United States Government Accountability Office

Report to Congressional Committees

July 2026

AVIATION CYBERSECURITY

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

GAO-26-107693

GAO Highlights

AVIATION CYBERSECURITY

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

GAO-26-107693 July 2026

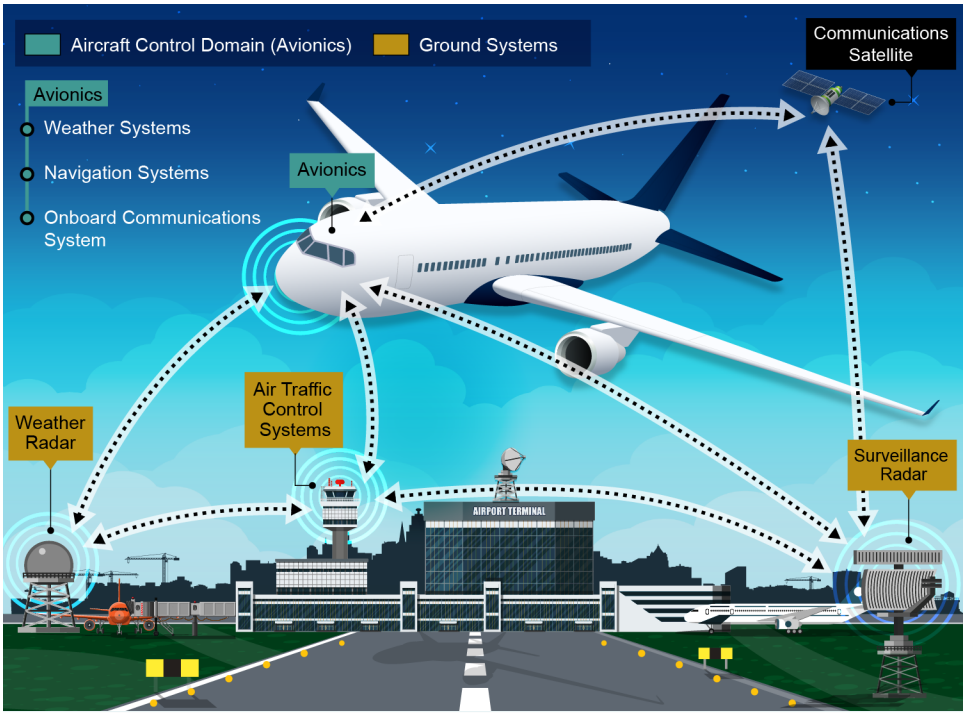
A report to congressional committees

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 However, the roadmap is outdated and no longer aligned with the latest Department of Homeland Security Cybersecurity Strategy.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.

Contents

Tables

Figures

Abbreviations

ACI	Aviation Cyber Initiative
AFN	Office of Financial Management
AIS	Information Security and Privacy Service
ANG	NextGen Office
ARP	Office of Airports
ASH	Office of Security and Hazardous Materials Safety
AST	Office of Commercial Space Transportation
ATO	Air Traffic Organization
AVS	Office of Aviation Safety
CISA	Cybersecurity and Infrastructure Security Agency
CyTF	Cybersecurity Test Facility
CSDS	Cybersecurity Data Science
DHS	Department of Homeland Security
DOD	Department of Defense
DOT	Department of Transportation
ExCom	ACI Executive Committee
FAA	Federal Aviation Administration
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
ISCM	information security continuous monitoring
NAS	national airspace system
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OT	operational technology
RTCA	Radio Technical Commission for Aeronautics
SECTR	Secure Enterprise Cyber Test Range
TSA	Transportation Security Administration

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

July 16, 2026

Congressional Committees

Each day, the Federal Aviation Administration (FAA) provides air traffic service to more than 44,000 flights and 3 million airline passengers traveling across the more than 29 million square miles that make up the U.S. national airspace system (NAS).[1] FAA also employs over 14,000 air traffic controllers and maintains over 100 ground navigation facilities to ensure passengers get to their destinations safely.

Relatedly, the Transportation Security Administration (TSA) provides security for more than 440 airports. The agency also employs over 1,300 aviation transportation security inspectors who ensure compliance with federal regulations, including in the aviation subsector.[2] In fiscal year 2024, these security inspectors found that 91.8 percent of airlines operating from domestic airports were in compliance with required security standards.

Cyber-based threats to federal information systems, such as those that FAA relies on for its air traffic control services, are evolving and growing. Avionics, the electronic systems used to control, monitor, and operate an aircraft, are similarly at risk. Additionally, although there have been no reports of successful cyberattacks on avionics, the increasing interconnectivity of these systems with other aircraft systems and external systems, presents increasing opportunities for such attacks. With the growing sophistication of advanced persistent threats and continuing advancements in technology, systems supporting flight operations remain at risk.

The FAA Reauthorization Act of 2024 includes a provision for GAO to review FAA and TSA's efforts to manage and differentiate their roles and

[1]The NAS is a shared network of U.S. airspace; air navigation facilities, equipment, and services; airports or landing areas; aeronautical charts, information, and services; rules, regulations, and procedures; technical information; and manpower and material.

[2]The nation's transportation system consists of seven subsectors: (1) aviation, (2) highway and motor carrier, (3) maritime transportation system, (4) mass transit and passenger rail, (5) freight rail, (6) pipeline systems, and (7) postal and shipping. The aviation subsector refers to a distinct segment of the broader aerospace and aviation industry, categorized by its specific function, such as commercial, military, or general aviation. This subsector includes manufacturing, air transport, airport operations, and maintenance.

responsibilities for avionics and ground systems cybersecurity. The act also includes a provision for GAO to review FAA's framework for mitigating risks to civil aviation, the agency's information systems, and the NAS (the FAA Cybersecurity Strategy), as well as the budgets of the entities responsible for implementing the framework.

Our objectives were to determine (1) the extent to which FAA and TSA defined their current roles and responsibilities for aviation cybersecurity, and collaborated to manage them; (2) the budget requests for the FAA entities responsible for implementing its Cybersecurity Strategy and to what extent are they meeting relevant Office of Management and Budget (OMB) reporting requirements; (3) the extent to which the FAA 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 has implemented its Cybersecurity Strategy to mitigate cybersecurity risks to its systems and networks.

