of agreement. For example, the draft memorandum does not address the following:

- the details necessary to establish solutions or mitigations between DOD and FAA for identified security risks. The draft memorandum focuses on equipage of ADS-B technology on military aircraft, cost estimates, and agency and office responsibilities. DOD acknowledges that it will equip military aircraft with ADS-B technology and operate to the greatest extent possible by the January 1, 2020, compliance date. However, the draft memorandum does not identify solutions for the identified operations and physical security risks.
- the electronic warfare and cyber-attack concerns and the effect on sensitive defense missions that DOD has identified.

³⁶DOD Comments to Docket No. FAA-2007-29305; Notice No. 07-15, "Automatic Dependent Surveillance – Broadcast (ADS-B) Out Performance Requirements to Support ATC Service."

³⁷Federal Register, Vol. 75, No. 103, at 30169 (May 28, 2010).

- the flexibility required by NORAD to support freedom of movement within the continental United States, Alaska, and Canada airspace for military missions. The draft memorandum would place negotiating accommodations for NORAD's bi-national mission at the local level—an act that NORAD officials characterized as unfeasible because military aircraft supporting NORAD missions require uninhibited airspace access throughout the United States and Canada, as a response may be required anywhere and at any time. According to NORAD officials, the command would incur a significant burden to finalize memorandums of agreement with more than 600 air traffic control facilities and ensure commonality with all facilities in the continental United States and Alaska. Furthermore, NORAD officials stated that these missions should not be limited by local restrictions created by the ADS-B Out rule. For example, DOD aircraft flying over one state while supporting an Operation Noble Eagle mission could be stationed at a military base in another state and thus not have an agreement with local FAA controllers.
- potential mission risks associated with the divestment of secondary-surveillance radars.

Delays in the completion of a memorandum of agreement have exacerbated uncertainty as to whether security issues will be addressed in any manner. DOD and FAA have met to discuss the existing draft memorandum of agreement since December 2016. In April 2017 officials from DOD Lead Service Office told us that they expected DOD and FAA to finalize the memorandum of agreement by June 2017; however, in May 2017 DOD officials informed us that the estimated completion date had slipped to February 2018.

A significant amount of work will likely need to be accomplished between the eventual approval of the memorandum and implementation in a timely manner. For example, FAA officials acknowledged that the agency would need to issue, update, or both issue and update internal guidance once the memorandum is signed prior to local FAA officials being able to negotiate and agree to arrangements with local military commanders. Similarly, the draft memorandum, if approved, would place a significant burden on local DOD entities to negotiate agreements. For example, the Army expressed concerns that local negotiations—at 76 locations, according to Army estimates—would take from 1 to 2 years to complete after FAA and DOD have signed the memorandum of agreement. Army officials also highlight concerns that local FAA air traffic controllers may not enter into agreements with Army units, or that local agreements will be contingent upon the density of local air traffic or the personalities of

those negotiating the agreements. Additionally, assuming that actions are agreed upon among the key stakeholders—DOD, FAA, and NORAD—to resolve or mitigate the identified security risks, DOD, FAA and NORAD will need sufficient time to implement these actions. This is due to the complexity of the ADS-B vulnerabilities and potential mitigations for operations and physical security, electronic warfare, cyber-attack, and potential effects of secondary-radar divestment.

As of June 2017, DOD and FAA had not identified any other solutions that could address the risks and concerns identified by DOD and others since 2008. Unless FAA and DOD approve one or more solutions that address all the risks associated with ADS-B technology, DOD security and military missions could face unmitigated risks. These include physical, cyber-attack, and electronic warfare security risks, as well as risks associated with divesting secondary-surveillance radars. Furthermore, unless FAA and DOD focus on the security risks of ADS-B and approve one or more solutions in a timely fashion, they may not have time to plan for and execute any technical, programmatic, or policy actions that may be necessary before all of DOD's aircraft are required to be equipped with ADS-B technology on January 1, 2020.

DOD Has Achieved Mixed Implementation of Key ADS-B Tasks Directed in 2007

Of the eight tasks associated with the implementation of ADS-B Out technology in the 2007 DOD NextGen memorandum—issued by the Deputy Secretary of Defense to ensure that the NextGen vision for the future national airspace system met DOD's requirements and the appropriate management of DOD's resources—DOD has implemented two, has partially implemented four, and has not implemented two.³⁸

Specifically, we found that DOD has implemented the following two tasks:

- **Establishing a Joint Program Office.** The Deputy Secretary of Defense directed the Secretary of the Air Force to establish and provide administrative support for a DOD Joint Program Office for NextGen. According to the 2007 NextGen memorandum, the office is responsible for coordinating DOD activities related to the NextGen

³⁸Deputy Secretary of Defense Memorandum, *Implementation of the Next Generation Air Transportation System within the Department of Defense* (Dec. 28, 2007).

effort, facilitating technology transfer for those research and development activities with potential NextGen application, and advocate for DOD interests, requirements, and capabilities in NextGen.³⁹ The Air Force established a Joint Program Office to provide services to the entire military aviation community on communication navigation surveillance/air traffic management issues in various capacities. Officials from the DOD Joint Program Office told us that the office has tested various avionics systems for methods of meeting ADS-B requirements. The office has also established an Internet portal for the services to order avionics, including those associated with ADS-B technology.

