GAO Highlights

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

October 2020

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.

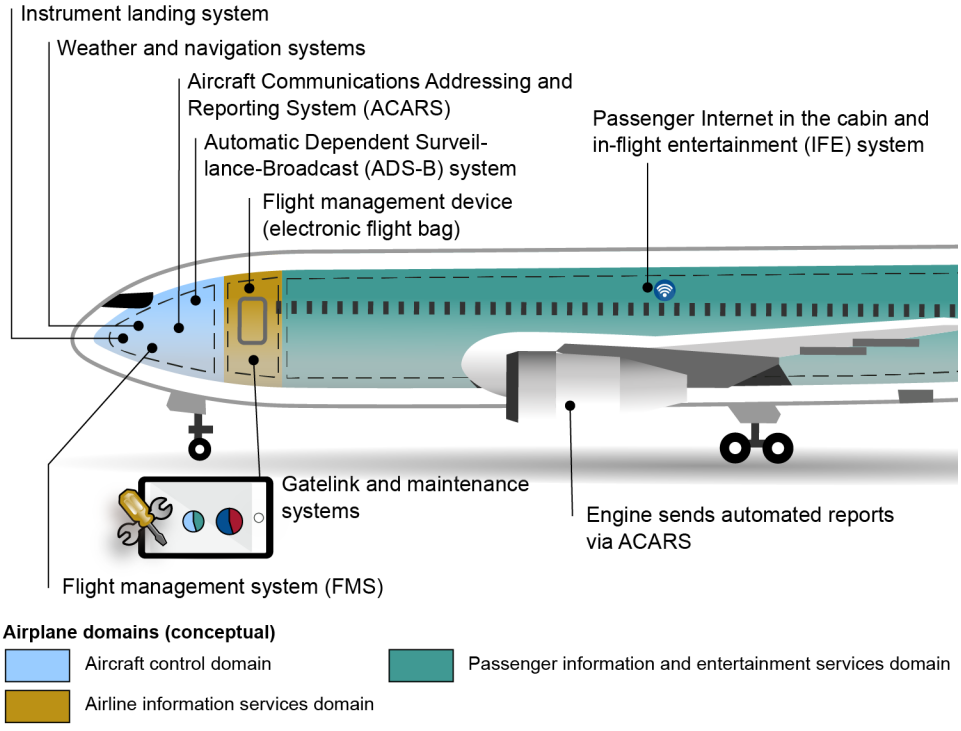
To do so, GAO reviewed information on key cybersecurity risks to avionics systems, as reported by major industry representatives as well as key elements of an effective oversight program, and compared FAA's process for overseeing the implementation of cybersecurity controls in avionics systems with these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

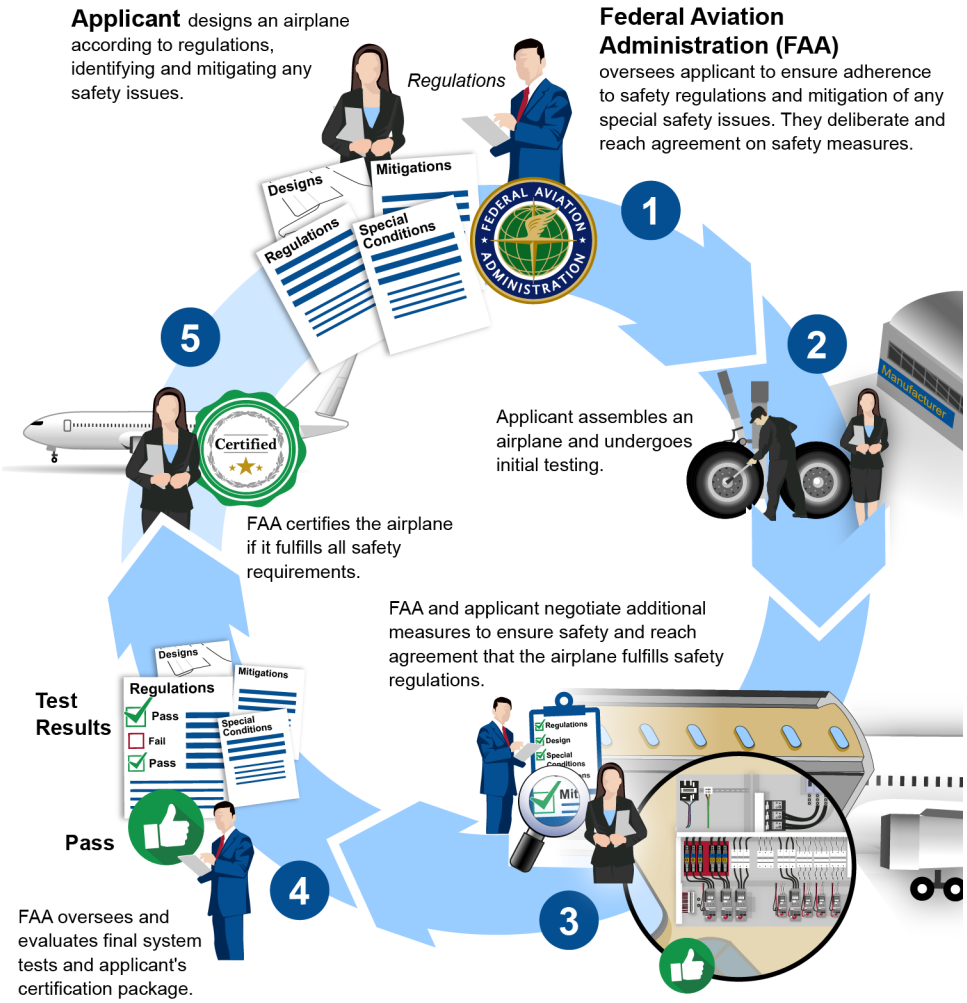
Based on the assessment of avionics cybersecurity risks, GAO recommends that FAA

- 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.