To address our first objective, we compared FAA and TSA's relevant strategies, policies, and websites to identify any duplication, overlap, or fragmentation in the agencies' roles and responsibilities for aviation cybersecurity.[3] This included identifying and comparing the offices within FAA and TSA that have responsibilities in aviation cybersecurity. Further, we compared the agencies' strategies against the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 guidance on roles, responsibilities, and authorities.[4] We also interviewed or collected written responses from selected aviation stakeholders, such as industry groups, avionics manufacturers, and airlines, to obtain their perspectives on FAA and TSA roles and responsibilities for aviation cybersecurity. We identified our non-generalizable sample of stakeholders based on our review of prior GAO work, a literature search, and recommendations from stakeholders that were obtained from our prior work related to aviation surveillance technologies. Appendix I has additional details about our selected stakeholders. Additionally, we assessed the group that FAA and TSA used to collaborate on aviation cybersecurity—the Aviation Cybersecurity Initiative (ACI)—against

[3]GAO, *Fragmentation, Overlap, and Duplication: An Evaluation and Management Guide*, GAO-15-49SP, (Washington, D.C.: Apr. 2015).

[4]National Institute of Standards and Technology, *The NIST Cybersecurity Framework, Version 2.0 (Gaithersburg, MD: February 2024).*

leading practices that we identified for interagency collaboration.[5] We also interviewed or collected written responses from the aviation stakeholders mentioned above to obtain their perspectives on FAA and TSA's collaborative efforts for aviation cybersecurity.

To address the second objective, we reviewed and described the fiscal year (FY) 2024 through 2026 President's budget requests for relevant FAA entities to describe their requested budgets for that time period. We also summarized the costs associated with cybersecurity activities outlined in the FAA Cybersecurity Strategy. Further, we assessed FAA's Cyber Budget Data Request Process to determine the extent to which it facilitated comprehensive reporting of its cybersecurity activities and costs to OMB.

To address the third objective, we reviewed standards and guidance issued by the NIST and aviation industry standards bodies, such as Radio Technical Commission for Aeronautics (RTCA) and American Society for Testing and Materials. From these, we identified key practices for mitigating cybersecurity risks and vulnerabilities to avionics and ground systems.[6] Then, we compared FAA's Cybersecurity Strategy, as of February 2026, and associated documentation against the key practices we identified to determine how they were addressed. In March 2026, FAA finalized an update to its Cybersecurity Strategy that outlines strategic objectives and associated key initiatives. According to the updated strategy, FAA will develop a centralized implementation plan to guide the agency's achievement of the strategic objectives outlined within it. Our review primarily focused on the strategy as of February 2026 given the timing of our review and FAA's update.

To address the fourth objective, we analyzed the FAA Cybersecurity Strategy as of February 2026 to identify and describe the agency's goal and supporting objectives to mitigate cybersecurity risks to its systems and networks. We then assessed agency policies, procedures, and plans to determine the extent to which FAA had fully implemented its goal. As part of this assessment, we analyzed the security authorization documentation for eight selected systems to determine whether the FAA

[5]GAO, *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges*, GAO-23-105520 (Washington, D.C.: Mar. 2023).

[6]For purposes of our review, we considered ground systems as those that are external to an aircraft but provide information and data necessary for its safe flight. These systems are operated and managed by FAA.

was consistently implementing its Security Authorization Handbook, which is intended to align the agency with NIST standards and guidance.

To select the eight systems, we used FAA's inventory of mission critical systems that were categorized as high- and moderate-impact.[7] For these systems operating in the mission support and national airspace system domains, we randomly selected one high-impact and one moderate-impact system from each domain using a computerized random function. Since the research and development domain did not have any mission critical systems, we judgmentally selected the one system categorized as high-impact and randomly selected a moderate-impact system using a computerized random function. Further, we used FAA's inventory of unsustainable systems to select one mission essential system with sustainability rating A and one with sustainability rating B.[8] We also randomly selected these systems using a computerized random function.

We supplemented our analysis for each objective with interviews of relevant FAA officials in the offices of Financial Management, NextGen, and Aviation Safety. We also interviewed TSA officials in the offices of Security Operations, Policy Plans, and Engagement, and Strategy, Policy, Coordination, and Innovation. These interviews assisted in corroborating evidence and providing additional context to the actions taken by FAA and TSA to carry out its roles, responsibilities, strategies, policies, procedures, and plans regarding aviation cybersecurity. Additional details on our objectives, scope, and methodology are provided in Appendix I.

We conducted this performance audit from August 2024 to July 2026 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

[7]Mission critical systems are vital to the operation of air travel, such as automation, communications, navigation, surveillance, and weather. Systems with a high-impact security categorization would have a severe or catastrophic adverse impact if compromised. Systems with a moderate-impact security categorization would have a serious adverse impact if compromised.

[8]Mission essential systems are vital to the operation of services indirectly supporting the safety and efficiency of air traffic operations, such as grant applications, airman and aircraft certification and regulatory services, and airport services. Sustainability rating of A means that the system has significant shortages in spare systems, shortfalls in sustainment funding, and little or no technology funding. Sustainability rating B means that the system has significant shortfalls in sustainment funding or capability.

