GAO Highlights

AVIATION CYBERSECURITY

FAA and TSA Are Collaborating on Cybersecurity but Need to Address Key Shortfalls

GAO-26-107693 July 2026

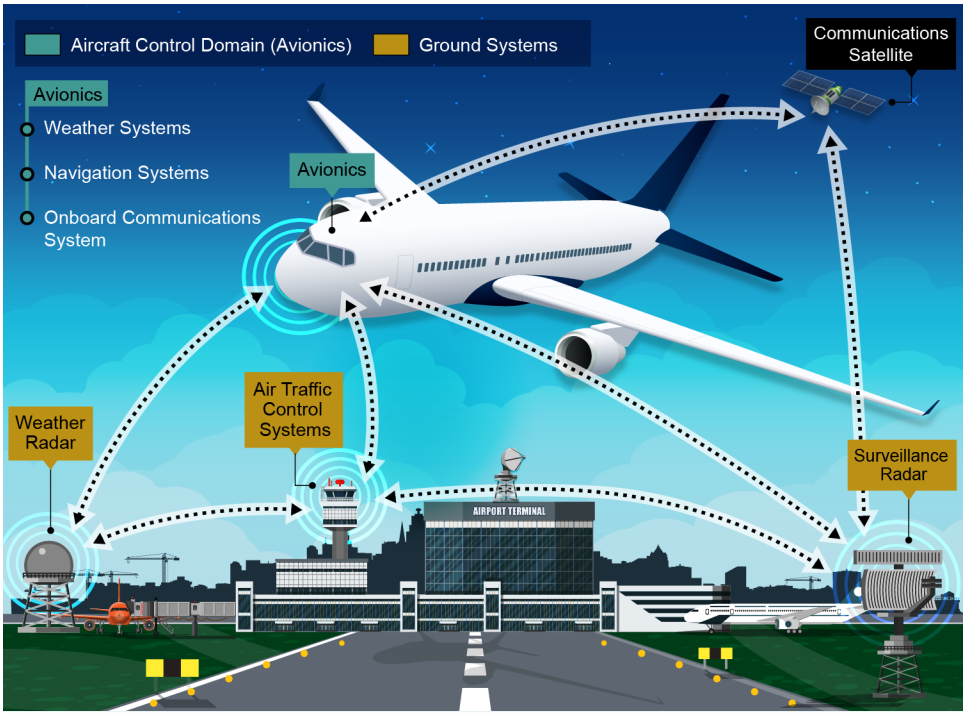
A report to congressional committees

For more information, contact: Jennifer R. Franks at FranksJ@gao.gov

What GAO Found

The Federal Aviation Administration (FAA) and Transportation Security Administration (TSA) work together to ensure the cybersecurity of the interconnected systems operating in the National Airspace System (NAS). FAA defined the roles and responsibilities of the entities responsible for carrying out the agency's related goals and objectives. In contrast, TSA did not. TSA defined its goals and objectives for prioritizing cybersecurity within the agency and in the transportation systems sector in its 2018 Cybersecurity Roadmap. However, the roadmap is outdated and no longer aligned with the latest Department of Homeland Security Cybersecurity Strategy. The roadmap also does not identify the offices responsible for implementing it or define the agency's cybersecurity-related roles and responsibilities in overseeing airport and aircraft operator security programs. Until TSA updates its Cybersecurity Roadmap to clearly identify its aviation cybersecurity roles and responsibilities, the agency cannot fully hold relevant entities accountable or enable continuous improvements to its related efforts. Moreover, clarity in TSA's cybersecurity roles, and in turn those of stakeholders, could help minimize the risk of covered systems being exploited.

Interconnection of Aircraft Avionics and Air Traffic Control Facilities on the Ground



Sources: GAO analysis of Federal Aviation Administration and industry documentation; absent84/stock.adobe.com (illustrations); Golden Sikorkan/stock.adobe.com (airplane). | GAO-26-107693

Seven FAA entities are responsible for implementing the agency's Cybersecurity Strategy. The President's budget requests from fiscal years 2024 through 2026 included funding requests for these entities ranging from approximately $42 million to $11 billion. In addition, the budget requests described programs and

Why GAO Did This Study

Commercial flight operations rely on interconnected systems that reside onboard an aircraft and on the ground in the National Airspace System. Given this interconnectivity, these systems are inherently more vulnerable to exploitation and are at an increased risk of being targeted by malicious actors. FAA and TSA are the primary federal agencies leading security and resilience efforts in the aviation subsector.

The FAA Reauthorization Act of 2024 includes a provision for GAO to evaluate FAA and TSA efforts to manage their roles and responsibilities for aviation cybersecurity. This report examines (1) the extent to which FAA and TSA defined their current roles and responsibilities for aviation cybersecurity; (2) the budget requests for the FAA entities responsible for implementing its Cybersecurity Strategy, and the extent to which they meet relevant OMB reporting requirements; (3) the extent to which the FAA's Cybersecurity Strategy incorporates key federal and industry practices to address cybersecurity risks and vulnerabilities for avionics and ground systems; and (4) the extent to which FAA implemented its Cybersecurity Strategy to mitigate cybersecurity risks to its systems and networks.