- **Appointing a DOD representative to the FAA's interagency Joint Planning and Development Office.** The 2007 NextGen memorandum directed that the Secretary of the Air Force appoint a DOD representative to the Joint Planning and Development Office's board of directors responsible for assisting in the development and coordination of DOD-wide policies and decisions concerning NextGen. In March 2012 DOD's Lead Service Office appointed an Air Force officer who also manages the DOD Lead Service Office as the DOD representative to the FAA's interagency Joint Planning and Development Office.⁴⁰

DOD partially implemented the following four tasks:

- **Validating NextGen program requirements.** The 2007 NextGen memorandum directed that the Secretary of the Air Force document and seek validation for NextGen program requirements through the Joint Capabilities Integration Development System process. The Air Force took the initial step in having its NextGen program requirements validated through DOD's Joint Capabilities Integration Development System process in October 2014. However, the focus of the assessment was on the Air Force's requirements and not that of other military services or components. This is not fully consistent with the 2007 memo, which states that the Air Force—as the lead service—

³⁹The Joint Program Office has different responsibilities from those of the Lead Service Office that the Secretary of Air Force established to assist the secretary in meeting the responsibilities assigned to the Air Force as the lead service for NextGen.

⁴⁰The Air Force established a Lead Service Office to undertake the responsibilities identified in the 2007 memo that were directed towards the Air Force as the lead service. In May 2014 the Interagency Planning Office assumed the Joint Planning and Development Office's lead responsibilities for coordinating FAA's NextGen implementation with other agencies.

should integrate the needs and requirements of the DOD components into cohesive plans and policies for inclusion in NextGen joint planning and development.

- **Establishing guidance on DOD NextGen responsibilities and objectives.** The 2007 NextGen memorandum directed the Assistant Secretary of Defense for Homeland Defense and Global Security, the DOD Chief Information Officer, and the Director of Administration, in consultation with the DOD Lead Service, to submit a proposed DOD directive within 180 days specifying the department's objectives with respect to NextGen and the continuing roles and responsibilities of the Lead Service and the DOD Policy Board on Federal Aviation.⁴¹ In 2013, about 5 years after the original due date for the 180-day requirement, DOD updated its DOD Directive 5030.19, DOD Responsibilities on Federal Aviation. While the updated directive references the responsibilities of the DOD Policy Board on Federal Aviation and the Secretary of the Air Force, per the 2007 NextGen memorandum, the directive does not specify DOD's objectives with respect to NextGen, as required by the memorandum.
- **Developing an initial plan defining actions, responsibilities, and milestones for DOD's NextGen efforts:** The 2007 NextGen memorandum required DOD's Lead Service, in coordination with the principal members of the DOD Policy Board on Federal Aviation, to develop an initial plan defining actions, responsibilities, and milestones for DOD's participation in the NextGen efforts and FAA's Joint Planning and Development Office. This initial plan was to include an implementation plan for the NextGen Joint Program Office and was to be updated semiannually. In 2013 the Air Force, in executing its responsibilities as Lead Service, issued a DOD NextGen Implementation Plan to describe the strategy, principles, and actions for the transition of DOD aviation operations (air and ground) to the national airspace system environment defined by FAA in its NextGen Implementation Plan. We found that the 2013 plan identified responsibilities of DOD components and established indicators meant to give a sense of progress made in NextGen implementation.

⁴¹The 2007 NextGen memorandum directed the Assistant Secretary of Defense for Homeland Defense and Americas Security Affairs; the Assistant Secretary of Defense for Networks and Information Integration; and, the Director of Administration and Management to take this action. However, DOD subsequently reorganized several offices within the Office of Secretary of Defense and this action became the responsibility of the Assistant Secretary of Defense for Homeland Defense and Global Security the DOD Chief Information Officer, and the Director of Administration, respectively.

However, the plan did not include detailed transition planning for ADS-B and was not updated semiannually, as required.

- **Incorporating NextGen into the planning, budgeting, and programming process:** According to the 2007 NextGen memorandum, the Secretary of the Air Force is to coordinate DOD-wide NextGen planning, budgeting, and programming guidance in conjunction with the Under Secretary of Defense for Policy and the Director of Program Analysis and Evaluation for consideration in the formulation of planning and programming guidance documents. The memorandum also directed DOD components to coordinate with the Air Force on NextGen programs they agreed to support using inter-service memorandums of understanding, and to fund procurement through service annual program objective memorandum processes. DOD provided evidence that the military departments used the program objective memorandum process to fund ADS-B Out. However, the DOD Lead Service Office did not provide department-wide planning, budgeting, and programming guidance for ADS-B or any other NextGen elements to DOD components. Similarly, DOD did not provide any inter-service memorandums of understanding that would document NextGen programs that the services agreed to fund. According to officials from the DOD Lead Service Office, this office is not responsible for planning, budgeting, and programming because the office is organizationally located within the Air Force Headquarters Office of the Deputy Chief of Staff for Operations. However, while the office may not be responsible for planning, budgeting, and programming within the Air Force, the office can issue—or coordinate the issuance—of such guidance, as directed by the Deputy Secretary of Defense.