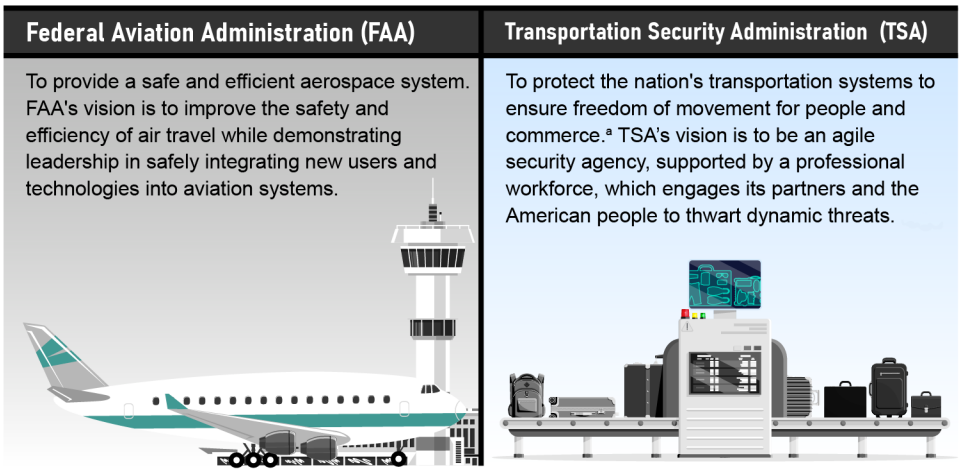
the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The Departments of Transportation (DOT) and Homeland Security (DHS) are designated as the co-sector risk management agencies for the transportation systems critical infrastructure sector.[9] Within these departments, FAA and TSA are the primary federal agencies leading security and resilience efforts in the aviation subsector. Given this, FAA and TSA's mission and vision statements focus on safety and security, respectively. Figure 1 illustrates the missions and vision statements for FAA and TSA.

[9]Sector risk management agencies are responsible for providing institutional knowledge and specialized expertise in leading their designated critical infrastructure sector's security and resilience activities. Presidential Policy Directive 21 on *Critical Infrastructure Security and Resilience* identified 16 critical infrastructure sectors, designated federal agencies to serve as the sector risk management agency for each sector, and outlined responsibilities for those agencies to serve in that role. The *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021* updated the responsibilities for sector risk management agencies. Pub. L. No. 116-283, § 9002, 134 Stat. 3388, 4768-4769 (Jan. 1, 2021). In April 2024 the White House National Security Council published National Security Memorandum-22 on Critical Infrastructure Security and Resilience, which replaced Presidential Policy Directive 21 and revised the framework for federal agency roles and responsibilities within national critical infrastructure risk management. The White House, *National Security Memorandum on Critical Infrastructure Security and Resilience*, National Security Memorandum-22 (Washington, D.C.: Apr. 30, 2024).

Figure 1: Mission and Vision Statements for the Federal Aviation Administration (FAA) and Transportation Security Administration (TSA)



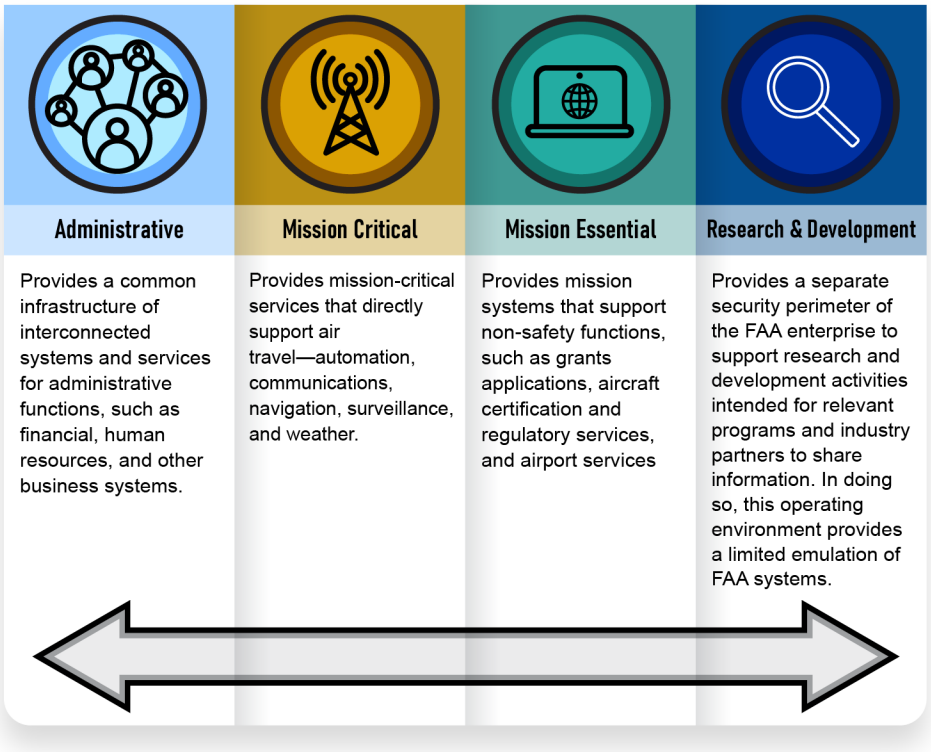
Sources: GAO analysis of FAA and TSA websites; serz72/stock.adobe.com (control tower and airplane); absent84/stock.adobe.com (baggage claim). | GAO-26-107693

[a]The nation's transportation system consists of seven subsectors: (1) aviation, (2) highway and motor carrier, (3) maritime transportation system, (4) mass transit and passenger rail, (5) freight rail, (6) pipeline systems, and (7) postal and shipping.

FAA operates information and operational technology in four operating environments to support its mission.[10] Each operating environment works together in supporting FAA's cybersecurity efforts. Figure 2 describes each operating environment.

[10]Operational technology is a broad range of programmable systems and devices that interact with the physical environment or manage devices that interact with the physical environment. Examples include industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems. National Institute of Standards and Technology (NIST), *Guide to Operational Technology Security*, NIST Special Publication 800-82, Revision 3. (Gaithersburg, Md.: Sept. 2023).

Figure 2: Description of the Federal Aviation Administration's (FAA) Operating Environments



Sources: GAO analysis of FAA's Cybersecurity Strategy; stas111/stock.adobe.com (icons). | GAO-26-107693

Note: The systems operating in the mission critical and mission essential operating environments support operations in the national airspace system.

