United States Government Accountability Office

Report to Congressional Requesters

October 2020

AVIATION CYBERSECURITY

FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks

GAO-21-86

October 2020

GAO Highlights

Highlights of GAO-21-86, a report to congressional requesters

AVIATION CYBERSECURITY

FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks

Why GAO Did This Study

Avionics systems, which provide weather information, positioning data, and communications, are critical to the safe operation of an airplane. FAA is responsible for overseeing the safety of commercial aviation, including avionics systems. The growing connectivity between airplanes and these systems may present increasing opportunities for cyberattacks on commercial airplanes.

GAO was asked to review the FAA's oversight of avionics cybersecurity issues. The objectives of this review were to (1) describe key cybersecurity risks to avionics systems and their potential effects, (2) determine the extent to which FAA oversees the implementation of cybersecurity controls that address identified risks in avionics systems, and (3) assess the extent to which FAA coordinates internally and with other government and industry entities to identify and address cybersecurity risks to avionics systems.

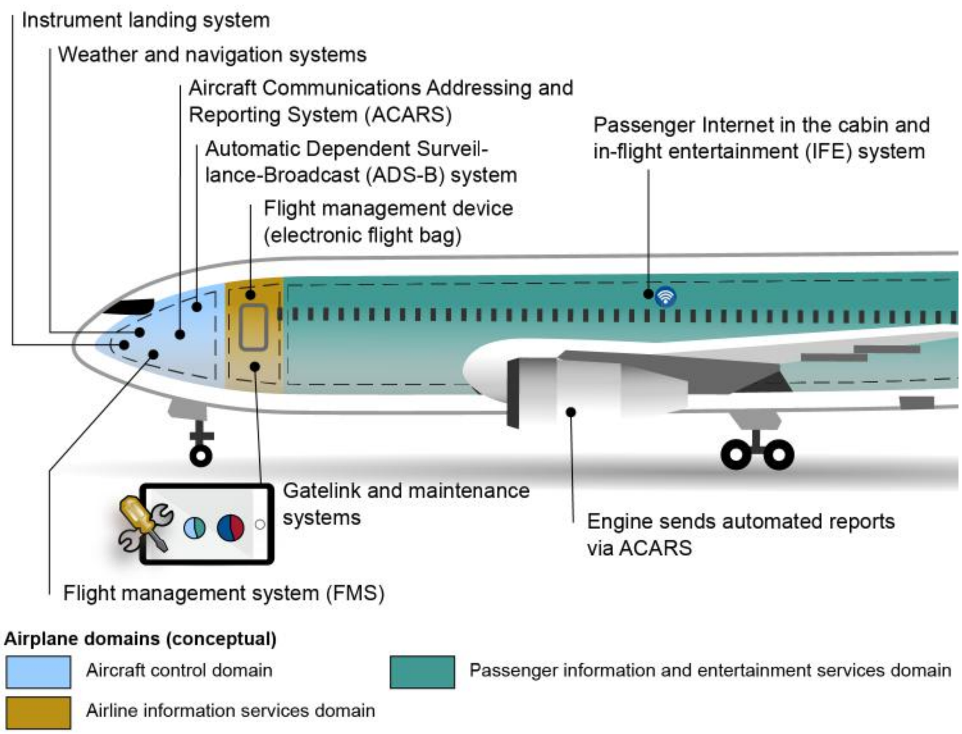
To do so, GAO reviewed information on key cybersecurity risks to avionics systems, as reported by major industry representatives as well as key elements of an effective oversight program, and compared FAA's process for overseeing the implementation of cybersecurity controls in avionics systems with these program elements. GAO also reviewed agency documentation and interviewed agency and industry representatives to assess FAA's coordination efforts to address the identified risks.

View GAO-21-86. For more information, contact Nick Marinos at (202) 512-9342 or MarinosN@gao.gov, or Heather Krause at (202) 512-2834 or KrauseH@gao.gov.

What GAO Found

Modern airplanes are equipped with networks and systems that share data with the pilots, passengers, maintenance crews, other aircraft, and air-traffic controllers in ways that were not previously feasible (see fig. 1). As a result, if avionics systems are not properly protected, they could be at risk of a variety of potential cyberattacks. Vulnerabilities could occur due to (1) not applying modifications (patches) to commercial software, (2) insecure supply chains, (3) malicious software uploads, (4) outdated systems on legacy airplanes, and (5) flight data spoofing. To date, extensive cybersecurity controls have been implemented and there have not been any reports of successful cyberattacks on an airplane's avionics systems. However, the increasing connections between airplanes and other systems, combined with the evolving cyber threat landscape, could lead to increasing risks for future flight safety.

Figure 1: Key Systems Connections to Commercial Airplanes



Source: GAO analysis of FAA and industry documentation. | GAO-21-86

The Federal Aviation Administration (FAA) has established a process for the certification and oversight of all US commercial airplanes, including the operation of commercial air carriers (see fig. 2). While FAA recognizes avionics cybersecurity as a potential safety issue for modern commercial airplanes, it has not fully implemented key practices that are necessary to carry out a risk-based cybersecurity oversight program.

What GAO Recommends

GAO is making six recommendations to FAA to strengthen its avionics cybersecurity oversight program:

- GAO recommends that FAA conduct a cybersecurity risk assessment of avionics systems cybersecurity within its oversight program to identify the relative priority of avionics cybersecurity risks compared to other safety concerns and develop a plan to address those risks.

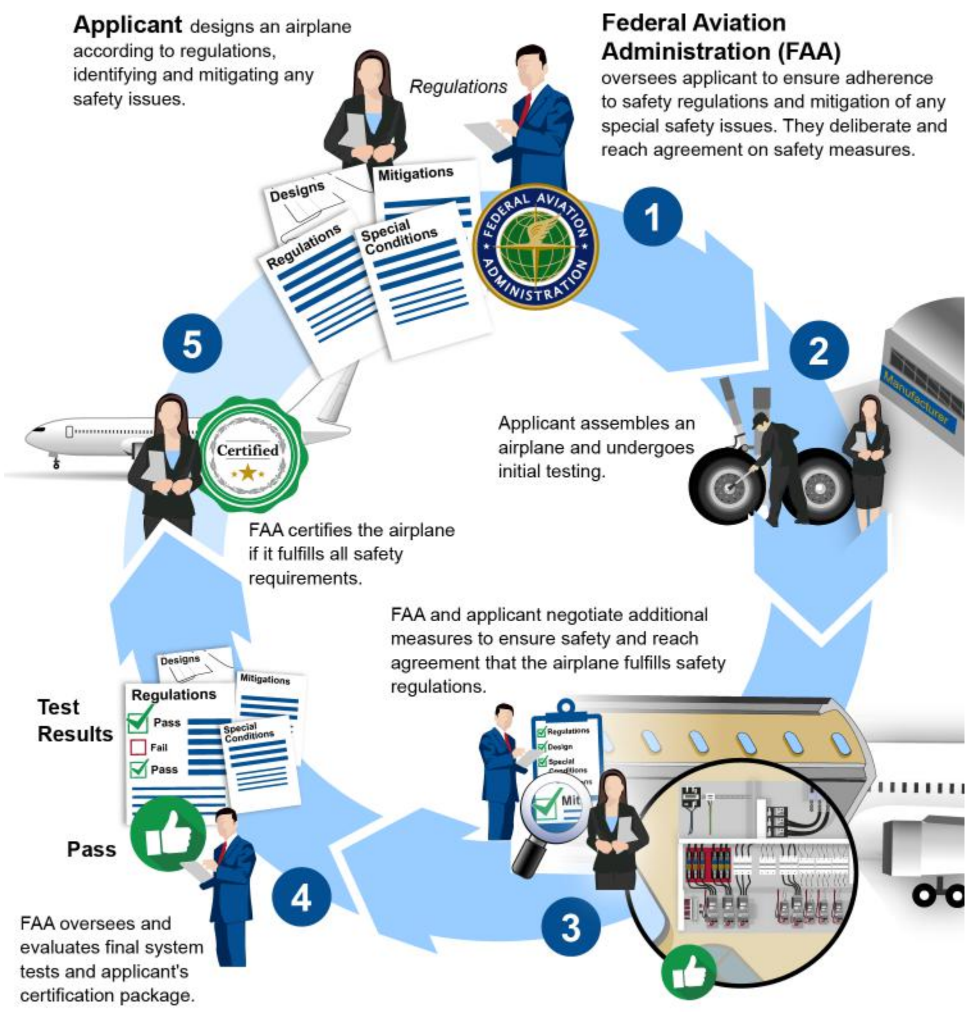
Based on the assessment of avionics cybersecurity risks, GAO recommends that FAA

- identify staffing and training needs for agency inspectors specific to avionics cybersecurity, and develop and implement appropriate training to address identified needs.
- develop and implement guidance for avionics cybersecurity testing of new airplane designs that includes independent testing.
- review and consider revising its policies and procedures for monitoring the effectiveness of avionics cybersecurity controls in the deployed fleet to include developing procedures for safely conducting independent testing.
- ensure that avionics cybersecurity issues are appropriately tracked and resolved when coordinating among internal stakeholders.
- review and consider the extent to which oversight resources should be committed to avionics cybersecurity.

FAA concurred with five out of six GAO recommendations. FAA did not concur with the recommendation to consider revising its policies and procedures for periodic independent testing. GAO clarified this recommendation to emphasize that FAA safely conduct such testing as part of its ongoing monitoring of airplane safety.

Specifically, FAA has not (1) assessed its oversight program to determine the priority of avionics cybersecurity risks, (2) developed an avionics cybersecurity training program, (3) issued guidance for independent cybersecurity testing, or (4) included periodic testing as part of its monitoring process. Until FAA strengthens its oversight program, based on assessed risks, it may not be able to ensure it is providing sufficient oversight to guard against evolving cybersecurity risks facing avionics systems in commercial airplanes.

Figure 2: Federal Aviation Administration's Certification Process for Commercial Transport Airplanes



Source: GAO analysis of FAA documentation. | GAO-21-86

GAO has previously identified key practices for interagency collaboration that can be used to assess interagency coordination. FAA coordinates with other federal agencies, such as the Departments of Defense (DOD) and Homeland Security (DHS), and with industry to address aviation cybersecurity issues. For example, FAA co-chairs the Aviation Cyber Initiative, a tri-agency forum with DOD and DHS to address cyber risks across the aviation ecosystem. However, FAA's internal coordination activities do not fully reflect GAO's key collaboration practices. FAA has not established a tracking mechanism for monitoring progress on cybersecurity issues that are raised in coordination meetings, and its oversight coordination activities are not supported by dedicated resources within the agency's budget. Until FAA establishes a tracking mechanism for cybersecurity issues, it may be unable to ensure that all issues are appropriately addressed and resolved. Further, until it conducts an avionics cybersecurity risk assessment, it will not be able to effectively prioritize and dedicate resources to ensure that avionics cybersecurity risks are addressed in its oversight program.

Contents

Abbreviations

ACARS	Aircraft Communications Addressing and Reporting System
ACI	Aviation Cyber Initiative
ADS-B	Automatic Dependent Surveillance-Broadcast
AFDX	Avionics Full-Duplex Switched Ethernet
AFS	Flight Standards Service
AIR	Aircraft Certification Service
A-ISAC	Aviation Information Sharing and Analysis Center
ARINC	Aeronautical Radio, Inc.
ASH	Security and Hazardous Material Safety
ATC	Air Traffic Control
AVS	Aviation Safety
CFR	Code of Federal Regulations
CyberCAT	Cyber Safety Commercial Aviation Team
DHS	Department of Homeland Security
DOD	Department of Defense
EUROCAE	European Organisation for Civil Aviation Equipment
EASA	European Aviation Safety Agency
FAA	Federal Aviation Administration
ICAO	International Civil Aviation Organization
IFE	in-flight entertainment
ILS	instrument landing system
NextGen	Next Generation Air Transportation System
NIST	National Institute of Standards and Technology
NSAS	National Strategy for Aviation Security
RTCA	Radio Technical Commission for Aeronautics
TSA	Transportation Security Administration

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

October 9, 2020

The Honorable Susan M. Collins
Chairman
The Honorable Jack Reed
Ranking Member
Subcommittee on Transportation,
Housing and Urban Development,
and Related Agencies
Committee on Appropriations
United States Senate

The U.S. aviation industry—including passenger air carriers, cargo air carriers, and aviation manufacturers and contractors—is vital to the U.S. economy. Generating billions of dollars in revenue each year, the aviation industry plays a substantial role in catalyzing economic growth and influencing the quality of peoples' lives around the globe. Although the COVID-19 pandemic has impacted the industry by diminishing passenger demand for air travel, Congress and the administration have taken a series of actions to assist the industry and ensure continued flight operations.[1]

These flight operations are enabled by the global network of airframe manufacturers, suppliers, carriers, airports, and other entities—generally referred to as the aviation ecosystem. The interdependencies across the aviation ecosystem underscore the importance of identifying, mitigating, and coordinating cybersecurity risks to ensure the safe operation of commercial airplanes in the National Airspace System.[2] Flight-critical airplane systems, known as avionics systems, are a key aspect of the National Airspace System. These include systems that provide weather information, positioning data, and communications to the airplane.