DOD had not taken significant action or fully implemented the following two actions:

- **Integrating NextGen requirements into plans and policies:** The Secretary of the Air Force, in executing the service's responsibilities as Lead Service, did not integrate the needs and requirements of DOD components related to ADS-B into cohesive plans and policies for inclusion in NextGen joint planning and development, as directed by the Deputy Secretary of Defense in 2007. According to officials from the DOD Lead Service Office, they met the intent of these tasks through the 2012 United States Air Force *Next Generation Air Transportation System Keystone Document*, the 2013 Department of Defense (DOD) *Mid-Term NextGen Concept of Operations*, and the 2013 Department of Defense (DOD) *Mid-Term Next Generation*

(NextGen) Implementation Plan. However, the Air Force *NextGen Keystone Document* applies to the Air Force and not to NORAD or other DOD components. In addition, the *DOD Mid-Term NextGen Concept of Operations* and the *DOD Mid-Term NextGen Implementation Plan* do not discuss planning for ADS-B Out requirements, which are critical to NextGen.⁴²

- **Providing periodic and recurring NextGen progress reports:** The Assistant Secretary of Defense for Homeland Defense and Global Security did not provide periodic and recurring NextGen progress reports to the Deputy Secretary of Defense, as instructed in the 2007 NextGen memorandum.⁴³ According to the memorandum, the Assistant Secretary was designated as the principal staff assistant for NextGen and was responsible for oversight, support, and advocacy for the lead service with respect to the interagency and Joint Planning and Development Office. Officials from the Office of the Deputy Assistant Secretary of Defense for Homeland Defense Integration and from Defense Support to Civil Authorities acknowledged that the Office of the Assistant Secretary of Defense for Homeland Defense and Global Security had not tracked ADS-B implementation or provided progress reports to the Deputy Secretary of Defense—with the exception of advocating for ADS-B installation exemptions for aircraft that could not comply with the mandate—for retention of ground-based radars, and some minimal advocacy related to compliance with the FAA ADS-B Out rule.⁴⁴

DOD could not provide a clear explanation with regard to those requirements that we determined not to have been fully implemented. Officials from the DOD Lead Service Office provided a number of potential reasons to explain why the memorandum's tasks might not have been fully implemented. For example, as noted earlier, officials stated that other documents captured those requirements. Further, officials told us they believe that implementation of many of the preceding tasks was accomplished through other means, although our analysis concluded that

⁴²In its comments adopting the final rule, FAA identified the implementation of ADS-B as a key component of the NextGen System. See Federal Register Vol. 75, No. 103 at 30161 (May 28, 2010).

⁴³The 2007 memo directed the Assistant Secretary of Defense for Homeland Defense and Americas Security Affairs to undertake this action. However, the Secretary of Defense subsequently reorganized the office and renamed the position as Assistant Secretary of Defense for Homeland Defense and Global Security.

⁴⁴The FAA largely maintains the ground-based radars.

the task was either not implemented or was partially implemented, as noted previously. These officials also noted that—although there is no expiration date on the 2007 NextGen memorandum—many DOD officials consider such memorandums to be applicable for 12 to 18 months. In addition, DOD Lead Service Office officials noted that many DOD components had not assigned a high level of priority to NextGen implementation.

As a result of DOD's not fully implementing the 2007 NextGen memorandum—including developing or revising a DOD directive that specifies DOD's objectives with respect to NextGen, issuing an implementation plan that includes detailed transition planning for ADS-B and is updated semiannually, and providing recurring progress reports to the Deputy Secretary of Defense—DOD components have lacked direction and cohesion while trying to address FAA's requirement to equip military aircraft. For example:

- Officials from the Air Force Life Cycle Management Center's Fighters and Bombers Directorate told us that they have not been provided any guidance. The directorate does not intend to install ADS-B technology on Air Force fighters or bombers until they receive DOD guidance. Yet, the deadline to equip DOD aircraft that will fly in the national airspace remains January 1, 2020.
- DOD does not have a coordinated or accurate schedule for equipping ADS-B technology on military aircraft. Although DOD submitted a schedule to Congress in June 2015, officials from the DOD Lead Service Office told us that the timeframes for that plan were no longer accurate, and that the plan would be updated as part of the memorandum of agreement in February 2018.
- Some DOD components have installed or plan to install civilian GPS receivers on their aircraft to meet FAA's ADS-B technical requirements. According to DOD officials, DOD aircraft that equip with commercial GPS receivers will not be as protected from GPS security issues as they would have been had they used a military GPS receiver. According to officials from the Office of the DOD Chief Information Officer, the office with primary responsibility for GPS receiver security policy, no one within DOD—including the DOD Lead Service Office or other DOD components—had made them aware that DOD components were installing civilian receivers on aircraft.
- Since—according to an official within the DOD Lead Service Office—neither the Office of the Assistant Secretary of Defense for Homeland Defense and Global Security nor any other elements of the Office of

the Under Secretary of Defense for Policy were engaged in discussion regarding the draft memorandum of agreement with the DOD Lead Service Office and FAA, the Secretary of Defense's senior policy advisor may not be aware of provisions that may be incorporated in the agreement. For example, the draft memorandum of agreement contains a provision that could result in the department's being financially responsible for sharing the costs of sustaining secondary-surveillance radars. According to a 2007 FAA document, it will cost FAA approximately \$442 million to maintain these radars from fiscal years 2017 to 2035.