The FAA Chief Information Security Officer and Chief Information Officer are responsible for the overall cybersecurity posture of the agency. Nonetheless, each operating environment represents a distinct security perimeter that is managed by a specific FAA entity. Specifically:

- Information Security and Privacy Service (AIS) is responsible for compliance, operations, and security services within the administrative operating environment.
- Air Traffic Organization (ATO) manages operational cybersecurity in the Mission Critical and Mission Essential operating environments, and provides identification, protection, detection, response, and

recovery capabilities in these environments to support safe air navigation services.[11]

- NextGen Office (ANG) had the primary responsibility for cybersecurity in the Research and Development operating environment.[12]

TSA has multiple pillars comprised of several offices that directly support the agency in carrying out its mission in the aviation subsector.[13] Specifically:

- Operations Support pillar develops processes and technologies to assess and mitigate the threats related to transportation security.
  - Intelligence and Analysis Office leads intelligence sharing to security stakeholders to protect travelers.
  - Policy, Plans, and Engagement Office develops and coordinates transportation security programs, directives, strategies, and initiatives.
  - Requirements and Capabilities Analysis Office analyzes the domestic and international risk landscape and assesses capability gaps to develop requirements and inform policy decisions.
  - Enrollment Services and Vetting Programs Office leads TSA's enrollment, vetting, credentialing, and prescreening programs and services.
- Security Operations pillar is intended to ensure the security of the nation's transportation systems, to include the safe movement of people and commerce by air.

[11]FAA systems in the Mission Critical and Mission Essential operating environments support NAS operations.

[12]Section 206 of the FAA Reauthorization Act of 2024 required FAA to terminate the NextGen Office on December 31, 2025, and transfer residual functions for the NextGen program to the Airspace Modernization Office. Section 207 of the act gives the Airspace Modernization Office responsibility for research and development, system engineering, enterprise architecture, and portfolio management for the continuous modernization of the national airspace system. On January 26, 2026, FAA announced the reorganization of the agency's structure. With the reorganization, the NextGen Office is to be replaced, and its functions divided across several internal entities, to include the new Airspace Modernization Office.

[13]In May 2026, TSA officials informed us that the agency is undergoing an organizational realignment and is, therefore, updating its internal documentation and organizational chart to reflect changes in the directorates and associated functions.

- Compliance Office oversees Transportation Security Inspectors that ensure stakeholders in each mode of transportation adhere to statutory, regulatory, and program security requirements.
- Domestic Aviation Operations Office manages TSA's domestic airport operations and oversees airport checkpoint, baggage, and air cargo screenings.

In addition to the pillars and offices above, the Strategy, Policy Coordination, and Innovation Office that sits under the Chief of Staff also supports the agency in carrying out its mission in the aviation subsector. Specifically, this office serves as the central point for the agency's strategic planning, policy coordination, and enterprise innovation, to include leading performance and risk management activities.

Interconnectivity Risk Among Avionics and Ground Systems

Avionics are generally considered one of the most critical components of an aircraft due to their criticality for safe flight operations. These systems provide weather information, positioning data, and communication mechanisms to ensure the safe operation of aircraft. For example, certain airplanes are equipped with a system known as the Automatic Dependent Surveillance-Broadcast that periodically broadcasts data such as flight identification number, current position, altitude, and velocity, which can be received by FAA air traffic control systems for tracking purposes and by other aircraft equipped with ADS-B In to assist with collision avoidance.

Ground systems in the NAS support air traffic control services by managing communications; monitoring weather, navigation, and surveillance; and directing aircraft from takeoff to landing to ensure safe travel within the U.S. airspace. For example, the Ground Based Augmentation System provides corrections to aircraft in the vicinity of an airport to improve the accuracy of aircraft navigational positions. It does this by augmenting the existing global positioning system used in U.S. airspace.

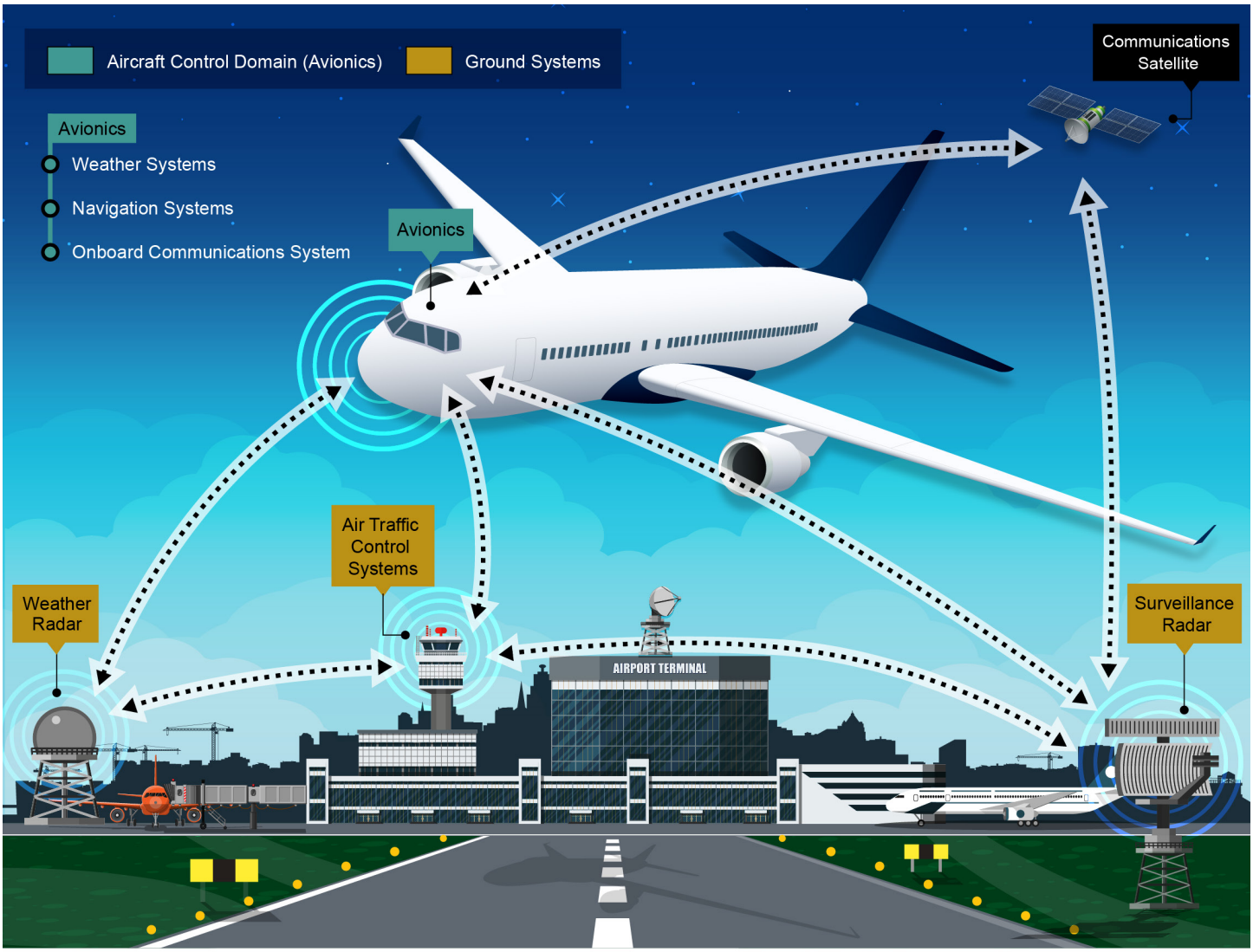
We previously reported that avionics systems are increasingly interconnected with external systems, such as ground systems.[14] For instance, the Aircraft Communications Addressing and Reporting System communicates flight plans and various weather conditions from air traffic