[1]COVID-19 relief laws enacted as of May 31, 2020, include the *Coronavirus Preparedness and Response Supplemental Appropriations Act*, 2020, Pub. L. No. 116-123, 134 Stat. 146; *Families First Coronavirus Response Act*, Pub. L. No. 116-127, 134 Stat. 178 (2020); CARES Act, Pub. L. No. 116-136, 134 Stat. 281 (2020); and Paycheck Protection *Program and Health Care Enhancement Act*, Pub. L. No. 116-139, 134 Stat. 620 (2020).

[2]The National Airspace System was created by the FAA to protect persons and property on the ground, and to establish a safe and efficient airspace environment for civil, commercial, and military aviation. The National Airspace System is made up of a network of air navigation facilities, air traffic control facilities, airports, technology, and appropriate rules and regulations that are needed to operate the system.

The Federal Aviation Administration (FAA) is responsible for the safety and oversight of commercial aviation, which includes the certification and oversight of all US commercial airplanes and the operation of commercial air carriers, among other things. Other federal agencies, such as the Department of Defense (DOD) and the Department of Homeland Security (DHS), have responsibilities related to airplane cybersecurity research in coordination with FAA and other stakeholders across the aviation ecosystem.

You asked us to review cybersecurity risks to avionics systems and the sufficiency of FAA's oversight of efforts to address these risks. Specifically, our objectives were to (1) describe key cybersecurity risks to avionics systems and their potential effects, (2) determine the extent to which FAA oversees the implementation of cybersecurity controls that address identified risks in avionics systems, and (3) assess the extent to which FAA coordinates internally and with other government and industry entities to identify and address cybersecurity risks to avionics systems.

To address the first objective, we developed a list of cyber threat actors that could pose a threat to commercial airplanes, identified internal and external electronic connections to airplane avionics systems that could be exploited, and identified the potential risks of cyberattacks if those vulnerabilities were exploited. To develop the list of cyber threat actors, we reviewed our previously issued report on cyber-based threats facing critical infrastructure,[3] as well as the threats identified by the 2019 Worldwide Threat Assessment of the U.S. Intelligence Community.[4] We also analyzed FAA documentation and public information, such as security consultant reports, to identify and describe major potential vulnerabilities on commercial transport airplanes.

In addition, we interviewed officials and representatives from the following entities to identify and discuss their perspectives regarding the significant cyber threats to avionics systems:

[3]GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid,* GAO-19-332 (Washington, D.C.: Aug. 26, 2019).

[4]Daniel R. Coats, Director of National Intelligence, *Worldwide Threat Assessment of the U.S. Intelligence Community*, testimony before the Senate Select Committee on Intelligence, 116th Cong. 1st sess., January 29, 2019.

- **Federal agencies.** Officials from DOD, DHS, and FAA that carry out aviation cybersecurity responsibilities for their agency.
- **Airlines.** Representatives of American Airlines, Alaska Airlines, Delta Airlines, JetBlue Airlines, Southwest Airlines, and United Airlines. We selected these airlines because they had the greatest number of domestic departures in 2018.
- **Manufacturers.** Knowledgeable representatives from airframe, avionics, and engine manufacturers that were selected based on their roles as major US-based aviation industry manufacturers. Specifically, we interviewed representatives from Boeing, Airbus, Rolls Royce, GE Aviation, and Rockwell Collins.
- **Industry associations.** Representatives from the Aviation Information Sharing & Analysis Center (A-ISAC) and the Aerospace Industries Association.
- **International organizations.** Representatives from the European Union Aviation Safety Agency (EASA) and the International Civil Aviation Organization (ICAO).
- **Subject matter experts.** Representatives from Pen Test Partners, a security consultancy firm, and Dr. Karl Koscher from the University of Washington and Dr. Stefan Savage from the University of California San Diego. These individuals are involved in security research and airplane avionics systems testing research. They were selected because of their research experience with testing cybersecurity controls for avionics systems.

To address the second objective, we identified four key elements of an effective oversight program by reviewing National Institute of Standards and Technology (NIST) guidance[5] and previous GAO reports on effective oversight programs.[6] These elements include (1) an assessment of risks, (2) training, (3) independent testing, and (4) ongoing monitoring.

We then obtained and analyzed information on the policies, procedures, and processes that FAA has in place for overseeing the implementation of cybersecurity controls in avionics systems. We assessed the

[5]NIST Special Publication 800-39, *Managing Information Security Risk* (Gaithersburg, MD: 2011). NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Rev. 4 (Gaithersburg, MD: April 2013).

[6]GAO, *Cybersecurity: Office of Federal Student Aid Should Take Additional Steps to Oversee Non-School Partners' Protection of Borrower Information,* GAO-18-518 (Washington, D.C.: Sept. 17, 2018).

consistency of these policies, procedures, and processes with the key elements of an effective oversight program.

Further, we conducted a site visit to FAA and Boeing facilities in Seattle, Washington. We interviewed Boeing officials regarding the manufacturer's processes for securing avionics systems from cyberattack during the manufacturing and certification processes. We also interviewed FAA officials in Seattle regarding their oversight practices as they review cybersecurity during certification. In addition to Boeing, we also interviewed Airbus, suppliers, airline officials, and other industry representatives to understand their respective roles in ensuring cybersecurity for airplane flight systems and to obtain their views on the sufficiency of FAA's efforts in overseeing avionics cybersecurity.

To address the third objective, we assessed the *National Strategy for Aviation Security*[7] and NIST's cybersecurity risk management guidance to identify the key requirements for managing and responding to risk at the organizational level: (1) determining cybersecurity risks, (2) developing actions to respond to them, and (3) monitoring the results.[8]

Further, for the agency's internal coordination efforts, we reviewed the extent to which FAA has adopted key practices, as identified in GAO's guide for implementing interagency collaborative mechanisms.[9] We assessed FAA documentation, such as strategies, plans, and directives describing cybersecurity coordination efforts across its internal components, against these collaborative practices to determine whether they had been fully implemented.

We then interviewed officials from FAA, DOD, and DHS, in addition to aviation industry stakeholders, regarding the extent to which coordination among government agencies, including internal FAA components, and industry stakeholders, addressed the identified avionics cybersecurity threats. We also obtained the views of industry officials and subject

[7]White House*, National Strategy for Aviation Security of the United States of America,* (Washington, D.C.: December 2018).

[8]NIST Special Publication 800-39, *Managing Information Security Risk* (Gaithersburg, MD: 2011).

[9]GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, GAO-12-1022 (Washington, D.C.: Sept. 27, 2012).

matter experts on FAA's efforts to coordinate specifically on avionics cybersecurity risks.

We conducted this performance audit from April 2019 to October 2020 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

Aviation Ecosystem and Avionics Systems

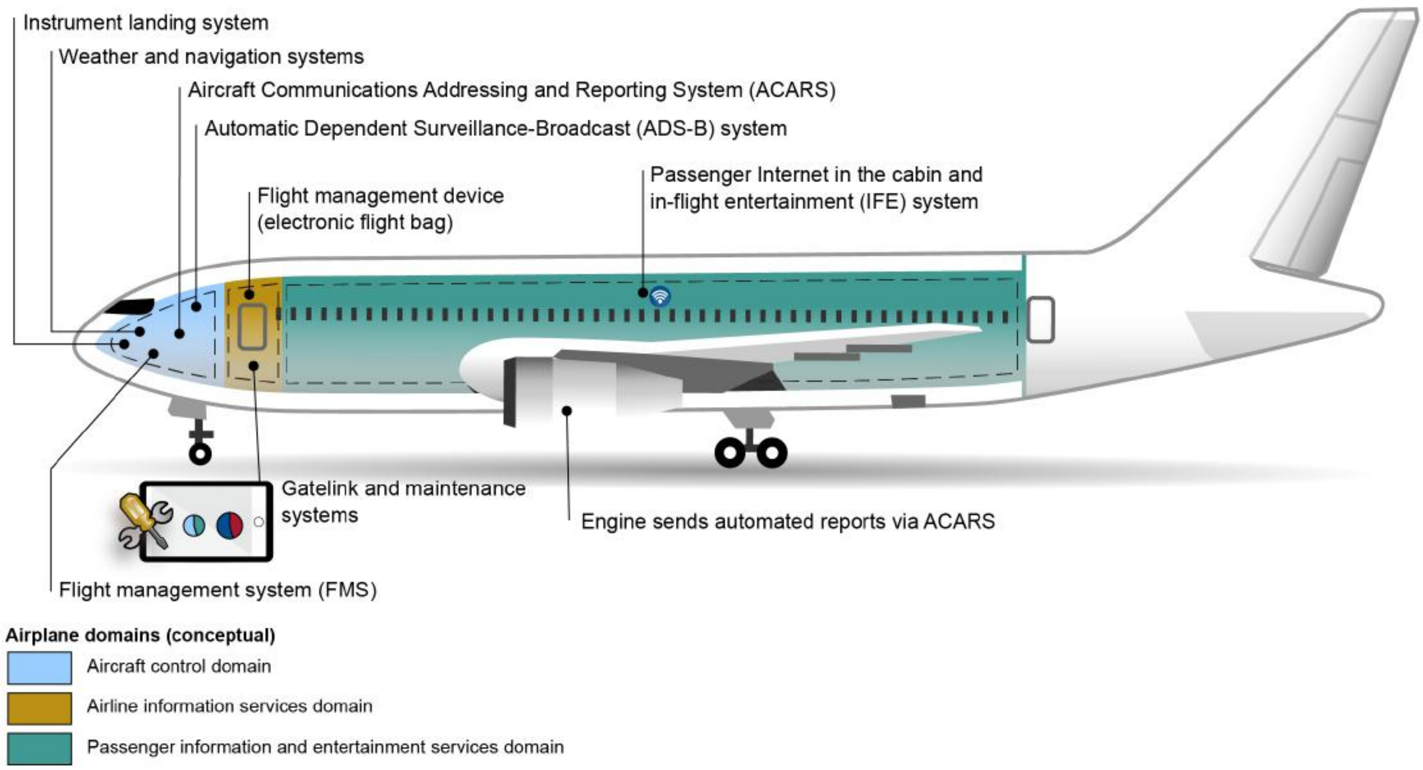
The aviation ecosystem is a large and complex international entity with many stakeholders. It consists of airplane manufacturers and air carriers, their employees, customers, suppliers, and vendors; other aviation-related companies; standards-making bodies, regulators, domestic and international research and policy-making bodies, and other aviation-related organizations; aviation-related products and equipment, such as airplanes and airplane components and systems; air traffic control personnel, equipment, and systems; communication systems among the various parties; and other aviation-related items.

Airplanes are the centerpiece of the aviation ecosystem. Further, avionics systems are generally considered one of the most critical components of an airplane due to their criticality for safe flight operations. They include engine controls, flight control systems, navigation, communications, flight recorders, lighting systems that provide interior and exterior illumination, fuel systems, weather radar, performance monitors, and systems that carry out hundreds of other mission and flight management tasks. In this report, we refer to avionics systems as any systems available to the flight crew or maintenance crew that are critical for the safe operation and maintenance of an airplane. Systems that exclusively provide customer services, such as in-flight entertainment, are not considered part of avionics systems.

Commercial Airplane Systems Are Becoming More Connected

Historically, the networks on an airplane were used primarily to exchange data among onboard systems. Now, modern commercial airplanes are equipped with networks and systems that share data with the flight crews, passengers, other airplanes, maintenance crews, and air traffic controllers in ways that were not previously feasible. Such network and system connections are depicted in figure 1.

Figure 1: Key Systems Connections to Commercial Airplanes



Source: GAO analysis of FAA and industry documentation. | GAO-21-86

Multiple networks for transmitting data internally and externally may be in place on any given airplane, and these networks provide many different types of connections between avionics and other systems. The connectivity of these networks varies, depending on the technical standards used to implement them. For example, commercial airplanes have traditionally used networks that relied on the Aeronautical Radio, Inc. (ARINC) 429 standard. Devised in 1977, this standard originally defined a one-way data bus that enhanced security by severely limiting how data and electronic commands could be exchanged.[10]

More advanced networks provide more efficient, two-way communications by using a new data bus standard developed by Rockwell Collins in 2005, called Avionics Full Duplex Switched Ethernet

[10]A data bus is a system within a computer or device that consists of a connector or set of wires that provide transportation for data.

(AFDX). Airlines and manufacturers use the enhanced capabilities of the AFDX standard on newer airplanes to capture and provide data about the condition of various airplane components and systems—including avionics systems—to maintenance crews so that issues can be resolved quickly.

Avionics systems use these advanced networks to exchange operational data with multiple systems located outside of the airplane. For example, certain airplanes are equipped with a system known as the Automatic Dependent Surveillance-Broadcast (ADS-B) that periodically broadcasts data such as flight identification number, current position, altitude, and velocity, which can be received by FAA air traffic control (ATC) systems for tracking purposes. Likewise, the Aircraft Communications Addressing and Reporting System (ACARS) communicates data, such as flight plans and weather information from ATC, between the airplane and ground systems and sends that data directly to flight management systems.

In addition, we have previously reported on FAA's efforts to implement the Next Generation Air Transportation System (NextGen), which includes ADS-B and is designed to transition the nation's ground-based air traffic control system to one that uses satellite navigation, automated position reporting, and digital communications.[11] NextGen is also designed to include enhanced interactions with airplane avionics systems.