If DOD components do not fully implement key tasks that would facilitate assurance of DOD requirements in the future NextGen system and appropriate management of DOD resources—such as those tasks that the Deputy Secretary of Defense originally directed in 2007, or any tasks that the Secretary deems appropriate—DOD may risk having less efficient and less effective implementation of NextGen requirements, increased costs of implementation, or missed opportunities to address operations risks.

Conclusions

The NextGen system has the potential to increase the efficiency and effectiveness of the nation's expanding air traffic. As with many such procedural and technological innovations, DOD stands to benefit from NextGen's vision. As is the case with all such electronic and cyber systems in the information age, this must be balanced with sufficient consideration of the operations and security effects for DOD. DOD and FAA have not approved any solutions that address risks resulting from ADS-B on DOD aircraft—including operations, physical, cyber, and electronic warfare security risks, as well as risks associated with divesting secondary-surveillance radars. Unless DOD and FAA focus their efforts on the security aspects of ADS-B on DOD aircraft and produce one or more solutions to these risks, DOD aircraft and missions will be exposed to unmitigated risks that could jeopardize safety, security, and mission success. Also, unless DOD fully implements the tasks that would facilitate consistent, long-term planning and implementation of NextGen throughout the department, DOD's full integration into the NextGen system and the integrity and security of DOD's forces and missions will be hindered. Given the amount of time that has transpired since DOD initially raised security concerns in 2008 and the amount of time it will take to formalize, operationalize, and train employees to implement any

agreements prior to the January 1, 2020, deadline, it is critical that both DOD and FAA make this a high priority.

Recommendations for Executive Action

We are making two recommendations, including one to the Secretaries of Defense and Transportation, and one to the Secretary of Defense:

We recommend that the Secretaries of Defense and of Transportation address ADS-B Out security concerns by approving one or more solutions that address ADS-B Out -related security risks or incorporating mitigations for security risks into the existing draft memorandum of agreement. These approved solutions should address operations, physical, cyber-attack, and electronic warfare security risks; and risks associated with divesting secondary-surveillance radars. The solution or mitigations should be approved as soon as possible in order to allow sufficient time for implementation.

We recommend that the Secretary of Defense direct DOD components to implement key tasks that would facilitate consistent, long-term planning and implementation of NextGen—such as those tasks that the Deputy Secretary of Defense originally directed in 2007, or any tasks that the Secretary deems appropriate based on a current assessment of the original tasks.

Agency Comments and Our Evaluation

We provided a draft of the report to DOD and the Department of Transportation for review and comment. Written comments from DOD on the classified draft and from the Department of Transportation on this report are reprinted in their entirety in appendixes II and III, respectively, and summarized below. DOD and the Department of Transportation also provided technical comments, which we incorporated as appropriate.

The Department of Transportation concurred and DOD partially concurred with the first recommendation to approve one or more solutions that address ADS-B Out security risks or incorporating mitigations for security risks into the existing draft memorandum of agreement and that these solutions should address operations, physical, cyber-attack, and electronic warfare security risks as well as risks associated with divesting secondary-surveillance radar. In its written comments, the Department of

Transportation stated that it has recently developed and is now in the process of validating military flight tracking risk mitigation solutions that are technologically viable and operationally effective. Both the Department of Transportation and DOD stated that they would approve one or more solutions to address ADS-B Out related security risks. For example, both departments stated that among other actions, they would complete a memorandum of agreement between FAA and DOD that would incorporate security concerns identified in the report. DOD estimated that the memorandum of agreement will be signed in February 2018. We believe the steps identified by both the Department of Transportation and DOD, if implemented as planned, would meet the intent of our recommendation.

DOD partially concurred with the second recommendation to implement key tasks that would facilitate consistent, long-term planning and implementation of NextGen—such as those tasks that the Deputy Secretary of Defense originally directed in 2007 or any tasks that the Secretary deems appropriate based on a current assessment of the original tasks. DOD stated the Secretary of the Air Force would identify within the next 120 days which relevant key tasks would facilitate the implementation of NextGen to include assessing the status of tasks that were directed in the Deputy Secretary of Defense memorandum, “Implementation of the Next Generation Air Transportation within the Department of Defense 2007.” DOD stated that the assessment would include a comprehensive review of modernization efforts regarding NextGen and other global initiatives and that includes suitable security and cybersecurity mitigation measures. DOD also stated that the Policy Board for Federal Aviation would track key task implementation in coordination with the Secretary of the Air Force and other appropriate DOD officials. This would also include periodic updates to the Deputy Secretary of Defense. We believe these steps would meet the intent of our recommendation if implemented as planned.

We are sending copies of this report to the appropriate congressional committees; the Secretary of Defense; the Secretary of Homeland Security; the Secretary of Transportation; and the commander of NORAD. We are also sending copies to the Under Secretary of Defense for Policy; the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Chairman of the Joint Chiefs of Staff; the Secretaries of the

military departments; and the Administrator of FAA. In addition, the report is available at no charge on the GAO website <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-9971 or kirschbaumj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

A handwritten signature in black ink that reads "Joe W. Kirschbaum" followed by a long horizontal flourish.