[14]GAO, Aviation Cybersecurity: *FAA Should Fully Implement Key Practices to Strengthen its Oversight of Avionics* Risks, GAO-21-86, (Washington, D.C.: Oct. 9, 2020).

controllers on the ground to avionics onboard aircraft.[15] The interconnection of avionics and ground systems presents increased vulnerabilities that can be exposed to carry out a variety of potential cyberattacks. Figure 3 shows how avionics onboard an aircraft are interconnected with air traffic control facilities on the ground.

[15]The Aircraft Communications Addressing and Reporting System is a communications network used 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.

Figure 3: Interconnected Avionics and Ground Systems That Support the National Airspace System



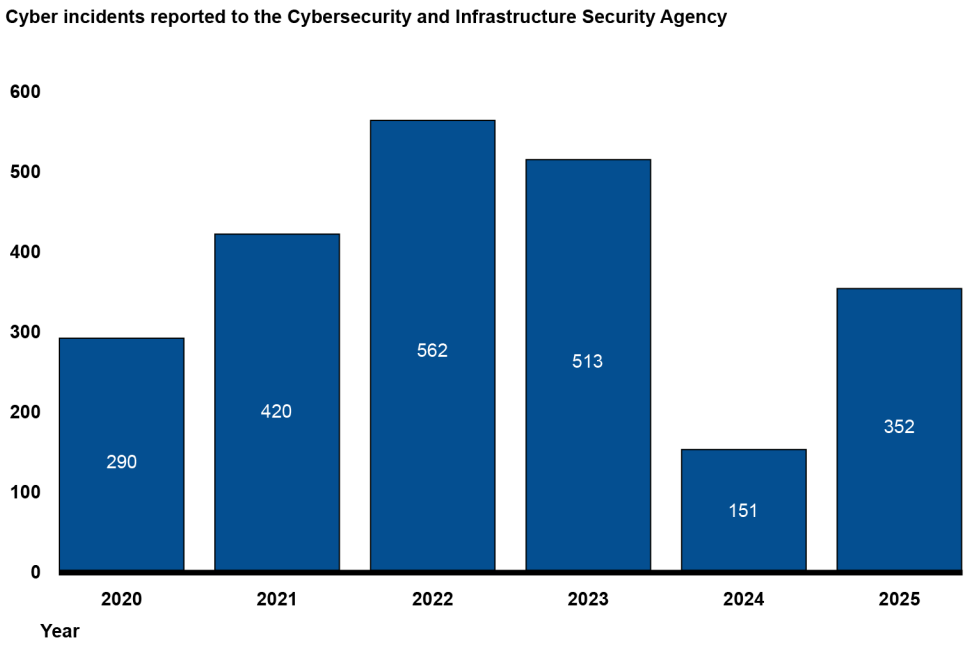
Sources: GAO analysis of Federal Aviation Administration and industry documentation; absent84/stock.adobe.com (illustrations); Golden Sikorkan/stock.adobe.com (airplane). | GAO-26-107693

Cybersecurity Incidents Reported in the Aviation Subsector

The Cybersecurity and Infrastructure Security Agency (CISA) provides quarterly reporting of exploited vulnerabilities within the transportation system critical infrastructure sector, including in the aviation subsector. More specifically, the agency reported cybersecurity incidents by state-sponsored actors, financially motivated groups, and hacktivists during the last three years that have impacted the aviation subsector. For example, according to the quarterly vulnerability reports that CISA issued in 2024, a

state-sponsored cyber actor from the People's Republic of China targeted the aviation subsector in its malicious cybersecurity activities. Figure 4 illustrates the number of cybersecurity incidents reported in the aviation subsector, from 2020 through 2025.

Figure 4: Number of Cybersecurity Incidents Reported in the Aviation Subsector (2020 – 2025)



Source: GAO analysis of cyber incidents reported to the Cybersecurity and Infrastructure Security Agency. | GAO-26-107693

Reports of cybersecurity incidents in the aviation subsector have highlighted the vulnerabilities exploited in avionics and ground systems to carry out attacks. Those vulnerabilities include the following:

- Improper software patching practices
- Unsecure internet accessible operational technology (OT) and IT
- Use of unsupported operating systems, outdated software, vulnerable services, and vulnerable remote services
- Default OT settings, ports, and credentials
- Lack of user training
- Insecure supply chains

- Poor network security implementation
- Lack of network segmentation of OT and IT

Additionally, based on the incidents reported in the aviation subsector, the successful exploitation of the vulnerabilities described above increases cybersecurity risks in avionics and ground systems. Such incidents could potentially lead to the following:

- Loss of flight data causing communication impacts to air traffic control services
- Unauthorized access to avionics and ground systems
- Alteration of critical data used by cockpit systems
- Manipulation of avionics and ground systems, leading to public safety concerns
- Jammed radio frequency signals
- Spoofing or interference in aircraft GPS location data
- Impersonation of ground stations to lower avionic systems' sensitivity settings

Federal Laws, Standards, and Guidance Set Forth to Secure Avionics and Ground Systems

Federal laws contain specific requirements for FAA to enhance the cybersecurity of avionics and ground systems. In addition, standards and guidance published by NIST provide best practices on cybersecurity risk management for organizations and their systems.