Airplane Domains

The aviation industry has defined conceptual airplane domains for commercial transport airplanes that are used as an aid to discuss cybersecurity protections with the understanding that airplane architectures can vary widely. As shown in figure 1, an airplane typically has three domains: (1) aircraft control, (2) airline information services, and (3) passenger information and entertainment services. The airline information services and passenger information and entertainment services domains may require connectivity with ground-based computing networks, such as those for maintenance and operations. The functions of each domain are as follows:

- **Aircraft control domain.** The most critical of the three domains, this domain consists of systems and networks whose primary function is to support the safe operation of the airplane. The domain includes the airplane's avionics and the flight controls, all air traffic control functions, flight management and navigation systems, and passenger

[11]GAO, *Air Traffic Control Modernization: Progress and Challenges in Implementing NextGen,* GAO-17-450 (Washington, D.C.: Aug. 31, 2017).

safety systems, such as environmental control and smoke detection systems, among many others. The systems in the aircraft control domain are separated from other airplane systems.

- **Airline information services domain.** This domain provides services and connectivity between other airplane domains, such as aircraft control, passenger information and entertainment services, and any connected off-board networks. For example, this domain encompasses crew systems, including flight management devices known as electronic flight bags,[12] fault monitoring systems, maintenance systems, and airport ground-based communications, which must remain isolated from the passenger domain. In addition, this domain provides a limited amount of data through a one-way (or "read-only") channel to the passenger domain from the aircraft control domain so passengers can receive flight status updates. While this domain includes data that support the safe operation of the airplane, systems within this domain do not have the ability to issue commands that directly control the airplane.
- **Passenger information and entertainment services domain.** This domain includes any device or function that provides services to passengers, including in-flight entertainment (IFE) systems, cabin management systems (such as cabin lighting and galley operations), and other passenger-facing systems. For example, this domain allows passengers to access the Internet with their personal devices, such as laptops and tablets. It may encompass multiple systems from different vendors that may or may not be interconnected with one another.

Federal Agencies Have Specific Roles in Supporting Aviation Cybersecurity

Three agencies have distinct roles and responsibilities with regard to aviation cybersecurity.

- **Federal Aviation Administration.** FAA has regulatory authority over the safety of civil aviation, which includes air traffic control and other ground operations as well as aircraft. The agency serves as co-lead with DHS on infrastructure protection activities for the aviation subsector of the transportation system critical infrastructure sector.

[12]An electronic flight bag (EFB) is an electronic device used by the flight crew that displays digital documentation, including navigational charts, operations manuals, and airplane checklists, replacing the physical flight bags that contained paper versions of these documents and other tools in the past. EFBs can also perform basic flight planning calculations. The most advanced electronic flight bags are included in the airplane's certified avionics systems and are fully integrated with the flight management system and other avionics systems. These advanced EFBs can display an airplane's position on navigational charts, depict real-time weather, and perform many complex flight-planning tasks.

Specifically, FAA is responsible for the safety and oversight of commercial aviation, which includes the certification and oversight of all US commercial aviation products and commercial entities. These include commercial airplanes and their avionics systems, airframe and component manufacturers, and air carriers. To the extent that cybersecurity risks could threaten the safety of civil aviation, FAA is responsible for overseeing efforts to mitigate those risks.

- **Department of Homeland Security.** DHS is the lead federal agency for cybersecurity protection. With regard to aviation, DHS is responsible for coordinating federal government activities addressing aviation security. DHS is to conduct these activities by identifying conflicting procedures, identifying vulnerabilities and consequences, and coordinating corresponding interagency mitigation actions. Further, DHS is responsible for overseeing critical aviation and transportation security activities, such as airport security, through the Transportation Security Administration (TSA). The Cybersecurity and Infrastructure Security Agency, a component within DHS, is responsible for identifying cybersecurity vulnerabilities and coordinating mitigation actions across the federal government, including aviation cybersecurity research efforts.
- **Department of Defense.** DOD conducts its missions within the National Airspace System as both an airplane operator and, as delegated by the FAA, a provider of air traffic control and other air navigation services. DOD has the authority to certify its own airplanes, manage airspace, and provide air traffic control-related services in accordance with FAA requirements. DOD is also responsible for aviation security programs and initiatives that support national security. The Air Force has several on-going efforts to address cybersecurity risks, including the Air Force Aircraft Cyber Threat Working Group to facilitate a threat-informed and risk-based approach to aviation cybersecurity and multiple programs to identify and mitigate cybersecurity vulnerabilities in airplanes. In 2016, the Air Force stood up the Cyber Resiliency Office for Weapons Systems to integrate cyber resiliency into new airplanes and avionics programs, which includes cyber resiliency on fielded airplanes and associated avionics systems.

The National Strategy for Aviation Security, which the White House issued in December 2018, describes the federal government's approach to securing the aviation ecosystem, prioritizing protective activities, and interagency collaboration.[13] The strategy identifies strategic objectives and actions, and directs the development of supporting plans to enhance the security of the aviation ecosystem. Further, the strategy calls for coordination across federal agencies with national aviation security responsibilities.

Following the release of the national strategy, in May 2019 the Secretaries of Transportation, Homeland Security, and Defense chartered a task force called the Aviation Cyber Initiative as a mechanism to coordinate and collaborate among federal agencies, including intelligence agencies, to identify and reduce cybersecurity risks in the aviation ecosystem with industry stakeholders. The task force is co-chaired by the three departments. FAA represents the Department of Transportation (DOT) on the task force.

FAA's Process for Certifying the Airworthiness of Commercial Transport Airplanes

FAA has established a certification process for commercial transport airplanes to determine the flight safety, or airworthiness, of airplanes. In addition, FAA has a separate process for the certification of individual components, such as avionics systems, that is initiated by the manufacturer of that component.[14]

Under these processes, manufacturers, referred to as certification applicants (applicants), are responsible for understanding FAA's safety regulations[15] and how they apply to airplanes and airplane-system designs and technologies. Applicants are also responsible for recognizing and informing FAA of any potential design or technological threat to airworthiness, and for proposing and implementing mitigations to reduce threats to within acceptable levels.[16] FAA's certification process for commercial transport airlines is depicted in figure 2.

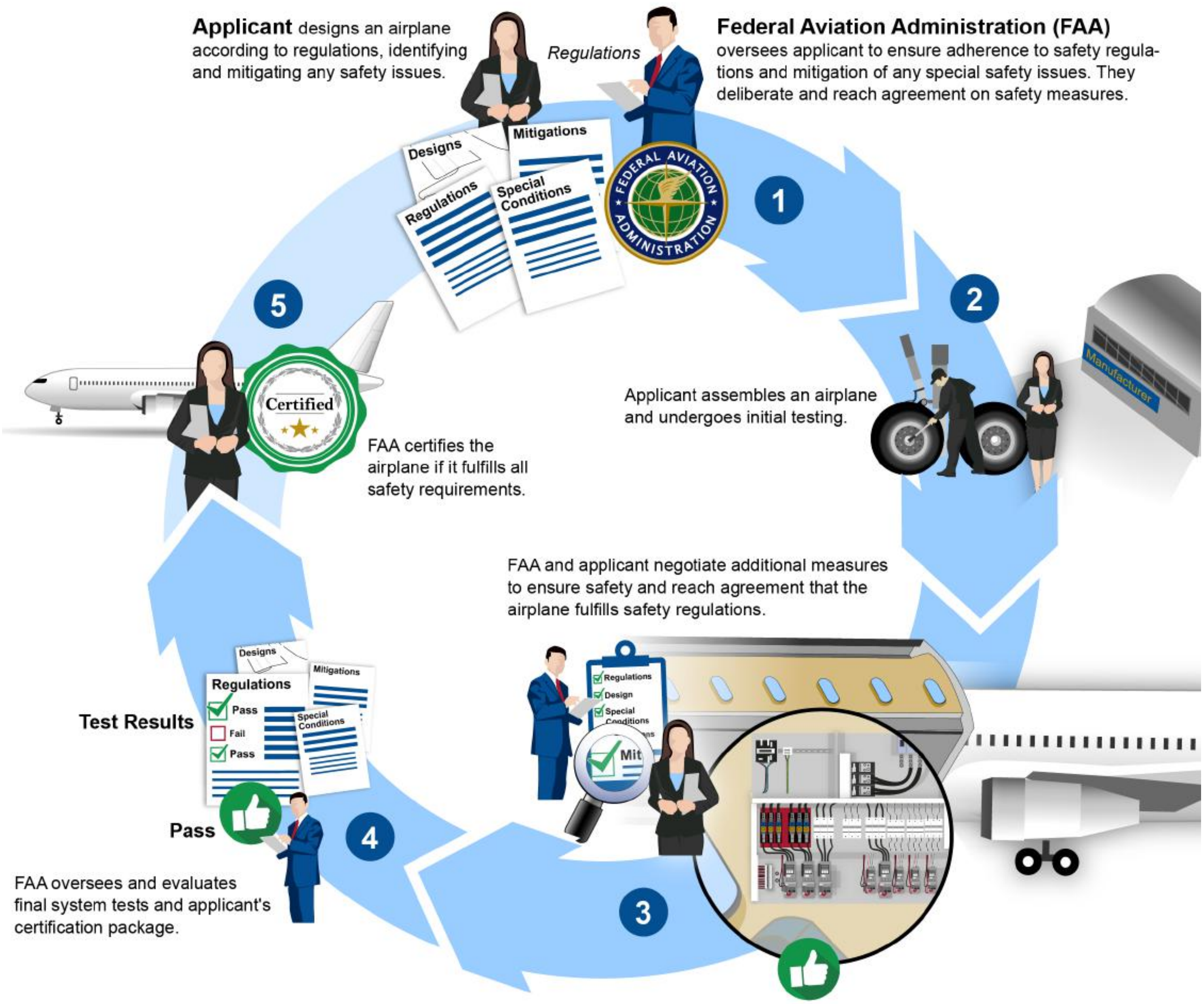
[13]White House*, National Strategy for Aviation Security of the United States of America,* (Washington, D.C.: December 2018).

[14]14 CFR Part 21—C*ertification Procedures for Products and Articles*.

[15]Regulations governing commercial transport airplane airworthiness are found in 14 CFR Part 25–*Airworthiness Standards: Transport Category Airplanes* and 14 CFR Part 26—*Continued Airworthiness and Safety Improvements for Transport Category Airplanes*. Other parts of Title 14 cover airworthiness standards for different categories of aircraft. Several of the Title 14 regulations are also referenced in FAA's Order 8110.4C *Type Certification.*

[16]FAA's current acceptable level of risk for airplane operations in the National Airspace System is a one-in-a-billion or less chance of injury to an individual member of the public.

Figure 2: FAA's Certification Process for Commercial Transport Airplanes



Source: GAO analysis of FAA documentation. | GAO-21-86

FAA's responsibility is to oversee that both the applicant's operational structure and its activities to design and manufacture an airplane adhere to regulations. FAA works with applicants during the certification process, which can last several years for new airplanes, to discuss and evaluate proposed airplane designs and technologies. FAA reviews and evaluates an applicant's ability to complete the certification process, design an airworthy airplane, manufacture that airplane, and provide the necessary guidance to, and oversight of, its eventual operator so that the airplane can be operated safely over its lifespan in service. FAA's certification process has been the subject of several recent reviews, including one by DOT's Special Committee to Review the Federal Aviation Administration's Airplane Certification Process, as well as a review by the DOT Office of Inspector General (OIG).[17]

For cybersecurity and other potential safety risks that are not specifically addressed in FAA's standing regulations, the agency uses Special Conditions. A Special Condition is a type of regulation that applies to a specific airplane design. FAA established a policy that is intended to provide guidance to the airplane certification offices regarding when to apply the Special Conditions to address cybersecurity vulnerabilities in airplane certification programs.[18] According to the policy, Special Conditions are issued for e-enabled airplane systems that directly connect to external services and networks under the following conditions:[19] 1) when the external service or network is non-governmental, 2) the airplane system receives information from the non-governmental service or network, and 3) the criticality of the airplane system is "major" or higher. Examples of non-governmental services include gatelink networks, public networks, wireless airplane sensors and sensor networks, cellular networks, and portable electronic devices, such as electronic flight bags.

FAA issues Special Conditions when its airworthiness regulations do not contain adequate or appropriate safety standards because of a novel or unusual design feature. Special Conditions have been developed for

[17]Department of Transportation, *Official Report of the Special Committee to review the Federal Aviation Administration's Aircraft Certification Process* (Washington, DC: Jan. 16, 2020), and Department of Transportation, Office of Inspector General, *Timeline of Activities Leading to the Certification of the Boeing 737 MAX 8 Aircraft and Actions Taken After the October 2018 Lion Air Accident,* AV2020037 (Washington, D.C.: Jun. 29, 2020).

[18]FAA Policy Statement, *Establishment of Special Conditions for Cybersecurity (*PS-AIR-21.16-02).

[19]E-enabled airplanes have one or more networks on board and require a connection to external networks (airborne and/or ground based) to support the flow of electronic data between the airplane and ground IT-systems to improve existing processes, such as maintenance, airline, and ground operations.

cybersecurity because, to date, the subject has not been addressed in the certification regulations governing commercial transport airplanes.

During the certification process, the applicant develops and provides FAA with risk assessments for the airplane as a whole and a risk assessment for individual Special Conditions, as needed. The assessment includes safety test results. FAA officials told us that, while agency engineers review these risk assessments, pose questions, and ensure that they understand all aspects of the risks and mitigations as presented by the applicant, the risk assessments are considered proprietary information and are ultimately returned to, and retained by, the applicant. FAA does not retain or use these risk assessments for any other purpose.