Joseph W. Kirschbaum
Director, Defense Capabilities and Management

List of Committees

The Honorable John McCain
Chairman

The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Mac Thornberry
Chairman

The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Senate Report 114-255, accompanying a bill for the National Defense Authorization Act of Fiscal Year 2017, included a provision that we assess issues related to the defense implications of implementation of the Federal Aviation Administration's (FAA) Next Generation Air Transportation System (NextGen) and Automatic Dependent Surveillance—Broadcast (ADS-B), a main component of NextGen.¹ This report assesses the extent to which (1) the Department of Defense (DOD) and the FAA have identified security and operations risks and approved solutions to address these risks to military aircraft equipped with ADS-B Out technology; and (2) DOD has implemented key tasks in the 2007 Deputy Secretary of Defense memorandum on implementing NextGen.

The scope of our review included all DOD and Department of Transportation offices responsible for oversight or administration of ADS-B implementation by DOD as part of the NextGen program. Our review also included Airlines for America, as it represented a significant portion of the civil aviation industry in negotiations with FAA on ADS-B implementation. Table 3 contains a list of the organizations and offices we contacted during the course of our review.

¹S. Rep. No. 114-255, at 287-288 (2016).

Table 3: Organizations and Offices We Visited or Contacted

NORAD Headquarters	<ul style="list-style-type: none"> • Operations Division • Airspace Management Branch
Office of the Secretary of Defense	<ul style="list-style-type: none"> • Under Secretary of Defense (Acquisition, Technology, and Logistics) • Under Secretary of Defense (Policy) – Deputy Assistant Secretary of Defense, Homeland Defense Integration and Defense Support to Civil Authorities • Department of Defense Chief Information Officer • Office of the Director of Operational Test and Evaluation • DOD Policy Board on Federal Aviation
Army	<ul style="list-style-type: none"> • Army Aeronautical Services Agency, Fort Belvoir, Virginia • Army Training and Doctrine Command, Fort Eustis, Virginia • Army Materiel Command, Redstone Arsenal, Alabama • Army Aviation and Missile Research, Development, and Engineering Center, Redstone Arsenal, Alabama • Army Forces Command, Fort Bragg, North Carolina
Navy	<ul style="list-style-type: none"> • Office of the Chief of Naval Operations, Air Warfare, Arlington, Virginia • Naval Air Systems Command, Patuxent River Naval Air Station, Maryland
Air Force	<ul style="list-style-type: none"> • Headquarters, Air Force, NextGen DOD Lead Service Office, Arlington, Virginia • Air Mobility Command, Scott Air Force Base, Illinois • Air Combat Command, Joint Base Langley-Eustis, Virginia • Global Strike Command, Barksdale Air Force Base, Louisiana • Air Force Life Cycle Management Center, Wright-Patterson Air Force Base, Ohio; Hanscom Air Force Base, Massachusetts
Other DOD Components	<ul style="list-style-type: none"> • Defense Intelligence Agency, Missile and Space Intelligence Center, Huntsville, Alabama
Department of Transportation, Federal Aviation Administration	<ul style="list-style-type: none"> • Air Traffic Organization, Washington, D.C. • Office of NextGen, Washington, D.C.
Other	<ul style="list-style-type: none"> • ADS-B Exchange • Airlines for America, Washington, D.C.

Source: GAO. | GAO-18-177

To assess the extent to which DOD and FAA have identified security and operations risks and approved solutions to address these risks to military aircraft equipped with ADS-B Out technology, we reviewed policies, procedures, guidance, assessments, and other relevant documents from DOD, FAA, and NORAD that address ADS-B Out implementation, acquisition, operations, and cybersecurity risk management and mitigation, and any other issues that might be pertinent to identifying and addressing operations and security risks resulting from ADS-B Out. We also reviewed publicly available literature discussing potential ADS-B Out cybersecurity vulnerabilities. Specifically, we conducted a literature review of work related to vulnerabilities in ADS-B technology. To identify studies that potentially highlighted vulnerabilities that we could discuss with agency officials, we conducted key-word searches of government and

private databases to identify public, private, academic, and other professional research related to ADS-B vulnerabilities. The government databases we searched included those of GAO, the Congressional Research Service, the Congressional Budget Office, and agency Inspectors General. The private databases searched include Web of Science, ProQuest, and ProQuest Professional. To determine relevance to our review, we assessed whether article subjects were related to vulnerabilities or vulnerability mitigations for ADS-B systems. We reviewed those studies cited in our report and found their methodologies to be sufficient. To further address our objective, we interviewed officials from NORAD, DOD, the military services, and FAA on potential risks, vulnerabilities, and mitigation strategies. We did not conduct independent security and vulnerability assessments of ADS-B technology to corroborate or validate security risks identified by NORAD, DOD, FAA, and others. While military aircraft and existing radar systems may be equipped with devices (including Mode S transponders) that could also pose security risks, this report focused on risks and potential solutions associated with ADS-B Out technology that FAA mandated DOD to install on its aircraft by January 1, 2020.

We also visited multiple public websites to understand the extent to which the public could track current military flights over the United States. We met with a representative from one of these websites to understand the underlying sources of information and how the information was used to compile the images.