To address these objectives, GAO compared FAA and TSA strategies and supporting documentation to determine how the agencies defined separate roles and responsibilities for aviation cybersecurity and compared them against the NIST Cybersecurity Framework 2.0 guidance on roles, responsibilities, and authorities. GAO also reviewed the fiscal year 2024 through 2026 President's budget requests for FAA and evaluated the agency's budget data and associated process to determine if the agency comprehensively reported its

costs associated with FAA's implementation of its Cybersecurity Strategy. However, FAA did not report all of its cybersecurity activities and costs to the Office of Management and Budget's (OMB) in each of the fiscal years from 2024 through 2026. Specifically, based on FAA's submitted budget data, the agency did not include spending data for its Information Security/Cybersecurity Program that supports its research and development activities. Until FAA reports all its cybersecurity activities and costs to OMB, policy officials and Congress may not have a complete understanding of FAA's cybersecurity activity spending that could also impact decisions regarding future cybersecurity funding needs.

FAA's current and proposed aircraft certification and system security authorization processes align with all key federal and industry practices that GAO identified for mitigating cybersecurity risks and vulnerabilities to avionics and ground systems in the NAS. However, FAA's Zero Trust Implementation Plan that describes the agency's approach for transitioning its operating environments to a zero trust architecture (ZTA), including during its NAS modernization effort, did not include details on transition steps for its Research and Development operating environment. Additionally, the plan fully aligned with three of the seven practices that the National Institute of Standards and Technology (NIST) outlined for migrating to a ZTA. Without fully aligning its zero trust implementation plan with NIST's best practices across all operating environments, FAA cannot ensure that it is effectively and comprehensively managing cybersecurity risks during NAS modernization.

FAA had not fully implemented the objectives supporting its Cybersecurity Strategy's goal to protect and defend its networks and systems. Specifically, FAA fully implemented three of the seven objectives supporting the goal, as shown in the table below. GAO found that FAA had not fully implemented its Cybersecurity Strategy, in part, because the agency lacked a comprehensive process to monitor and evaluate the implementation of its goals. While the strategy established monitoring requirements for FAA entities, GAO found that one of the seven applicable FAA entities had demonstrated doing so. In March 2026, FAA updated the strategy, which now describes the agency's plans to develop and use a centralized implementation plan to achieve its strategic objectives and develop performance metrics to track progress towards each of those objectives. As FAA implements its new strategy, taking steps to ensure it carries out the monitoring as planned, including incorporating lessons learned from its past experiences, would help position the agency to achieve its goals for protecting its networks and systems and to effectively mitigate cybersecurity risks. In addition, the agency will be better able to identify challenges, make adjustments, and prioritize resources to address identified risks to its missions and service delivery.

Assessment of Federal Aviation Administration's (FAA) Efforts to Implement Its Cybersecurity Strategy Goal to Protect and Defend its Networks and Systems

Goal and associated objectives	GAO assessment
Improve cyber threat intelligence collection, processing, dissemination, and reporting	●
Improve FAA cyber monitoring, detection, and response capabilities	◐
Improve privileged user control, monitoring, and visibility	◐
Improve capabilities for detection and mitigation of threats, internal and external	●
Leverage cybersecurity research and development across FAA domains and systems	●
Ensure FAA information security controls, policies and processes are aligned with current National Institute of Standards and Technology standards and guidelines	◐
Develop and implement Zero Trust Architecture capabilities	◐

Legend: ○ = not implemented; ◐ = partially implemented; ● = fully implemented

Source: GAO analysis of the FAA Cybersecurity Strategy. | GAO-26-107693

cybersecurity spending in accordance with OMB's reporting requirements.

Additionally, GAO compared the FAA Cybersecurity Strategy as of February 2026 and associated processes for aircraft certification, system security authorization, and zero trust implementation against key practices GAO identified for mitigating risks and vulnerabilities for avionics and ground systems. Further, GAO evaluated documentation demonstrating FAA's implementation of its Cybersecurity Strategy's goal and associated objectives to protect and defend its networks and systems against risks. Lastly, GAO interviewed or collected written responses from FAA, TSA, and selected aviation stakeholders representing industry groups, avionics manufacturers, domestic airlines, and a research organization. GAO selected these aviation stakeholders based on a review of prior work, a literature search, and recommendations obtained from stakeholders interviewed during prior related work.

What GAO Recommends

GAO is making a total of five recommendations, including one for TSA to (1) update its Cybersecurity Roadmap to define the agency's roles and responsibilities for the entities responsible for carrying out the goals and objectives described within it, among other things.

GAO is also recommending that FAA (1) update its cyber budget data request process to ensure that it includes all cybersecurity spending from program offices; (2) update its zero trust implementation plan to include detailed steps for transitioning all operating environments to a zero trust architecture; (3) update its zero trust implementation plan to align with NIST zero trust best practices; and (4) take steps, as it implements its revised Cybersecurity Strategy, to ensure that its Cybersecurity Steering Committee carries out monitoring as planned and incorporates lessons learned from its past experiences.

Both the Departments of Homeland Security and Transportation agreed with GAO's recommendations to TSA and FAA, respectively.