Starting in 2017, FAA began implementing a risk-based process to make determinations about the resources and level of involvement that the agency needs for each certification project. In this process to determine risk, FAA engineers are to review the plane's architecture holistically and determine how to address risks with airplane systems, including avionics. FAA's risk management process is embodied in its Safety Management System, a formal, top-down, organization-wide approach that includes systematic procedures, practices, and policies for the management of safety risk. While FAA requires operators to develop and implement processes based on the Safety Management System, it encourages, but does not require this approach for airplane manufacturers.[20]

As part of using Special Conditions, FAA and the applicant develop and agree on Means of Compliance, the name given for the steps the applicant must take to meet the Special Conditions and address associated potential risks to safety. For example, airplane cybersecurity standards that have been passed by RTCA (formerly the Radio Technical Commission for Aeronautics) and the European Organisation for Civil Aviation Equipment (EUROCAE)—aviation standards development organizations—are an FAA-accepted Means of Compliance for applicable Special Conditions. Any potential risks associated with the novel technologies addressed by the Special Condition must be mitigated to FAA's satisfaction prior to certification of an airplane.

During the certification process, if a Special Condition is found pertaining to internal electronic networking or external connectivity on an airplane,

[20]At the time of our review, FAA was in the process of reviewing a rulemaking that would require airplane manufacturers to have a Safety Management System.

the applicant must develop a network security guidance document specific to that airplane, which contains operator instructions for continued airworthiness once the airplane has been deployed. FAA is to review and approve this document as part of the applicant's certification package.[21]

When the FAA believes the applicant has fulfilled all the regulations that apply to its certification project, including Means of Compliance for Special Conditions, the applicant assembles a prototype airplane with all its subsystems in place. A final testing regime is developed by the applicant that is approved by FAA.

In the case of e-enabled airplanes, final testing includes the internal networking and cybersecurity controls needed to ensure that mitigations are in place and functioning properly.[22] FAA officials or their delegates are present during final testing to oversee the tests and review the results. Once the final tests have been completed and the certification package is complete, FAA reviews the certification package to determine:

- that all evidence has been provided that regulations and Special Conditions have been met,
- whether or not the airplane is functioning as intended and is airworthy, and
- whether the airplane may now be manufactured and sold by the applicant.

FAA can grant or deny certification based on its final review. Once the airplane has received certification approval from FAA, the airplane can be manufactured, sold, and delivered to customer airlines.

[21]Once the airplane has been certified, manufactured, and sold, the manufacturer is to provide the FAA-approved airplane network security guidance to its airplane customers (airlines) to assist in the continued protection and safe operation of the airplane. Any changes made to this guidance by the manufacturer must be updated in the airlines' Airplane Network Security Program within 30 days, so that the airlines can make any needed changes to their processes. According to a manufacturer, network security guidance has been updated in the past based on cybersecurity threat information received from the Department of Homeland Security.

[22]E-enabled airplanes have one or more networks on board and require a connection to external networks (airborne and/or ground based) to support the flow of electronic data between the airplane and ground IT-systems to improve existing processes, such as maintenance, airline, and ground operations.

Federal Laws, Directives, and Regulations Set Forth Responsibilities for Airplane Safety, Including Cybersecurity

In 2003, the Vision 100 Century of Aviation Reauthorization Act was enacted. This law introduced NextGen and led to the development of an integrated plan to support safety, security, mobility, efficiency, and capacity needs related to air transportation.

The *National Security Presidential Directive-47/Homeland Security Presidential Directive-16* (NSPD-47/HSPD-16), issued in 2006, established US policy, guidance, and implementation actions that supported national security and further coordination for the federal aviation security program and initiatives that built on the ongoing efforts of federal departments and agencies.[23] Specifically, these requirements included enhancing the sharing of information, coordinating efforts among executive departments and agencies, and integrating US allies and private sector partners into an improved global security framework. Further, NSPD-47/HSPD-16 called for the use of a risk-based approach to address information system-based attacks on air domain infrastructure.

In 2013, Presidential Policy Directive 21 (PPD-21) established national policy on critical infrastructure and resilience.[24] The directive identified 16 critical infrastructure sectors that were vital to the ability of the United States to function and that, if incapacitated or destroyed, would have a debilitating effect on national security, the economy, or public health and safety. Aviation is part of the Transportation Systems Sector, for which DHS and DOT are designated as co-sector-specific agencies.

In addition, the *FAA Extension, Safety, and Security Act of 2016* further promoted aviation safety by directing FAA to enhance the safety posture of commercial aviation by reducing cybersecurity risks to civil aviation.[25] Specifically, section 2111 calls for FAA to develop a comprehensive and strategic framework of principles and policies to reduce cybersecurity risks to the National Airspace System, civil aviation, and agency information systems using a total systems approach that takes into consideration the interactions and interdependence of different components of airplane systems and the National Airspace System. The

[23]The White House, National Security Presidential Directive 47/Homeland Security Presidential Directive 16 (Washington, D.C.: Jun. 20, 2006) (NSPD-47/HSPD-16), *National Strategy for Aviation Security* (Washington, D.C.: Mar. 26, 2007).

[24]The White House, Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013).

[25]*FAA Extension, Safety, and Security Act of 2016*, Pub. L. No. 114–190, §2111, 130 Stat. 625-627 (2016).

act tasked FAA to identify and address the cybersecurity risks associated with airplanes and airplane systems, create a threat model, and coordinate with aviation stakeholders, among other things.

In March 2019, the DOT Office of Inspector General reported that FAA had made progress meeting section 2111 requirements, but additional actions remained to implement cybersecurity initiatives across the agency. For example, FAA had completed a cybersecurity strategic plan, coordinated with other federal agencies to identify cyber vulnerabilities, developed the threat model, and established a research and development plan as required in section 2111. However, the report also stated that FAA had not completed a comprehensive and strategic cybersecurity framework of policies designed to identify and mitigate cybersecurity risks.[26]

In addition, section 506 of the 2018 FAA Reauthorization Act contains provisions related to securing airplane avionics systems.[27] Specifically, the provisions call for the Administrator to consider making revisions, where appropriate, regarding regulations related to airworthiness certification 1) to address cybersecurity for avionics systems, including software components; and 2) to require that aircraft avionics systems used for flight guidance or aircraft control be secured against unauthorized access via passenger in-flight entertainment systems through such means as the Administrator determines appropriate to protect the avionics systems from unauthorized external and internal access.

FAA officials stated that, following recommendations from the Aviation Rulemaking Advisory Committee, the agency had begun drafting regulations on aircraft systems information security protection that are intended to meet the intent of all section 506 provisions and to alleviate the need for security Special Conditions, once enacted. As of August 2020, the officials said they were in the process of determining timeframes to address the provisions.

[26]Department of Transportation, Office of Inspector General, *FAA Has Made Progress But Additional Actions Remain To Implement Congressionally Mandated Cyber Initiatives,* AV2019021 (Washington, D.C.: Mar. 20, 2019).

[27]Pub. L. No. 115-254, § 506.

Regulations Promulgated by DOT and FAA Established Responsibilities and Requirements Related to Airplane Security

Title 14 of the *Code of Federal Regulations* contains the rules and regulations promulgated by DOT and the FAA regarding aeronautics and space.[28] Included in Title 14 are the Federal Aviation Regulations, which include regulations for airplane design and maintenance, pilot and operator certification, and other matters. Part 21 of Title 14, Certification Procedures for Products and Articles, prescribes rules and procedural requirements for evaluating and certifying airplanes and parts. Certificate holders authorized to conduct operations under Part 21 must have an approved Safety Management System in place. Development of a Safety Management System is a formalized process that involves collecting and analyzing data on aviation operations to identify emerging safety problems, determine risk severity, and mitigate that risk to an acceptable level.

We Have Previously Reported on the Cybersecurity of Aviation Critical Infrastructure

Protecting the cybersecurity of critical infrastructure has been a longstanding challenge. Since 1997, we have designated information security as a government-wide high-risk issue. In 2003, we expanded this high-risk issue to emphasize the increased importance of protecting the information systems that support critical infrastructures.[29]

In 2004, we reported on the use of cybersecurity technologies for critical infrastructure protection.[30] We pointed out that FAA systems provided information to airplanes regarding weather, routes, terrain, and flight plans and that, if these systems did not function properly, there would be detrimental effects on the national economy and possibly on passenger safety.

In 2015, we reported that, as FAA transitioned to NextGen, FAA faced cybersecurity challenges in at least three areas: (1) protecting air traffic control information systems, (2) protecting airplane avionics used to operate and guide airplanes, and (3) clarifying cybersecurity roles and

[28]Title 14, Code of Federal Regulations. Aeronautics and Space.

[29]GAO, *High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures*, GAO-03-121 (Washington, DC: January 1, 2003).

[30]GAO, *Technology Assessment: Cybersecurity for Critical Infrastructure*, GAO-04-321 (Washington, DC: May 28, 2004).

responsibilities among multiple FAA offices.[31] We recommended that FAA assess the potential cost and timetable to develop an agency-wide cybersecurity threat model, include Aviation Safety as a full voting member of the Cybersecurity Steering Committee, and develop a plan to fund and implement the latest NIST security controls to mitigate the exposure of cybersecurity threats to NextGen systems. FAA subsequently implemented all three recommendations.

Further, in 2018, we reported on the national defense implications of DOD's and FAA's implementation of ADS-B.[32] In this report, we recommended 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.

As of July 2019, DOD and FAA had taken action to partially address the recommendation. Specifically, the agencies signed a memorandum of agreement to jointly develop solutions that mitigate ADS-B-related security risks and identify a path to fully implement the recommendation. In addition, in July 2019, FAA issued a rule permitting federal, state, and local governments that operate airplanes to turn off ADS-B transponders when conducting sensitive national defense, homeland security, intelligence, and law enforcement missions that could be compromised by transmitting real-time identification and positional flight information over ADS-B.

[31]GAO, *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).

[32]GAO, *Homeland Defense: Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft,* GAO-18-177, (Washington, D.C.: January 18, 2018).

Increasing Cybersecurity Risks to Avionics Systems, If Unaddressed, Could Impact Flight Safety as Airplanes Become More Connected

The aviation ecosystem faces increasing risks to flight safety from a complex and diverse set of threats. In particular, the growing connectivity between airplane networks and systems and various other systems via the Internet increasingly presents more opportunities for cyberattacks. For example, critical data used by cockpit systems could be altered, someone with authorized access could intentionally or unintentionally misuse flight data, commercial components within avionics systems could contain vulnerabilities that enable cyberattacks, and malevolent hackers could seek to disrupt flight operations with various types of attacks on navigational data.

It is important to note that, to date, there have been no reports of successful cyberattacks on an airplane's avionics systems. Airplane and avionics manufacturers have undertaken extensive measures to thwart any such attacks. However, the evolving cyber threat landscape, combined with the increasing use of internal networks on airplanes and the increasing connections between airplanes and external sources, could lead to increasing risks for future flight safety.

Cyber Threats That Could Impact the Aviation Sector Could Originate From a Variety of Sources

Among others, cyber threats pose increasing risks to avionics systems. Cyber threats, which include any circumstances or events with the potential to have an adverse impact on cybersecurity, can be intentional or unintentional and can come from a variety of sources. Unintentional threats can come from anyone and anywhere, while intentional threats can include criminal groups, hackers, disgruntled employees, foreign nations engaged in espionage and information warfare, drug trafficking organizations, and terrorists. According to the *2019 Worldwide Threat Assessment of the U.S. Intelligence Community,* nations, criminal groups, and terrorists pose the most significant cyber threats to U.S. critical infrastructure.[33]

As with all of the nation's infrastructure, the source of a cyber threat within the aviation subsector could include any of the following:

- **Cybercriminals.** Criminal groups, including organized crime organizations, use cyberattacks for monetary gain. For example, criminals have used cyber techniques to attack ground-based systems and commit financial crimes against aviation-related

[33]Daniel R. Coats, Director of National Intelligence, *Worldwide Threat Assessment of the U.S. Intelligence Community*, testimony before the Senate Select Committee on Intelligence, 116th Cong. 1st session, Jan. 29, 2019.

companies and their customers. One such attack occurred from 2016 to 2017 when the Sabre reservations system experienced a data breach that resulted in stolen personal consumer data.[34]

- **Nations.** Nations, including nation-state, state-sponsored, and state-sanctioned groups or programs, may use cyberattacks as part of covert activities to gather information about individuals, government organizations, and private sector entities. Nation states may also leverage their espionage and reconnaissance activities to develop capabilities for future computer network attacks, which could be designed to damage, destroy, or disrupt computers and networks. For example, in 2019, the Airbus company experienced a series of cyberattacks via the computer systems of its engine suppliers.
- **Terrorists.** Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, inflict mass casualties, weaken the economy, and damage public morale and confidence. While there have not yet been reported terrorist cyberattacks on avionics systems, aviation has long been and likely remains a target for terrorist groups.
- **Insiders.** Insiders are entities with authorized access to information systems who have the potential to cause harm—intentionally or unintentionally—through destruction, disclosure, modification of data, or a denial of service attack.[35] Within the aviation industry, these insiders include personnel employed by airports, airlines, and other aviation stakeholders, including vendors, suppliers, and sub-contractors, that may have access to airplanes or secure areas in airports or in sensitive locations off the airport site. Insiders in the aviation industry pose a particular threat because of their proximity to and unique knowledge of aviation, including the systems and components on an airplane that could be used to disrupt flight operations.