Avionics and Ground Systems Cybersecurity

Federal Information Security Modernization Act of 2014 (FISMA). Among other things, FISMA requires agencies to develop, document, and implement an agency-wide program to secure federal information systems and data.[16] These information security programs are to provide risk-based protections for the information and information systems that support the operations and assets of the agency. FISMA requires agencies to comply with OMB's policies and procedures, DHS's binding

[16]The Federal Information Security Modernization Act of 2014 (FISMA 2014), Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014) largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers to the new requirements in FISMA 2014, and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

operational directives, and NIST's federal information standards and guidelines.[17]

FAA Extension, Safety, and Security Act of 2016. This act directed FAA to reduce cybersecurity risks to the NAS and civil aviation by developing a comprehensive and strategic framework that considered the cybersecurity risk of interconnected aircraft and NAS systems.[18] In carrying out the development of the framework, FAA was to coordinate with aviation stakeholders; consult with relevant federal agencies; convene an expert panel, if necessary; and evaluate the effectiveness of the principles supporting the framework, on a periodic basis. Additionally, the act required FAA to identify and address cybersecurity risks by reviewing existing and new recommendations for rulemaking, policy, and guidance to promote safety and aircraft systems information security protection. Further, the act called for FAA to clarify the cybersecurity roles and responsibilities of its offices and employees.

FAA Reauthorization Act of 2018. This act directed FAA to revise regulations to require aircraft avionics systems used for flight guidance or aircraft control to be secured from unauthorized external and internal access. The act also directs FAA to initiate a review of its comprehensive and strategic framework of principles and policies that was developed pursuant to Section 2111 of the FAA Extension, Safety, and Security Act of 2016.[19]

FAA Reauthorization Act of 2024. Among other things, this act requires FAA to establish a cyber threat management process to protect the NAS. Additionally, the act requires FAA to revise regulations regarding airworthiness certification to establish a process and timeline for software-based systems and equipment to be regularly screened to detect compromise. Further, the act directs FAA to convene an aviation rulemaking committee on civil aircraft cybersecurity. The purpose of the committee is to conduct reviews and develop findings and recommendations on cybersecurity standards for civil aircraft, aircraft

[17]Binding operational directives are compulsory and require agencies to take specific actions to safeguard federal information and information systems from a known threat, vulnerability, or risk.

[18]FAA Extension, Safety, and Security Act of 2016, Pub. L. No. 114–190, § 2111, 130 Stat. 615, 625-627 (2016).

[19]The strategic framework required by Section 2111 of the FAA Extension, Safety, and Security Act of 2016 is referenced in the FAA Cybersecurity Strategy.

ground support information systems, airports, air traffic control mission systems, and aeronautical products and articles.

Cybersecurity Risk Management

The NIST Cybersecurity Framework 2.0. This framework is designed to help organizations manage and reduce their cybersecurity risks.[20] It outlines high-level cybersecurity outcomes to enable organizations to understand, assess, prioritize, and communicate their cybersecurity efforts effectively across six core functions.

1. **Govern.** Establish, communicate, and monitor the organization's risk management strategy, expectations, and policy to guide cybersecurity decisions.
2. **Identify.** Understand the current cybersecurity risks to the organization's assets.
3. **Protect.** Apply safeguards to manage and support the organization's cybersecurity risks.
4. **Detect.** Find and analyze potential cybersecurity attacks and compromises.
5. **Respond.** Take coordinated actions to contain and manage a detected cybersecurity incident.
6. **Recover.** Restore operations affected by a cybersecurity incident in a timely manner.

NIST Risk Management Framework. This risk management framework provides a process to manage cybersecurity risk for organizations and their information systems.[21] In doing so, the framework outlines seven steps for the successful execution of the risk management framework.

[20]National Institute of Standards and Technology, The *NIST Cybersecurity Framework* 2.0.

[21]National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations, Special Publication 800-37, Revision 2.* (Gaithersburg, MD: December 2018).

1. **Prepare** for using the risk management framework by carrying out essential activities at the organization, mission and business process, and information system levels.

2. **Categorize** systems and the information they process, store, and transmit based on the impact they would have on organizational operations and assets, individuals, other organizations, and the Nation in the event of a potential loss.

3. **Select,** tailor, and document the security controls necessary to protect systems based on the risk to organizational operations and assets, individuals, other organizations, and the Nation.

4. **Implement** the security controls and document specific details regarding how they are implemented.

5. **Assess** security controls to determine if they are implemented correctly, operating as intended, and producing the desired outcomes.

6. **Authorize** systems to operate based on associated risks to the organization.

7. **Monitor** the security of systems by maintaining ongoing situational awareness about risks.

NIST Zero Trust Architecture Guidance. This guidance provides a roadmap for organizations migrating to a zero trust design.[22] It outlines specific steps for migrating an agency's environment to a zero-trust architecture, while continuing to manage cybersecurity risks.[23] Specifically, the guidance instructs agencies to do the following:

- Identify the actors on the enterprise, to include humans and non-person entities (e.g., service accounts that interact with resources).

[22]National Institute of Standards and Technology, *Zero Trust Architecture*, Special Publication 800-207, (Gaithersburg, MD: August 2020). Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.

[23]Zero trust architecture is an enterprise's cybersecurity plan that uses zero trust concepts and encompasses component relationships, workflow planning, and access policies.