To understand DOD and FAA coordination, we reviewed laws, guidance, and directives related to agency cooperation for the NextGen system and implementation of ADS-B technology. This included the 2010 FAA Federal Register entry that provided guidelines and requirements for coordination between agencies and the 2007 Deputy Secretary of Defense memorandum on implementing NextGen, which states that DOD components must develop cohesive plans and policies.

To assess the extent to which DOD has implemented key tasks in the 2007 Deputy Secretary of Defense memorandum on implementing NextGen, we reviewed the Deputy Secretary of Defense's 2007 NextGen memorandum and identified 20 tasks that were directed by the Deputy Secretary for the purpose of ensuring that NextGen meets DOD requirements, and that DOD's resources are appropriately focused and

managed.² We focused on the 8 tasks wherein the accomplishment of the task would be significant to the development of plans and policies related to the implementation of the FAA's ADS-B Out technology requirement. To evaluate the implementation status of these 8 tasks, we collected relevant documentation, interviewed officials from DOD, and reviewed this information. Initially, two analysts separately reviewed this information to determine whether each of the 8 tasks was implemented or not implemented. Later, a panel of four analysts collectively reviewed both sets of analyses completed for each task and determined whether a task would be better categorized as partially implemented, instead of implemented, or as not implemented.

We conducted this performance audit from June 2016 to January 2018, 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.

²Deputy Secretary of Defense Memorandum, *Implementation of the Next Generation Air Transportation System within the Department of Defense* (Dec. 28, 2007).

Appendix II: Comments from the Department of Defense



HOMELAND DEFENSE &
GLOBAL SECURITY

ASSISTANT SECRETARY OF DEFENSE
2600 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-2600

AUG 28 2017

Mr. Joseph W. Kirschbaum
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Mr. Kirschbaum:

This is the Department of Defense (DoD) response to the GAO Draft report, GAO-17-509C, "HOMELAND DEFENSE: Urgent Need for DoD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft," dated July 13, 2017 (GAO Code 101011).

Thank you for the opportunity to comment on this important GAO report. The Department places its highest priority on the defense of the United States and its citizens. To accomplish this, our military aircraft must operate seamlessly and safely in the National Airspace System, ensuring that DoD's security and missions are not adversely affected. We are working with the Federal Aviation Administration (FAA) to mitigate security risks arising from the implementation of Automatic Dependent Surveillance-Broadcast Out (ADS-B Out) technology and from the FAA's radar modernization effort, particularly in light of rapid changes in flight-tracking technology.

We appreciate GAO's efforts to ensure that DoD's written comments (enclosure) are included in the final report. Our point of contact for this action is Col Wendy Wenke, (703) 695-1157 or wendy.b.wenke.mil@mail.mil.

Sincerely,

Robert G. Salesses
Deputy Assistant Secretary of Defense
Homeland Defense Integration and
Defense Support of Civil Authorities

Enclosure:

This report (GAO-18-177) is an unclassified version of GAO-18-176C—which had report number GAO-17-509C at the time it was transmitted to DOD for comment.

DoD response to Draft Report GAO-17-509C

**GAO DRAFT REPORT DATED JULY 13, 2017
GAO-17-509C (GAO CODE 101011)**

**“HOMELAND DEFENSE: URGENT NEED FOR DOD AND FAA TO ADDRESS RISKS
AND IMPROVE PLANNING FOR TECHNOLOGY THAT TRACKS MILITARY
AIRCRAFT”**

**DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATIONS**

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense address ADS-B Out security concerns through approving one or more solutions that address ADS-B Out-related security risks or incorporating mitigations for security risks into the existing draft memorandum of agreement. These approved solutions should address operations, physical, cyber-attack, and electronic warfare security risks; and risks associated with divesting secondary-surveillance radars. The solution or mitigations should also be approved as soon as possible in order to allow sufficient time for implementation.


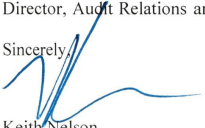
DoD RESPONSE: Partially concur. The rapid development of private sector flight-tracking technology, coupled with the FAA’s (and foreign government) modernization plans toward a satellite-based air transportation system, presents challenges to the Department’s national defense and security missions. The interagency Aviation Government Coordinating Council, Cyber Work Group, will develop recommended solutions for ADS-B Out cyber-attack and electronic warfare security risks. DoD is providing the FAA with input, informed by national security risks, on the appropriate divestiture of secondary surveillance radar and, together, DoD and FAA have developed a draft memorandum of agreement (MOA) informed by operations, physical, cyber-attack, and electronic warfare security risks that facilitates support of national defense mission requirements. The MOA will incorporate language that ensures DoD security concerns, associated with DoD aircraft transmitting ADS-B data, are addressed. We anticipate a signed MOA in February 2018.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense direct DoD Components to implement key tasks that would facilitate consistent, long-term planning and implementation of NextGen—such as those tasks that the Deputy Secretary of Defense originally directed in 2007, or any tasks the Secretary thinks appropriate based on a current assessment of the original tasks.