[34]From August 2016 to March 2017, Sabre—a company that processes reservations for hotels and airlines—experienced a data breach that compromised data including credit card numbers, addresses, and other personal consumer data.

[35]A method of attack that denies system access to legitimate users without actually having to compromise the targeted system. From a single source, the attack overwhelms the target computers with messages and blocks legitimate traffic. It can prevent one system from being able to exchange data with other systems or prevent the system from using the Internet.

A Range of Potential Vulnerabilities Could Affect Avionics Systems

Avionics systems, which are increasingly interconnected with other airplane systems and with external systems, face a wide variety of potential vulnerabilities if proper protections are not in place. As highly interconnected systems, unprotected avionics systems could be vulnerable to a variety of potential cyberattacks. Vulnerabilities could occur due to (1) modifications (patches) to commercial software not being applied, (2) insecure supply chains, (3) malicious software uploads, (4) outdated systems on legacy airplanes, and (5) flight data spoofing attacks.[36]

Commercial Software May Not Always Be Updated Promptly to Correct Flaws

Airplanes are increasingly reliant on complex software that may have security vulnerabilities potentially could be exploited by those with criminal intentions. Airplane systems may be built with commercial off-the-shelf software and components, which may support a variety of functions on board the airplane, including the maintenance and crew devices that connect to them. If not completely isolated from external networks, such software will likely need to be updated on a continuous basis to respond to newly-identified vulnerabilities and changing threat scenarios. While commercial-off-the-shelf software have built-in mechanisms to protect the availability and integrity of the software code, industry officials we spoke with cited potential software vulnerabilities as a key concern.

Software that is not updated in a timely fashion may be vulnerable to cyber exploitation. While software patches are essential to mitigating this risk, industry officials reported that software developers are often slow to issue a fix. For example, the officials stated that modifying one line of safety-critical flight software can take a year and cost around one million dollars due to the amount of testing and review that is generally required. Long update cycles that leave unpatched flaws exposed create cybersecurity risks, which could have safety implications. Further, GAO has previously reported that attacks on unpatched software vulnerabilities in non-aviation systems have caused billions of dollars in damage.[37]

[36]Spoofing is the process of disguising a communication from an unknown source as being from a known, trusted source.

[37]GAO, *Information Security: Effective Patch Management is Critical to Mitigating Software Vulnerabilities*, GAO-03-1138T (Washington, D.C.: September 10, 2003).

Vulnerabilities Could Be Introduced in the Supply Chain If It Is Not Assessed or Components Are Not Properly Tested

A supply chain is a complex, globally distributed, interconnected set of resources and processes that extends across multiple entities. Within the aviation industry, the supply chain is a global ecosystem of tiers of suppliers, such as original equipment manufacturers; maintenance, repair, and overhaul providers; and customers, including air carriers—all of which could contain cyber vulnerabilities within their systems.

Without adequately assessing the security practices of manufacturers and thoroughly testing electronic components, cybersecurity vulnerabilities can be introduced to avionics systems at multiple points within insecure supply chains. This could potentially result in a range of impacts, from allowing an adversary to take control of a system to decreasing the availability of materials needed to develop a system.

Within commercial airplanes, software and hardware compromised by malware could enable malicious persons to perpetrate exploits after the compromised parts are installed on the airplane. Additionally, supply chain failures could create exploitable defects. Airplanes feature electronic hardware components known as line replaceable units,[38] which could be compromised and adversely affect flight operations. It is also possible that counterfeit line replaceable units containing malware or other security vulnerabilities could be inadvertently installed.

Systems that Connect to Avionics Could Spread Malicious Software

Activities carried out by air carriers and airports related to the operations and maintenance of airplanes could also pose vulnerabilities by facilitating the installation of malicious software in avionics systems. The systems that connect the airplane to maintenance and operations functions might also connect to the avionics systems onboard an airplane. For example, malware could be installed on an electronic flight bag (EFB), which is an airline-owned and operated electronic device used by pilots and flight crews. Currently, EFBs can be standalone devices, such as a tablet, or integrated with systems such as the flight management system. Previously, these devices had no connectivity to other systems in the flight control domain when an airplane was in flight. However, vendors are developing EFBs with the capability to communicate instructions directly to flight management systems during a flight. Such EFBs, if connected to the airplane and infected with malware, could enable denial-

[38] A line replaceable unit is a modular component of an airplane that is designed to be replaced quickly during maintenance activities to minimize downtime and restore a system to operational readiness.

of-service attacks or intrusion to other connected on-board systems, such as flight management systems.

With respect to airport operations, gatelink systems—high capacity data transfer/communications links that transmit data between airplanes and the airport—could also be vulnerable. Gatelink systems are positioned in the airport near the gate and interface with an airplane's avionics after the airplane lands. If these systems are infected by malware, they could affect key airport operations. For example, after an airplane lands, it uses gatelink systems to automatically transfer data from the airplane to passenger terminals, maintenance operations, baggage handling and ground support, among other airport operations. A compromised gatelink system could cause disruptions across these airport operations.

Legacy Systems on Airplanes May Lack Up-to-Date Cybersecurity Controls

Cybersecurity risks may increase when legacy airplanes are upgraded or retrofitted with newer avionics systems. As previously discussed, avionics systems on older airplanes have generally not been connected to the internet; therefore, they were not built with cybersecurity controls. As these legacy airplanes get retrofitted with newer systems and enhanced connectivity, it is important to ensure that software and upgrades to existing systems are free of vulnerabilities.

Industry officials told us that upgrading legacy systems to fit the current operational environment can present challenges because vulnerabilities could be introduced as the airplanes are updated to connect with Internet Protocol (IP)-enabled external networks, such as satellite communications and wireless networks.[39] GAO has previously reported that legacy systems are increasingly difficult to protect from cybersecurity vulnerabilities.[40]

Airplane Communications Systems Could be Vulnerable to Flight Data Spoofing

Airplanes rely on various forms of communication to perform key functions, such as sending and receiving data related to flight routes, navigation, and landing. These communications systems could be vulnerable to spoofing, the process of disguising a communication from an unknown source as being from a known, trusted source.

[39]Internet Protocol defines how data moves across networks. IP-enabled networks refer to those that were originally designed for non-IP-based communications, but which have been updated to provide IP-network-based communications.

[40]GAO, *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems*, GAO-19-471 (Washington, D.C.: June 11, 2019).

Airplanes use a communications network known as ACARS to transmit messages from the airplane to ground-based users (such as air traffic control) and to send and receive flight plans and other messages. ACARS transmissions are unauthenticated and, thus, could be intercepted and altered or replaced by false transmissions. For example, unprotected ACARS communications could be spoofed and manipulated to send false or erroneous messages to an airplane, such as incorrect positioning information or bogus flight plans. In addition, many airplanes today use ACARS to transmit flight plans through the flight management system, an avionics system that manages navigation routes.

In addition, ADS-B is a surveillance technology in which an airplane determines its position via satellite navigation and periodically broadcasts it, enabling the airplane's location to be tracked by air traffic controllers and others. ADS-B consists of two distinct airplane information services: ADS-B Out and ADS-B In. ADS-B Out uses an airplane's avionics equipment to broadcast the airplane's position, altitude, and velocity to any ground, air, or space-based receiver. ADS-B In is the technology that enables airplane receivers to have direct access to information broadcast through ADS-B Out transponders.

The data that are transmitted using ADS-B are unencrypted and unauthenticated, which raises security concerns. Potential spoofing scenarios that could adversely affect flight operations include alterations to an airplane's location information, which could make the airplane seem to disappear from the skies, thus preventing an ADS-B ground station from receiving its true location information. Spoofing could also affect the airplane's situational awareness by creating the appearance of nearby "ghost" airplanes, which could cause a pilot to alter an airplane's course. While air traffic controllers could help a pilot resolve such a scenario, FAA and researchers are aware that ADS-B spoofing poses a threat and are working on ways to mitigate it.

As another example, security researchers have shown that an airplane's instrument landing system, which provides crucial data such as angle of descent and alignment with the runway to the pilots as they land (particularly in dark and foggy conditions), can be attacked by overcoming the physical access controls in place on the ground and by intercepting and spoofing the radio signals that the landing system relies on. Spoofing these signals can make the landing instrument show an airplane's flight track, which could cause a pilot to alter the airplane's flight angle or descent rate, thus creating a safety hazard.

Airframe and Avionics Manufacturers Have Taken Steps to Mitigate Cybersecurity Vulnerabilities to Avionics Systems

Airframe and avionics manufacturers have put extensive hardware and software protections in place to mitigate cybersecurity vulnerabilities, thus significantly reducing the overall risk to flight safety. For example, onboard networked systems on new airplanes are segregated into several independent domains. Each segregated domain contains only the system functions, data pathways, and data necessary to perform the functions established for that domain. In addition, the flight control domain system functions do not require input from any systems in the passenger cabin, so flight control systems are isolated from receiving any electronic transmissions from the passenger cabin. In contrast, providing flight status information from the cockpit to the passengers in the cabin is desirable, so a one-way link allowing the transmission of this data to the passenger cabin is allowed.

Hardware protections include, among other things, one-way buses to control the direction of data flow and built-in, automatic switches that control when systems are activated. For example, airplanes use a weight switch in the wheels to verify that an airplane is on the ground before it will allow software changes to be uploaded to an airplane's avionics systems. Such a system prevents software changes while an airplane is in flight. These hardware protections are similar to those used in industrial control systems. Software protections include firewalls, which limit the traffic that passes through a network, and built-in layers of redundancy in avionics software that are designed to provide a high degree of reliability and prevent failures during flight. In addition, manufacturers subject flight-critical avionics components and systems to extensive testing to minimize the possibility of software flaws.

Actions taken by manufacturers to mitigate current risks to avionics systems have been successful insofar as no known cybersecurity attacks, to date, have occurred on an operational airplane. However, the increasing use of internal networks on airplanes and the increasing connections between airplanes and other external systems, combined with the evolving cyber threat landscape, will likely lead to increasing risks for future flight safety that will require increasing vigilance to maintain the same level of cybersecurity assurance.

FAA Has Not Fully Implemented Key Practices to Oversee Industry Mitigation of Avionics Cybersecurity Risks

Implementing effective cybersecurity requires organizations to identify, prioritize, and manage cyber risks across the enterprise. To help organizations improve their cybersecurity posture, the National Institute of Standards and Technology (NIST) established the *Framework for Improving Critical Infrastructure Cybersecurity* (commonly referred to as the NIST Cybersecurity Framework).[41] Further, we have identified practices for an effective oversight program that incorporates risk management principles from NIST as part of an effective oversight program.[42] These elements include (1) an assessment of risks, (2) training, (3) independent testing, and (4) ongoing monitoring.

FAA is responsible for the safety and oversight of commercial aviation, and it recognizes avionics cybersecurity as a potential airworthiness and safety issue for e-enabled commercial transport airplanes. However, the agency has not fully addressed the four elements that are necessary to ensure the effective implementation of a risk-based cybersecurity oversight program. Without fully addressing these elements, FAA will not be able to ensure that it is effectively overseeing the implementation of cybersecurity controls that address the risks to avionics systems on commercial airplanes.

FAA Has Not Assessed Avionics Cybersecurity Risks to Determine Priorities for Its Oversight Program

As previously mentioned, the *FAA Extension, Safety, and Security Act of 2016* tasked FAA to identify and address the cybersecurity risks associated with airplanes and airplane systems.[43] Further, as discussed in NIST guidance, a risk assessment is one of the fundamental components of an organizational risk management process.[44] Risk assessments are used to identify, estimate, and prioritize risk to organizational operations, such as mission and function. Further, they inform and support how to implement the other aspects of risk management: training, independent testing, and monitoring.

[41]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1. (Gaithersburg, MD: April 2018).

[42]GAO, *Cybersecurity: Office of Federal Student Aid Should Take Additional Steps to Oversee Non-School Partners' Protection of Borrower Information,* GAO-18-518 (Washington, D.C.: Sept. 17, 2018).

[43]*FAA Extension, Safety, and Security Act of 2016*, Pub. L. No. 114–190, §2111, 130 Stat. 625-627 (2016).

[44]NIST Special Publication 800-39, *Managing Information Security Risk* (Gaithersburg, MD: March 2011).

According to FAA's *Strategic Plan* for fiscal years 2019 through 2022, the agency has adopted NIST's Cybersecurity Framework to reduce aviation critical infrastructure risk.[45] In addition, it has performed risk assessments for its enterprise and mission-related systems, including its numerous air traffic control systems.

However, FAA has not conducted an assessment of the risks to avionics systems to determine the relative priority of cybersecurity risks to avionics systems versus other safety concerns in its oversight program. While the agency uses its Safety Management System to assess risks for certification projects, this form of risk assessment is only at the certification project-level and, therefore, does not inform a larger agency strategy to oversee industry actions to address avionics cybersecurity risks.[46]

Major aviation industry stakeholders have raised concerns about the sufficiency of FAA's oversight of avionics cybersecurity. Although no cyberattacks on, or breaches of, avionics systems have been reported, FAA, its international counterparts, and stakeholders throughout the aviation ecosystem recognize that cybersecurity risks can pose safety risks. As previously discussed, technological developments make it clear that the risks to avionics are likely to increase. Therefore, assessing and mitigating avionics cybersecurity risks will likely also become more important to ensuring the safety of the National Airspace System. The DOT Office of Inspector General issued a report in 2019 that found that FAA had not completed a comprehensive and strategic cybersecurity framework of policies designed to identify and mitigate cybersecurity risks.[47]

Without an assessment of the relative priority of avionics cybersecurity risks within FAA's oversight program, the agency has relied on Special Conditions when certifying the airworthiness of commercial airplanes. According to FAA officials, the use of Special Conditions has been adequate to address such risks. However, because Special Conditions

[45]FAA Strategic Plan, FY 2019-2022.