- Identify and manage assets owned by the enterprise, including hardware components (e.g., laptops and phones) and digital artifacts (e.g., user accounts, applications, and digital certificates).
- Identify and rank key processes and data flows, and the risk associated with them in relation to their impact on the organization's mission.
- Determine the set of criteria or confidence level weights for the trust algorithm that will be used to grant, deny, or terminate access to the organizations' assets and workflows.[24]
- Develop a list of zero-trust solutions that are appropriate for the organization's assets and workflows. Factors to consider in identifying these solutions include how it will be installed, logging and analysis capabilities, range of protocols covered, and performance requirements.
- Start initial deployment of the zero trust solutions and monitor them for effectiveness.
- Expand the zero-trust architecture and implement a steady operational phase for the enterprise. In this phase, networks and assets are still monitored, traffic is logged, feedback from relevant stakeholders is obtained, and any changes to the workflow are reevaluated.

[24]The trust algorithm is the process used by the policy engine to ultimately grant or deny access to a resource. A criteria-based trust algorithm assumes a set of qualified attributes that must be met before access is granted to a resource or an action is allowed. A score-based trust algorithm computes a confidence level based on values for every data source and enterprise-configured weights. If the score is greater than the configured threshold value for the resource, access is granted or the action is performed. If the score is lower, access is denied or access privileges are reduced.

FAA Clearly Defined Aviation Cybersecurity Roles and Responsibilities, but TSA Has Not; Both Met All Collaboration Practices

FAA's Cybersecurity Strategy, as of February 2026, defined the roles and responsibilities of the entities responsible for carrying out the agency's goals and objectives for aviation cybersecurity.[25] However, TSA's planning documents do not clearly define its roles and responsibilities for carrying out the agency's goals and objectives for aviation cybersecurity. Finally, FAA and TSA collaborated through the Aviation Cyber Initiative (ACI) and, in doing so, addressed all of the leading practices for interagency collaboration.[26]

FAA's Cybersecurity Strategy Defined Roles and Responsibilities for Carrying Out the Agency's Goals and Objectives

Based on our prior work, strategies should include overarching goals and objectives that address the overall results desired from implementing the strategy.[27] In addition, The NIST Cybersecurity Framework 2.0, states that organizations should define the cybersecurity roles and responsibilities of key parties to foster accountability and continuously improve effort.[28]

According to our analysis of FAA's Cybersecurity Strategy as of February 2026, FAA defined and documented its role and responsibilities for aviation cybersecurity. According to the strategy, it is intended to guide development of FAA's cybersecurity program and support efforts to balance and prioritize activities based on risk and mission needs. Figure 5 outlines the goals and supporting objectives described in FAA's Cybersecurity Strategy:

[25]In March 2026, FAA finalized an update to its Cybersecurity Strategy. The updated strategy outlines strategic objectives and associated key initiatives. While some of the strategic objectives and key initiatives are similar to the goals and objectives of the previous Cybersecurity Strategy that was the focus of our review, some of them differ. Additionally, the updated strategy does not identify the specific entities that are responsible for implementing it. However, the strategy states that FAA will develop a centralized implementation plan to guide the agency's achievement of the strategic objectives outlined within it.

[26]GAO-23-105520.

[27]GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

[28]National Institute of Standards and Technology, *The NIST Cybersecurity Framework.*

Figure 5: The Federal Aviation Administration (FAA) Cybersecurity Strategy Goals and Supporting Objectives

Goals	Objectives
Goal 1: Refine and maintain a cybersecurity governance structure to enhance cross-operating environment synergy.	• Maintain cross-organization processes for cybersecurity strategic planning and budget development. • Codify and maintain FAA-wide cybersecurity roles and responsibilities. • Improve understanding of cybersecurity risk for FAA-owned, FAA-contracted, and FAA-regulated systems. • Increase integration of cybersecurity activities across the agency's operating environments. • Update and maintain FAA-wide information security policies. • Implement the National Institute of Standards and Technology Cybersecurity Framework to manage risk.
Goal 2: Protect and defend FAA networks and systems to mitigate risks to FAA missions and service delivery.	• Improve cyber threat intelligence processing, dissemination, and reporting. • Improve FAA cyber monitoring, detection, and response capabilities. • Improve privileged user control, monitoring, and visibility. • Leverage cybersecurity research and development across FAA operating environments and systems. • Ensure FAA information security controls, policies, and processes are aligned with current NIST standards and guidelines. • Develop and implement zero trust architecture capabilities.
Goal 3: Enhance data-driven risk management decision capabilities.	• Continue implementing and enhancing the enterprise cyber threat modeling capability. • Expand information security continuous monitoring capabilities within the agency's operating environments. • Integrate threat, attack, and vulnerability data with mission focus to prioritize risks. • Reduce the time required to address high value threats and vulnerabilities.
Goal 4: Build and maintain cybersecurity workforce capabilities.	• Enhance the FAA-wide cybersecurity training, education, and awareness program. • Support cyber workforce training through participation in exercises. • Ensure that personnel with cybersecurity responsibilities receive appropriate role-based training. • Enhance FAA competitiveness in cybersecurity recruiting, hiring, and retention.
Goal 5: Build and maintain relationships with external partners in government and industry to improve cybersecurity in the aviation ecosystem.	• Expand participation in cyber exercises with external partners. • Increase collaboration with other government, industry, and private sector cybersecurity teams. • Ensure cybersecurity requirements are addressed in the Acquisition Management System and all FAA contract vehicles. • Expand information sharing with appropriate external partners, including through automated cyber threat indicator sharing. • Leverage the agency's regulatory role to identify and address cybersecurity risks in aircraft systems as well as automation of aircraft, equipment, and technology. • Represent the United States in global engagement on aviation cybersecurity through engagement with international partners. • Develop innovative cyber research initiatives with the Aviation industry sector.