DoD RESPONSE: Partially Concur. Within the next 120 days, the Secretary of the Air Force (SecAF), as the head of the lead service for NextGen, will identify which relevant key tasks would facilitate the implementation of NextGen, to include assessing the status of tasks that were

directed in Deputy Secretary of Defense memorandum, "Implementation of the Next Generation Air Transportation within the Department of Defense, 2007." The assessment will include a comprehensive review of the modernization efforts, NextGen and other global initiatives (SESAR) with respect to the entire aviation ecosystem that includes suitable security and cybersecurity mitigation measures. The Policy Board for Federal Aviation will track key task implementation, with the SecAF, in coordination with other appropriate DoD officials, providing periodic updates to the Deputy Secretary of Defense.

Appendix III: Comments from the Department of Transportation

 U.S. Department of Transportation Office of the Secretary of Transportation	Assistant Secretary for Administration	1200 New Jersey Avenue, SE Washington, DC 20590
Joseph W. Kirschbaum Director, Defense Capabilities and Management U.S. Government Accountability Office (GAO) 441 G Street NW Washington, DC 20548	NOV 30 2017	
<p>The Federal Aviation Administration (FAA) is charged with developing and maintaining regulations that facilitate adaptation of the air transportation system to the present and future needs of the national defense¹ and other stakeholders. As part of this effort, the FAA is working to develop sound operations security (OPSEC) risk mitigations for the Department of Defense (DOD) regarding Automatic Dependent Surveillance Broadcast (ADS-B) Out. We have recently developed and are now in the process of validating military flight tracking risk mitigation solutions that are technologically viable and operationally effective.</p> <p>FAA actions to support effective OPSEC risk mitigation solutions for flight tracking of military aircraft include the following:</p> <ul style="list-style-type: none">• In March of 2017, at the direction of the Administrator, FAA established a cross organizational ADS-B Steering Group tasked with developing and recommending solutions to accommodate sensitive missions in the National Airspace System after the January 1, 2020 implementation date for ADS-B Out.• On June 30, 2017, FAA met with DOD and other interagency security partners to discuss how to best maintain the OPSEC for interagency sensitive flight operations in the context of the ADS-B environment and discussed possible OPSEC solutions identified by the ADS-B Steering Group. <p>Upon review of the GAO's draft report, we concur with the recommendation to approve one or more solutions to address ADS-B Out related security risks and we will provide a detailed response to the recommendation within 60 days of the final report's issuance.</p> <p>This letter shall serve as the Department's official response to GAO's draft report. We appreciate the opportunity to respond to the GAO draft report. Please contact Madeline M. Chulumovich, Director, Audit Relations and Program Improvement, at (202) 366-6512 with any questions.</p> <p>Sincerely,</p>  <p>Keith Nelson Assistant Secretary for Administration</p>		
<p><small>¹ 49 U.S.C. § 40101(a)(7)(C)</small></p>		

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Joseph W. Kirschbaum, (202) 512-9971 or kirschbaumj@gao.gov

Staff Acknowledgments

In addition to the contact named above, Tommy Baril (Assistant Director), Tracy Barnes, David Beardwood, Virginia Chanley, Benjamin Emmel, Kevin Newak, Joshua Ormond, Matthew Sakrekoff, Amanda Weldon, and Edwin Yuen made major contributions to this report.

Colleen Candri, Mark Canter, Raj Chitikila, Tracy Harris, Kirk Kiester, Amie Lesser, Nicholas Marinos, Madhav Panwar, John Shumann, James Tallon, and Cheryl Weissman also made contributions to this report.

Appendix V: Accessible Data

Agency Comment Letters

Text of Appendix II: Comments from the Department of Defense

Page 1

AUG 28 2017

Mr. Joseph W. Kirschbaum

Director, Defense Capabilities and Management

U.S. Government Accountability Office 441 G Street, N.W.

Washington, DC 20548 Dear Mr. Kirschbaum:

This is the Department of Defense (DoD) response to the GAO Draft report, GAO-17-509C, "HOMELAND DEFENSE: Urgent Need for DoD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft," dated July 13, 2017 (GAO Code 101011).

Thank you for the opportunity to comment on this important GAO report. The Department places its highest priority on the defense of the United States and its citizens. To accomplish this, our military aircraft must operate seamlessly and safely in the National Airspace System, ensuring that DoD's security and missions are not adversely affected. We are working with the Federal Aviation Administration (FAA) to mitigate security risks arising from the implementation of Automatic Dependent Surveillance-Broadcast Out (ADS-B Out) technology and from the FAA's radar modernization effort, particularly in light of rapid changes in flight-tracking technology.

We appreciate GAO's efforts to ensure that DoD's written comments (enclosure) are included in the final report. Our point of contact for this

action is Col Wendy Wenke, (703) 695-1157 or wendy.b.wenke.mil@mail.mil.

Sincerely,

Robert G. Salesses

Deputy Assistant Secretary of Defense Homeland Defense Integration and

Defense Support of Civil Authorities

Enclosure:

Page 2

DoD response to Draft Report GAO-I 7-509C

GAO DRAFT REPORT DATED JULY 13, 2017 GAO-17-509C (GAO CODE 101011)

"HOMELAND DEFENSE: URGENT NEED FOR DOD AND FAA TO ADDRESS RISKS AND IMPROVE PLANNING FOR TECHNOLOGY THAT TRACKS MILITARY AIRCRAFT"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1:

The GAO recommends that the Secretary of Defense address ADS- B Out security concerns through approving one or more solutions that address ADS-B Out- related security risks or incorporating mitigations for security risks into the existing draft memorandum of agreement. These approved solutions should address operations, physical, cyber-attack, and electronic warfare security risks; and risks associated with divesting secondary- surveillance radars. The solution or mitigations should also be approved as soon as possible in order to allow sufficient time for implementation.