[46]A Safety Management System is a formalized process that involves collecting and analyzing data on aviation operations to identify emerging safety problems, determining risk severity, and mitigating that risk to an acceptable level.

[47]Department of Transportation, Office of Inspector General, *FAA Has Made Progress But Additional Actions Remain To Implement Congressionally Mandated Cyber Initiatives*, AV2019021 (Washington, D.C.: March 20, 2019).

are unique requirements that are developed for individual airplanes and are not standardized as part of FAA's regulations, they do not provide industry applicants with overall clarity regarding FAA's oversight focus, and their use could potentially result in inconsistent implementation of cybersecurity controls across airplane certification projects. Industry stakeholders told us that standardized rulemaking on avionics cybersecurity safety could provide applicants with clearer direction when developing airplane designs and moving through the certification process.

FAA officials also said they were aware of past inconsistencies in the certification process and had revised the process by clarifying FAA's role and the applicant's responsibility, including processes for the agency's early engagement with applicants when developing new technologies, among other things. However, they agreed that a permanent regulation would provide greater overall clarity regarding cybersecurity oversight. FAA officials told us that the agency is preparing internally for new rulemaking on avionics cybersecurity that would codify the use of commonly used Special Conditions in June 2021.

In contrast to FAA, actions taken by the European Union Aviation Safety Agency—FAA's European counterpart—indicate a greater focus on avionics cybersecurity risks. Specifically, in September 2019, a coordinating committee released its Strategy for Cybersecurity in Aviation, which states that avionics cybersecurity is a safety issue and that systems operating in the airspace should be reevaluated over time to ensure that the original assumptions regarding cybersecurity protections still hold. Industry stakeholders have stated that the European Union Aviation Safety Agency's efforts to publish guidance on cybersecurity has put it ahead of FAA in the area of avionics cybersecurity and has shown the kinds of actions that are possible to ensure that appropriate attention is focused on the subject.

In addition, the International Civil Aviation Organization is currently developing policies and procedures to reduce potential opportunities for cyberattack in a digitally connected aircraft environment. Specifically, the processes for digital identity assurance for information that is exchanged between ground-to-ground systems and ground-to-air systems over different networks. Until FAA assesses the cybersecurity risks to avionics systems versus other safety concerns, it may not be able to appropriately strengthen its oversight program specific to avionics systems cybersecurity issues.

FAA Does Not Have a Training Program for Avionics Cybersecurity Oversight

To ensure the appropriate implementation of controls to mitigate cybersecurity risks, staff must have the skills necessary to address cybersecurity risks. The NIST *Cybersecurity Framework* states that training is a critical and indispensable component of implementing a cybersecurity program. Further, specific to aviation, the International Civil Aviation Organization has called for the aviation sector, including regulators, to take tangible steps to increase the number of personnel that are qualified and knowledgeable in both aviation and cybersecurity.

FAA does not currently have a staff training program specific to avionics cybersecurity and none of the agency's certification staff are required to take cybersecurity training tailored to their oversight role. While FAA officials said the agency has some personnel with the aviation and cybersecurity expertise needed to conduct certification reviews, it does not have dedicated staff with direct responsibility to oversee cybersecurity.

According to FAA officials, few of the agency's certification engineers have received cybersecurity training, and, when training was provided, it was limited. For example, staff from FAA's Aviation Safety office took industry training courses related to aviation cybersecurity standards. The officials stated that inadequate resources and limited cybersecurity staff have prevented them from undertaking further initiatives related to avionics cybersecurity training. They acknowledged that cybersecurity expertise is a challenge for FAA's workforce but stated that the current level of expertise has not hindered the agency's ability to conduct certification oversight.[48]

Industry stakeholders across the aviation sector expressed concern that FAA lacks personnel with cybersecurity expertise and generally agreed that the agency's certification workforce needs additional cybersecurity skills to effectively oversee avionics cybersecurity. The stakeholders emphasized that cybersecurity expertise is different than aviation engineering expertise, and that FAA staff may not have sufficient training

[48]As required by Section 549 of the FAA Reauthorization Act of 2018, Pub. Law 115-254, 132 Stat. 3186, 3378 (Oct. 5, 2018), the FAA Administrator was to enter into an agreement with the National Academy of Sciences to study the FAA's cybersecurity workforce. This study was to (1) examine FAA's cybersecurity workforce challenges, (2) review FAA's current strategy for meeting those challenges, and (3) provide recommendations related to strengthening FAA's cybersecurity workforce, including consideration of its size, quality, and diversity.

or knowledge to independently recognize cybersecurity vulnerabilities in airplane operating systems.

The stakeholders added that cybersecurity expertise varies among FAA officials and, as a result, the certification process has not always been guided by appropriate avionics cybersecurity expertise. For example, industry representatives told us that when FAA engineers reviewed cybersecurity-related documents or test results, it was unclear whether they understood the results or the applicant's explanations. According to two stakeholders, in cases where manufacturers provided technical information to FAA certification engineers, the engineers often sought out other subject matter experts to review, understand, and explain the information to them.

In January 2020, FAA officials told us that they were in the process of developing a cybersecurity training program for engineers who work on FAA certification projects associated with airplanes and avionics equipment connectivity. FAA estimated that the program would be available in December 2020 as an online learning course. However, lacking an avionics cybersecurity risk assessment to gauge oversight priorities, FAA cannot ensure that its staffing and associated training program are adequately tailored to meet its oversight needs. Until FAA establishes a staffing and training program appropriately tailored to avionics cybersecurity and based on the results of a risk assessment, the agency may not have the expertise necessary to address the increasing cybersecurity risks to these systems.

FAA Has Not Issued Guidance Regarding Independent Avionics Cybersecurity Testing For Airplane Certification

To ensure that cybersecurity controls have been implemented appropriately, it is important that they are independently tested. NIST guidance requires organizations to ensure that security assessment results are obtained with the appropriate level of independence, are current, and are relevant to the determination of security control effectiveness.[49]

Currently, FAA does not have specific guidance regarding independent avionics cybersecurity testing during the certification process. FAA officials told us that, in the final days before an airplane design is certified as airworthy, an assembled airplane undergoes final testing of all its systems and sub-systems, including cybersecurity testing. The

[49]NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Rev. 4 (Gaithersburg, MD: April 2013).

manufacturer proposes the testing requirements in advance and negotiates with FAA on testing scenarios that show whether the requirements have been fulfilled.

During the cybersecurity tests, FAA engineers are present to observe and review the results. Penetration test results must show that the systems and cybersecurity protections meet all requirements.[50] Finally, the results are bundled into the final certification package that FAA program managers review and approve to indicate that the systems have achieved compliance.

FAA officials told us that inspectors do not review system schematics to look for potential cybersecurity issues but, instead, rely on the applicant to explain the systems, identify any cybersecurity issues, explain how the issues are addressed or mitigated to meet requirements, and explain the test results that confirm the mitigating controls have been implemented correctly. In at least one instance, representatives from an airframe manufacturer stated that FAA required them to work with an independent cybersecurity testing company to perform testing on a particular airplane model to ensure the validity of the cybersecurity protections. However, the current certification process does not standardize the use of independent testing.

Industry experts told us that having an independent entity involved in testing is valuable to bring a fresh set of viewpoints and assumptions to the cybersecurity review. The experts stated that, generally, the team that developed the airplane is not independent enough to bring that fresh perspective to testing. Although keeping FAA's involvement at a higher level of oversight adheres to the concept of deferring to the manufacturer on technical expertise, it does not align with the concept of independent testing of cybersecurity controls.

Most of the manufacturers of commercial transport airplanes and avionics systems we spoke with told us that engaging independent cybersecurity testers is not a standard product development practice for them. These manufacturers' officials all told us that they test their avionics systems and airplane internal networking systems in-house for cybersecurity vulnerabilities and apply appropriate controls. Representatives of one

[50]NIST defines penetration testing as security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques that would be used by actual attackers.

manufacturer told us they contracted out for independent testing of airplane systems on that manufacturer's own initiative, while representatives of another manufacturer told us that they contracted out for independent testing when directed to do so by FAA. Officials at a third manufacturer said the company acquired a cybersecurity testing company specifically to keep independent testing in-house.

Further, these officials are aware that cybersecurity threats are increasing and told us that they are trying to engage more with the security community to test and ensure the cybersecurity of their airplanes. For example, Airbus officials said they allow controlled third-party penetration testing during the development process of their airplanes. Specifically, Airbus involved security agencies from France, Germany and the United Kingdom in a series of cyber penetration tests, in addition to conducting tests on airplane systems by a separate, independent Airbus cyber team. Moreover, Boeing recently allowed controlled third-party testing during the certification process for its airplane in response to a request from the FAA. According to Boeing officials, the external third-party cybersecurity experts provided validation and attestation for airplane safety and airworthiness cyber certification projects. In response to a security's researcher's claims in 2019, Boeing also recently set up a formal vulnerability disclosure program, including a website for security researchers to report potential vulnerabilities directly to the company.

Most airline officials we interviewed expressed concerns about the extent to which FAA's certification process addresses avionics cybersecurity. In addition, FAA does not require manufacturers to disclose to the airlines the extent of independent testing or the types of tests that were conducted. Airlines are, thus, at a disadvantage in ensuring the cybersecurity of their airplanes because they do not know the extent of testing that has occurred or whether independent testing took place. For example, representatives from one airline stated that this lack of transparency hinders their ability to perform certain functions, such as comprehensive threat analysis, that would allow for thorough threat identification and mitigation. Until FAA issues guidance regarding independent cybersecurity testing of commercial transport airplanes, it may be unable to ensure that commercial transport airplanes are tested with a necessary level of independence.

FAA's Monitoring Process for Avionics Cybersecurity in Deployed Airplanes Does Not Include Periodic Independent Testing

Because cybersecurity risks are continually evolving, it is important for organizations to conduct ongoing monitoring, including recurring testing of deployed systems, such as airplane avionics systems. In many cyber environments, ongoing monitoring can facilitate near real-time risk management. NIST states that, while conducting a thorough point-in-time assessment of the deployed security controls is necessary, it is not a sufficient practice to demonstrate due diligence of systems security.[51] NIST recommends that continuous monitoring of threats, vulnerabilities, and security controls effectiveness be conducted to provide situational awareness.

FAA's monitoring of the implementation of avionics cybersecurity controls in airplanes that are deployed in active service with air carriers does not include policies or procedures for periodic testing. FAA's ongoing oversight of airlines' fleet safety includes monitoring airlines' adherence to the Aircraft Network Security Programs they have filed with FAA for the airplane models in their fleet.[52] The Aircraft Network Security Program is based on guidance provided to the airline by the manufacturer when the airplane is purchased. It includes instructions on maintenance of an airplane's internal networks and external connections and a forensic analysis process to address safety-related cybersecurity incidents. The guidance requires cybersecurity incident reporting, but there is no specification for periodic testing as a preventive measure to reduce risks.

DOD and industry officials told us that periodic testing is critical to ensuring the continued effectiveness of cybersecurity controls. According to the DOD officials, the Air Force conducts ongoing monitoring of its commercial derivative aircraft by conducting reoccurring cybersecurity risk assessments.[53] Air Force's Commercial Derivative Aircraft Division is responsible for the modification and sustainment of this aircraft type and

[51]NIST SP 800-39.

[52]An Aircraft Network Security Program is a document that is required for airplanes certified with a Special Condition requiring operator actions to mitigate electronic security risks. Its purpose is for the operator to ensure that security protection prevents unauthorized access by external sources, that appropriate risk mitigation strategies are implemented, that inadvertent or malicious changes to the airplane network are prevented, and that unauthorized network access from sources onboard the airplane are also prevented. The airline bases its Aircraft Network Security Program on the FAA-approved airplane network security guidance provided by the airplane manufacturer. The airline and manufacturer often work together to ensure the document is complete and accurate.

[53]Commercial derivative aircraft are commercial type-certified aircraft that are modified to meet military mission requirements.

ensures cybersecurity compliance through recurring assessment of “as installed” avionics for its commercial derivative aircraft fleets. Likewise, various industry stakeholders told us that periodic testing should have a role in ensuring that avionics cybersecurity controls continue to be effective. One manufacturer told us that it is developing a plan to conduct periodic reviews, including cybersecurity testing of its deployed airplanes.

Existing airplane avionics systems include embedded mechanisms for monitoring by the manufacturer. For example, these systems have multiple layers of redundancy that include built-in tests and fault monitoring for networks for quick failure detection, among other things. However, without FAA-approved policies or procedures, periodic cybersecurity testing of deployed airplanes, such as penetration testing, is particularly difficult for airlines because such testing could inadvertently cause alterations to an airplane’s software systems that may be difficult to correct. Any such misconfiguration from the originally certified configuration could invalidate the airplane’s airworthiness certificate, thus, rendering the airplane inoperable. Both airlines and airframe manufacturers expressed concerns that penetration testing could negatively affect an airplane’s network and systems configurations. Further, misconfigurations that could affect an airplane’s airworthiness might not become apparent until an airplane is put back into service and a problem occurs.

In the absence of FAA guidance, representatives from one airline stated that they have formed a group with four other airlines to try to determine how to safely perform independent testing on their respective fleets. However, the representative stated that, without guidance from FAA, these efforts are not enough to ensure the periodic cybersecurity testing will not compromise the airworthiness of their fleets.

All of the airline representatives we spoke with supported periodic, ongoing testing of avionics systems on their airplanes to ensure their airworthiness. A number of airline representatives said that increased information sharing from manufacturers about how their systems function would be useful to airlines when gauging the ongoing cybersecurity status of their airplanes. Specifically, representatives from one airline stated that, while the network security guidance provided by the manufacturer explains the functions of the airplane’s systems, it does not include critical information, such as details of what testing was conducted and key assumptions made during the testing process. Such information is important for the airlines to have as they develop independent testing programs.

Industry representatives told us that over the last year they have begun conversations about how and when to use periodic testing to review the cybersecurity status of deployed avionics systems. The representatives told us that these discussions are ongoing among airlines, manufacturers, and FAA. Until FAA develops policies and procedures for periodic testing as part of its monitoring process, it may be unable to ensure that cybersecurity controls remain effective in mitigating evolving threats in deployed airplanes.

FAA Has Taken Steps to Coordinate Cybersecurity Issues, but Has Not Focused on Avionics Cybersecurity Risks

FAA coordinates with other federal agencies and private sector stakeholders to address cybersecurity risks that have been identified by industry or other federal agencies. However, internally, the agency's activities do not include initiatives focused on avionics cybersecurity, because FAA has not established an organizational priority for addressing avionics cybersecurity risks. Further, FAA's internal coordination activities do not fully reflect key collaboration practices, including establishing a mechanism to track issues and dedicating resources to avionics cybersecurity oversight.

FAA Participates in External Coordination Efforts to Address Avionics Cybersecurity with Public and Private Stakeholders

Coordination across the public and private sectors is of critical importance in ensuring cybersecurity within the aviation ecosystem. The President's *National Strategy for Aviation Security* (NSAS), issued in 2018, was intended to help strengthen aviation security from physical and cyber threats. It called for a coordinated effort between government and the private sector to reduce cyber threats and ensure a resilient aviation ecosystem.[54]

The Secretaries of Transportation, Defense, and Homeland Security stood up the Aviation Cyber Initiative (ACI) in May 2019 as a collaborative effort designed to respond to the needs identified in the NSAS. FAA is one of three agencies that jointly chair the ACI, in addition to DHS and DOD. The three agencies intend ACI to be a forum to identify, assess, and analyze cyber threats, vulnerabilities, and consequences and to engage with stakeholders across the aviation ecosystem on activities for reducing cyber risks.

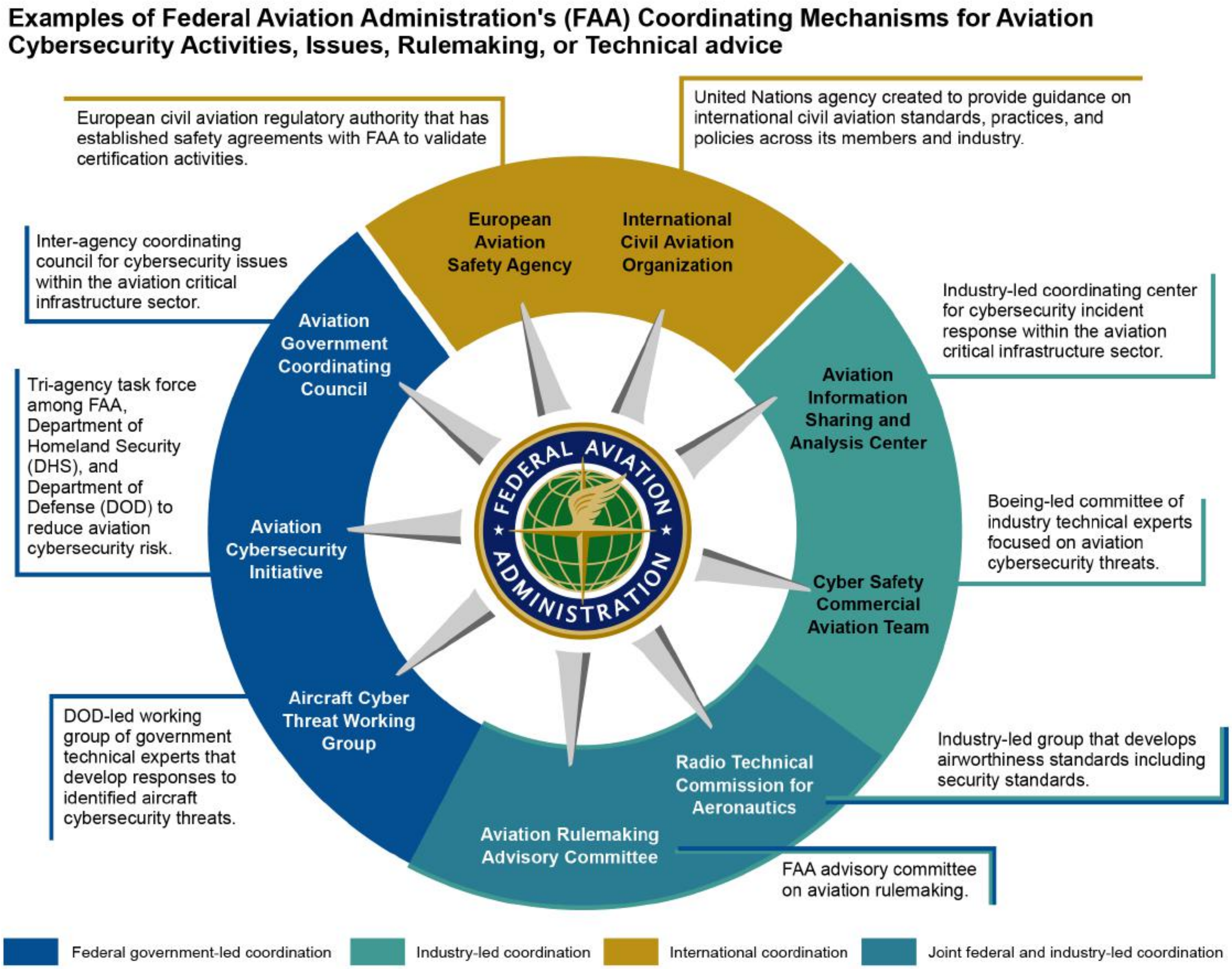
In addition to the ACI, other industry- and government-led coordination groups have been organized, with FAA endorsement and participation. For example, Boeing, through the Aerospace Industries Association,

[54]The White House*, National Strategy for Aviation Security of the United States of America,* (Washington, D.C.: December 2018).

established a Cyber Safety Commercial Aviation Team of subject matter experts, and participants from the public and private sectors to focus on airplane cybersecurity issues across the aviation ecosystem, including cybersecurity safety risks associated with avionics systems. As another example, FAA also participates in the Aviation Information Sharing and Analysis Center, which is an industry-led coordinating center that responds to cybersecurity incidents across the aviation critical infrastructure center. FAA's mechanisms for externally coordinating on aviation cybersecurity issues, which are consistent with leading federal collaborative practices to define short and long-term outcomes, identify key participants, and share and leverage resources, are shown in figure 3.[55]

[55]GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, GAO-12-1022 (Washington, D.C.: Sept. 27, 2012).

Figure 3: Examples of FAA's External Coordinating Mechanisms for Aviation Cybersecurity Activities, Issues, Rulemaking, or Technical Advice



Source: GAO analysis of FAA and industry documentation. | GAO-21-86

While FAA leverages the activities of these groups to maintain an awareness of and involvement in cybersecurity activities, the ACI is one of its major external coordination mechanisms. The ACI was established to address the full range of cybersecurity risks across the aviation ecosystem. Among its initiatives, the group has several efforts underway that address cybersecurity risks to avionics systems. In 2020, the DOT OIG reported that while the ACI has initiated work on these efforts, it has not developed mechanisms to monitor and evaluate results for meeting milestones and timeframes for its initiatives.[56]

FAA Coordinates on Internal Aviation Cybersecurity Efforts, but Has Not Established Mechanisms to Effectively Track Issues or Dedicated Resources to Avionics Cybersecurity Oversight

Coordinating cybersecurity risks within an organization entails adopting a risk management approach for identifying, assessing, and mitigating those risks. NIST guidance specifies a process for addressing cybersecurity at the organizational level by identifying and prioritizing risks, developing appropriate actions to respond to them, and monitoring the results.[57] Moreover, successful collaboration within the federal government entails adopting key practices, including:

- Documenting and clearly defining collaborative outcomes
- Including all relevant participants and clearly defining their roles and responsibilities,
- Establishing tracking mechanisms for monitoring progress, and
- Having the ability to commit resources.[58]

FAA's internal coordination mechanism addresses two of these four key collaborative practices.

FAA's Cybersecurity Steering Committee Was Established to Coordinate Cybersecurity Issues

Collaborative outcomes related to avionics cybersecurity have been documented and defined through FAA's Cybersecurity Steering Committee (CSC). According to FAA officials, the primary way that cybersecurity issues are coordinated across its component offices is through the CSC. FAA established this committee in November 2013 to coordinate agency-wide cybersecurity efforts and provide an integrated agency approach to cybersecurity. The CSC addresses topics related to the cybersecurity of FAA's enterprise systems as well as the cybersecurity of the aviation ecosystem. The committee's charter defines the committee's collaborative outcomes, such as identifying and agreeing

[56] Department of Transportation, Office of Inspector General, *FAA and Its Partner Agencies Have Begun Work on the Aviation Cyber Initiative and Are Implementing Priorities*, AV2020043 (Washington, D.C.: Sept. 2, 2020).

[57] NIST, *Managing Information Security Risk*, Special Publication 800-39 (Gaithersburg, MD: Mar. 2011).

[58] GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, GAO-12-1022 (Washington, D.C.: Sept. 27, 2012).

on an integrated approach to the agency's cybersecurity priorities and strategies.

Several FAA Components Have Cybersecurity Responsibilities That Are Coordinated by the Cybersecurity Steering Committee

The CSC includes all relevant participants and clearly defines their roles and responsibilities. The committee's charter describes the roles and responsibilities of leadership and committee membership, which includes several of the agency's components. FAA has four components that have responsibilities for reviewing the cyber safety aspects of airplanes as they are manufactured and approved for commercial service.

- **Aviation Safety (AVS)** is responsible for certifying the airworthiness of new airplanes and aviation equipment, including software components for avionics systems. The components of AVS are the Aircraft Certification Service (AIR) and Flight Standards Service (AFS).
  - **Aircraft Certification Service (AIR)** is responsible for the certification of airplanes, oversight of design, production, and airworthiness certification of aviation products. This includes avionics and continued airworthiness programs for all US civil aviation and foreign products.
  - **Flight Standards Service (AFS)** is responsible for the certification of airplane operators, as well as the inspection, surveillance, investigation, and enforcement actions against them.
- **Security and Hazardous Material Safety (ASH**) is responsible for various areas of cybersecurity, physical and technical security, interagency communications, and intelligence and investigations, among other responsibilities. Its relevant cybersecurity responsibilities currently include FAA's internal systems, working with DHS on aviation cybersecurity, and cyber concerns that could be introduced to the aviation ecosystem by new airplane equipment or designs.
- **Air Traffic Control (ATO)** is responsible for providing safe and efficient air navigation services to airspace over the United States and large portions of the Atlantic and Pacific Oceans and the Gulf of Mexico. This includes managing at least 50,000 average daily flights in and out of the U.S.
- **Information Security and Privacy Service (AIS)** includes the agency's Chief Information Security Officer, who chairs FAA's Cybersecurity Steering Committee. This office is responsible for the security of the FAA's networks and infrastructure and develops and ensures compliance with IT security and privacy policies. Office responsibilities include operation of the agency's Security Operations

Center, which provides 24/7 monitoring and technical support to detect cybersecurity threats and attacks against the agency's enterprise systems. As part of its responsibilities, AIS also works with the Flight Standards Service to process approvals and assist with IT-related oversight of air carriers' Aircraft Network Security Programs.

In 2015, we recommended that FAA incorporate AVS into its agency-wide cybersecurity efforts by including it in the CSC.[59] Subsequently, FAA made AVS a voting member of the Cybersecurity Steering Committee, in an attempt to ensure that relevant participants are included in the agency's collaborative efforts.

FAA's Cybersecurity Steering Committee Has Not Established a Documented Mechanism to Track Avionics Cybersecurity Efforts to Resolution

The CSC has not established a documented tracking mechanism for monitoring progress on cybersecurity issues that are raised in committee meetings. Specifically, committee meeting minutes show that when issues concerning avionics cybersecurity risks were raised, they were not subsequently tracked to ensure they were adequately resolved. For example, in August 2017 and August 2018, the CSC discussed an effort to test cybersecurity vulnerabilities in Full Authority Digital Engine Control systems.[60] While committee members raised concerns about the feasibility of the proposed tests, subsequent meeting minutes do not document any follow-up discussion to resolve the issue of how the tests should be conducted. According to FAA officials, the proposed tests were part of a DHS initiative that has since been terminated and no further briefings were provided to the CSC. However, this outcome was not documented in the meeting minutes or any other tracking mechanism.