DoD RESPONSE: Partially concur.

The rapid development of private sector flight-tracking technology, coupled with the FAA's (and foreign government) modernization plans toward a satellite-based air transportation system, presents challenges to the Department's national defense and security missions. The interagency Aviation Government Coordinating Council, Cyber Work Group, will develop recommended solutions for ADS-B Out cyber-attack and electronic warfare security risks. DoD is providing the FAA with input, informed by national security risks, on the appropriate divestiture of secondary surveillance radar and, together, DoD and FAA have developed a draft memorandum of agreement (MOA) informed by operations, physical, cyber- attack, and electronic warfare security risks that facilitates support of national defense mission requirements. The MOA will incorporate language that ensures DoD security concerns, associated with DoD aircraft transmitting ADS-B data, are addressed. We anticipate a signed MOA in February 2018.

RECOMMENDATION 2:

The GAO recommends that the Secretary of Defense direct DoD Components to implement key tasks that would facilitate consistent, long-term planning and implementation of NextGen—such as those tasks that the Deputy Secretary of Defense originally directed in 2007, or any tasks the Secretary thinks appropriate based on a current assessment of the original tasks.

DoD RESPONSE: Partially Concur.

Within the next 120 days, the Secretary of the Air Force (SecAF), as the head of the lead service for NextGen, will identify which relevant key tasks would facilitate the implementation of NextGen, to include assessing the status of tasks that were

Page 3

directed in Deputy Secretary of Defense memorandum, "Implementation of the Next Generation Air Transportation within the Department of Defense, 2007." The assessment will include a comprehensive review of the modernization efforts, NextGen and other global initiatives (SESAR) with respect to the entire aviation ecosystem that includes suitable security and cybersecurity mitigation measures. The Policy Board for Federal Aviation will track key task implementation, with the SecAF, in

coordination with other appropriate DoD officials, providing periodic updates to the Deputy Secretary of Defense.

Text of Appendix III: Comments from the Department of Transportation

NOV 30, 2017

Joseph W. Kirschbaum

Director , Defense Capabilities and Management

U.S. Government Accountability Office (GAO) 441 G Street NW

Washington, DC 20548

The Federal Aviation Administration (FAA) is charged with developing and maintaining regulations that facilitate adaptation of the air transportation system to the present and future needs of the national defense¹ and other stakeholders. As part of this effort, the FAA is working to develop sound operations security (OPSEC) risk mitigations for the Department of Defense (DOD) regarding Automatic Dependent Surveillance Broadcast (ADS-B) Out. We have recently developed and are now in the process of validating military flight tracking risk mitigation solutions that are technologically viable and operationally effective.

FAA actions to support effective OPSEC risk mitigation solutions for flight tracking of military aircraft include the following:

- In March of 2017, at the direction of the Administrator, FAA established a cross organizational ADS-B Steering Group tasked with developing and recommending solutions to accommodate sensitive missions in the National Airspace System after the January 1, 2020 implementation date for ADS-B Out.
- On June 30, 2017, FAA met with DOD and other interagency security partners to discuss how to best maintain the OPSEC for interagency sensitive flight operations in the context of the ADS-B environment and discussed possible OPSEC solutions identified by the ADS-B Steering Group.

Upon review of the GAO's draft report, we concur with the recommendation to approve one or more solutions to address ADS-B Out related security risks and we will provide a detailed response to the recommendation within 60 days of the final report's issuance.

This letter shall serve as the Department's official response to GAO's draft report. We appreciate the opportunity to respond to the GAO draft report. Please contact Madeline M. Chulumovich, Director, Audit Relations and Program Improvement, at (202) 366-6512 with any questions.

Keith Nelson

Assistant Secretary for Administration

Related GAO Products

Next Generation Air Transportation System: Improved Risk Analysis Could Strengthen FAA's Global Interoperability Efforts. [GAO-15-608](#). Washington, D.C.: July 29, 2015

Air Traffic Control: FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen. [GAO-15-370](#). Washington D.C.: April 14, 2015.

National Airspace System: Improved Budgeting Could Help FAA Better Determine Future Operations and Maintenance Priorities. [GAO-13-693](#). Washington, D.C.: August 22, 2013.

NextGen Air Transportation System: FAA Has Made Some Progress in Midterm Implementation, but Ongoing Challenges Limit Expected Benefits, [GAO-13-264](#). Washington D.C.: April 8, 2013.

Next Generation Air Transportation System: FAA Faces Implementation Challenges. [GAO-12-1011T](#). Washington, D.C.: September 12, 2012.

Next Generation Air Transportation: Collaborative Efforts with European Union Generally Mirror Effective Practices, but Near-Term Challenges Could Delay Implementation, [GAO-12-48](#). Washington, D.C.: November 3, 2011.

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](#), [LinkedIn](#), [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 and read [The Watchblog](#).

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, 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, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

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