In another example, DHS officials briefed FAA staff in 2017 on a DHS-led effort to work with an avionics manufacturer to conduct cybersecurity testing in a simulated environment. However, no further discussion of this effort was recorded in the CSC's minutes. According to FAA officials, FAA was not a participant in this effort and did not have any further information about it.

In that same year, CSC members discussed a DOD-initiated aviation cyber guidance study; however, according to FAA officials, the agency was not the sponsor of this study and only participated in a tabletop

[59]GAO, *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).

[60]Full Authority Digital Engine Control is a computer-managed airplane ignition and engine control system used in modern airplanes to digitally control engine performance.

exercise associated with the study. FAA officials did not provide any further information on the status of the study or its results. Later, in April 2018, meeting minutes indicated that FAA and its contractor discussed initiating a cybersecurity threat action plan for avionics systems. While FAA officials told us this initiative has been pursued by a working group led by ASH, its progress was undocumented.

FAA officials stated that they did not have a formal process for tracking the various issues and projects raised at committee meetings beyond recording them in meeting minutes or assigning them to working groups. They stated that the CSC established an Aviation Systems Cyber Vulnerability Working Group to address reported airplane system vulnerabilities, including avionics vulnerabilities. However, this group does not conduct research or any other activities to discover new vulnerabilities and does not track resolution of avionics cybersecurity issues that are raised at CSC meetings. Without adopting a tracking mechanism to monitor progress, FAA may be unable to ensure that all issues are appropriately addressed and resolved.

FAA Has Not Dedicated Spending to Avionics Cybersecurity When Allocating Resources

FAA's efforts to coordinate internally on avionics cybersecurity activities are not supported by dedicated resources within the agency's budget; further, FAA has not determined what resources are to be dedicated to the identification and mitigation of avionics cybersecurity risks. According to FAA officials, the agency is not functionally organized in a manner that lends itself either to a budget or easy person count for cybersecurity or any other area of functional expertise. While staff such as engineers, inspectors and IT specialists devote time to avionics cybersecurity, they can have several different technical areas in which they engage.

Further, the officials stated that FAA is not staffed according to budgeted technical areas of responsibility; thus, the agency has not been able to determine the full extent of the resources devoted to addressing cybersecurity risks associated with avionics systems. In the absence of a discrete number, FAA officials provided rough estimates that within its certification office, there are about 101 people that collectively spend approximately 24,000 man-hours per year working in various areas of aviation cybersecurity.

FAA received $3 million in funding in fiscal year 2017 to develop and implement an integrated cyber testbed at the FAA Technical Center in Atlantic City, New Jersey, to address cybersecurity requirements for air traffic control and to identify and address cybersecurity risks in avionics systems. However, FAA officials stated that the cyber testbed does not test avionics systems for cyber vulnerabilities. Instead, it focuses on the potential vulnerabilities of FAA's ground infrastructure and tests protections for that infrastructure. The officials also told us the agency has no planned or ongoing research and development activities related to addressing the cybersecurity risks to avionics systems.

As previously mentioned, FAA has not conducted a risk assessment of avionics cybersecurity risks within its oversight program to determine the relative priority of these risks versus other safety concerns. Without that assessment, the agency has not had a basis to prioritize or focus its coordination efforts, including committing resources for it. Until FAA conducts a risk assessment of avionics cybersecurity, it will not be able to effectively prioritize and dedicate resources to ensure avionics cybersecurity risks are addressed by its oversight program.

Conclusions

Increasing use of technology and connectivity in avionics has brought new opportunities for persons with malicious intentions to target commercial transport airplanes. The connections among avionics and other systems onboard airplanes and throughout the aviation ecosystem are growing more complex as airplanes become more connected to systems that are essential for flight safety and operations. Airframe manufacturers are deploying software and hardware protections to reduce the risk of the cyber threats currently facing avionics systems.

FAA has established cybersecurity requirements for airframe and manufacturers as part of the certification process and recognizes avionics cybersecurity as a potential airworthiness and safety issue for e-enabled airplanes. However, FAA has not conducted an overall assessment of the cybersecurity risks to avionics systems, and it has not developed policies and procedures for overseeing the implementation of avionics cybersecurity controls based on such an assessment. Without risk-based policies and procedures that address internal training needs, independent cybersecurity testing of avionics systems during the airplane certification process, and ongoing monitoring after an airplane is deployed, FAA may not be able to ensure sufficient oversight to guard against evolving avionics cybersecurity risks.

Further, while FAA has mechanisms for coordinating among its internal components and with other federal agencies and private sector stakeholders to address cybersecurity risks, it has not established avionics cybersecurity risks as a priority. As a result, avionics cybersecurity issues that have been raised within FAA have not been consistently tracked to resolution. Until FAA conducts an overall assessment of the cybersecurity risks to avionics systems and prioritizes coordination efforts based on that assessment, it may not be allocating resources and coordinating on risks as effectively as it could.

Recommendations for Executive Action

We are making a total of six recommendations to FAA. Specifically,

The FAA Administrator should direct the Associate Administrator for Aviation Safety to conduct a risk assessment of avionics systems cybersecurity to identify the relative priority of avionics cybersecurity risks for its oversight program compared to other safety concerns and develop a plan to address those risks. (Recommendation 1)

The FAA Administrator should direct the Associate Administrator for Aviation Safety, based on the assessment of avionics cybersecurity risks, to identify staffing and training needs for agency inspectors specific to avionics cybersecurity, and develop and implement appropriate training to address identified needs. (Recommendation 2)

The FAA Administrator should direct the Associate Administrator for Aviation Safety, based on the assessment of avionics cybersecurity risks, to develop and implement guidance for avionics cybersecurity testing of new airplane designs that includes independent testing. (Recommendation 3)

The FAA Administrator should direct the Associate Administrator for Aviation Safety, based on the assessment of avionics cybersecurity risks, to review and consider revising its policies and procedures for monitoring the effectiveness of avionics cybersecurity controls in the deployed fleet to include developing procedures for safely conducting independent testing. (Recommendation 4)

The FAA Administrator should direct the Associate Administrator for Aviation Safety to develop a mechanism to ensure that avionics cybersecurity issues are appropriately tracked and resolved when coordinating among internal stakeholders. (Recommendation 5)

The FAA Administrator should direct the Associate Administrator for Aviation Safety, based on the assessment of avionics cybersecurity risks, to review and consider the extent to which oversight resources should be committed to avionics cybersecurity. (Recommendation 6)

Agency Comments and Our Evaluation

We requested comments on a draft of this report from DOD, DHS, and DOT. In response, we received written comments from DOD and DOT (on behalf of FAA). Their comments are reprinted in appendices I and II, respectively.

In its comments, reproduced in appendix I, DOD concurred with the statements made in the report. In its comments, reproduced in appendix II, DOT concurred with five of our recommendations and did not concur with one. DOD, DHS, and DOT also provided technical comments, which we incorporated as appropriate.

DOT concurred with recommendations 1,2,3,5, and 6 and stated it would provide a detailed response to each recommendation after the report is publicly released. DOT did not concur with our recommendation to, based on the assessment of avionics cybersecurity risks, review and consider revising its policies and procedures for monitoring the effectiveness of avionics cybersecurity controls in the deployed fleet to include procedures for conducting independent testing. According to the agency, the FAA believes any type of testing conducted on the in-service fleet could result in potential corruption of airplane systems, jeopardizing safety rather than detecting cybersecurity safety issues. Further, the agency stated that the FAA has processes in place to address and correct cybersecurity safety issues should they occur.

We understand FAA's concern and recognize that testing, such as penetration testing, could negatively affect an airplane's network and systems configurations if improperly conducted. However, penetration testing standards call for measures to be taken ahead of testing, such as in an isolated "sandbox" environment, which would ensure that systems aren't negatively impacted either by the burden on the system of the test or the potential for data to be manipulated. Further, ongoing monitoring, including recurring testing of deployed systems, is important to ensuring cybersecurity. In addition, the development of FAA-approved policies and procedures for such testing is critical for air carriers to be able to ensure the continued effectiveness of cybersecurity controls in their deployed fleets. To address FAA's concern, we have clarified that our recommendation is for FAA to consider developing policies and procedures to safely conduct such testing as part of its ongoing monitoring of airplane safety.

We are sending copies of this report to the appropriate congressional committees and to the Department of Defense, the Department of Homeland Security, and the Department of Transportation. We are also sending copies of this report to the relevant private sector entities. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov, or Heather Krause at (202) 512-2834 or krauseh@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.

Sincerely yours,

Nick Marinos
Director, Information Technology and Cybersecurity

Heather Krause
Director, Physical Infrastructure

Appendix I: Comments from the Department of Defense

DEPARTMENT OF THE AIR FORCE
WASHINGTON DC

17 September 2020

MEMORANDUM FOR U.S. GOVERNMENT ACCOUNTABILITY OFFICE
ATTN: NICK MARINOS, DIRECTOR, INFORMATION TECHNOLOGY AND CYBERSECURITY
441 G Street NW
Washington DC 20548

FROM: HQ USAF A3
1790 Air Force Pentagon, Rm 4E1024
Washington DC 20330-1790

SUBJECT: Department of Defense Response to GAO Draft Report, GAO-21-86, "AVIATION CYBERSECURITY: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks," dated August 27, 2020 (GAO Code 103503)

1. This is the Department of Defense (DoD) response to the GAO Draft Report, "AVIATION CYBERSECURITY: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks," (GAO Code 103503). The DoD concurs with comment and welcomes the opportunity to reinforce the report's accurate description of aviation cybersecurity collaboration between the FAA and DoD.

2. Attached is the DoD's technical review comments to the subject report. The DoD point of contact is Mr. Alan Burke, AF/A2/6C / A3C, and can be reached at (703) 695-6018, DSN: 225-6018, or by email alan.burke.1@us.af.mil.

ROWAYNE A. SCHATZ, JR., SES, DAF
Associate Deputy Chief of Staff, Operations

Attachment: Comment Resolution Matrix

Appendix II: Comments from the Department of Transportation

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

Assistant Secretary for Administration

1200 New Jersey Avenue, SE
Washington, DC 20590

September 24, 2020

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

Nick Marinos
Director, Information Technology and Cybersecurity
GAO
441 G Street NW
Washington, DC 20548

Dear Ms. Krause and Mr. Marinos:

The Federal Aviation Administration (FAA) is committed to defending against new and evolving cybersecurity threats to safety critical aircraft systems. Since 2005, the FAA's Office of Aviation Safety has been applying airworthiness standards through special conditions under the authority of CFR 21.16 and 21.101(d) to address cybersecurity risk to aircraft avionics systems. On June 26, 2007, the FAA chartered RTCA Special Committee (SC)-216, "Aeronautical Systems Security," to develop industry standards for the initial design and continued airworthiness for aircraft systems and networks. These standards contain the safety, performance, interoperability, and security requirements used to assess and mitigate cybersecurity threats; they were created with industry participation, as well as involvement from FAA, European Union Aviation Safety Agency, and other international civil aviation authorities.

The FAA continues to pursue its mission to provide the safest, most efficient aerospace system in the world by:

- Ensuring cybersecurity safety risk assessments are performed which lead to the appropriate implementation of cybersecurity controls for avionics systems and equipment for all aircraft identified by FAA Policy Statement, Establishment of Special Conditions for Cybersecurity (PS-AIR-21.16-02);
- Prioritizing recurrent education and training in the aviation cybersecurity disciplines allowing employees to perform effectively in the service(s) they are assigned;
- Continuing to require independent testing through the invocation of special conditions for relevant aircraft during certification;
- Engaging with federal agencies, industry, and international partners through ongoing participation with working groups and standards organizations to strengthen and maintain aviation's fundamental level of safety; and
- Utilizing established safety management processes to track, address, and resolve all safety and potential safety issues (cyber or otherwise) that constitute an unacceptable risk to aviation safety.

Upon review of GAO's draft report, the FAA concurs with recommendations 1,2,3,5 and 6. The FAA non-concurs with recommendation 4, that the Associate Administrator for Aviation Safety, "based on the assessment of avionics cybersecurity risks . . . review and consider revising its policies and procedures for monitoring the effectiveness of avionics cybersecurity controls in the deployed fleet to include procedures for conducting independent testing." The FAA believes any type of testing conducted on the in-service fleet could result in potential corruption of airplane systems, jeopardizing safety rather than detecting cybersecurity safety issues. Should a cybersecurity safety issue occur, or be deemed likely to occur, on particular airplane models or any portion of the current fleet, the FAA has processes in place to address and correct the safety issue.

We will provide a detailed response to each recommendation within 180 days of the final report's issuance. 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.

Sincerely,

Keith Washington

Deputy Assistant Secretary for Administration

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Nick Marinos, (202) 512-9342, MarinosN@gao.gov

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

Staff Acknowledgments

In addition to the individuals named above, John de Ferrari and Ed Laughlin (assistant directors); Tina Torabi (analyst-in-charge); Amy Apostol, Chris Businsky, Alan Daigle, Nancy Glover, Rich Hung, William Hutchinson, Franklin Jackson, Elke Kolodinski, and Alec Yohn made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

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

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@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