Sources: GAO analysis of FAA's Cybersecurity Strategy; warmworld/stock.adobe.com (icons). I GAO-26-107693

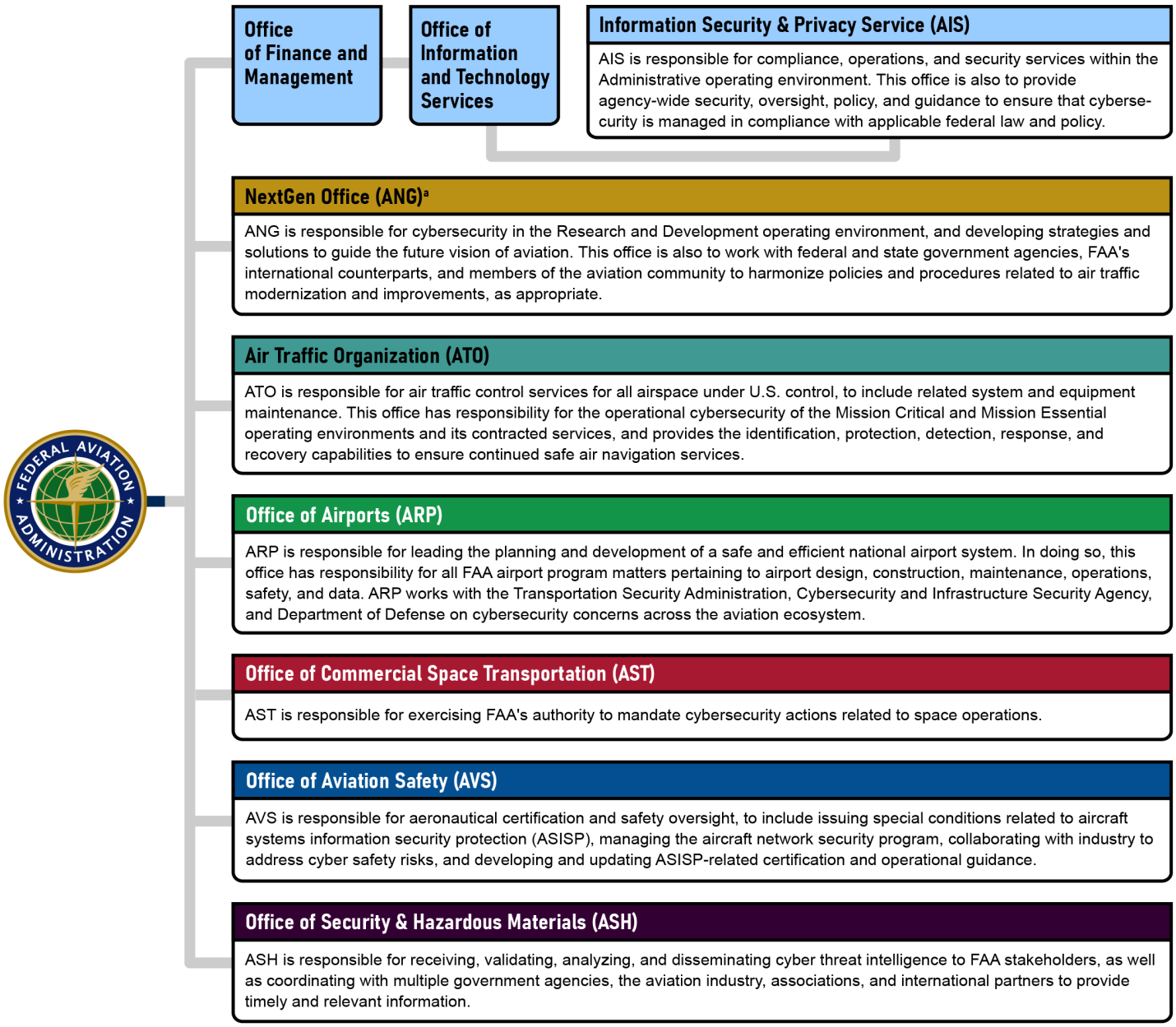
Note: In March 2026, FAA finalized an update to its Cybersecurity Strategy. The updated strategy outlines strategic objectives and associated key initiatives. While some of the strategic objectives and key initiatives are similar to the goals and objectives of the previous Cybersecurity Strategy that was the focus of our review, some of them differ.

Based on the FAA Cybersecurity Strategy as of February 2026, the agency has responsibilities for

- securing its internal systems,
- managing cybersecurity of the NAS,
- overseeing the cybersecurity of avionics through its aircraft certification process, and
- collaborating with relevant aviation stakeholders on cybersecurity.

The strategy further identified and described the responsibilities of seven FAA entities that have a role in implementing the strategy.
Figure 6 below illustrates the organizational structure and describes the responsibilities of the FAA entities that implement the strategy.

Figure 6: Organizational Structure of the Federal Aviation Administration (FAA) Entities Responsible for Implementing FAA's Cybersecurity Strategy



Sources: GAO analysis of FAA's Cybersecurity Strategy; Federal Aviation Administration logo. I GAO-26-107693

[a]Section 206 of the FAA Reauthorization Act of 2024 required FAA to terminate the NextGen Office on December 31, 2025, and transfer residual functions for the NextGen program to the Airspace Modernization Office. Section 207 of the act gives the Airspace Modernization Office responsibility for

research and development, systems engineering, enterprise architecture, and portfolio management for the continuous modernization of the national airspace system. On January 26, 2026, FAA announced the reorganization of the agency's structure. With the reorganization, the NextGen Office is to be replaced and its functions divided across several internal entities, to include the new Airspace Modernization Office.

TSA's Planning Documents Do Not Clearly Define Roles and Responsiblities for Carrying Out Goals and Objectives for Aviation Cybersecurity

As previously noted, strategies should include overarching goals and objectives that address the overall results desired from implementing the strategy.[29] Also, NIST's Cybersecurity Framework 2.0, states that organizations should define and communicate the cybersecurity roles and responsibilities of key parties to foster accountability and continuously improve effort.[30]

Together, TSA's Strategy for 2018 through 2026 and supplemental Administrator's Intent 3.0 define roles and responsibilities for the entities responsible for implementing the goals and objectives outlined in the strategy. However, these documents do not explicitly outline cybersecurity-specific goals and objectives for aviation cybersecurity. In addition, the 2018 TSA Cybersecurity Roadmap, which outlines goals and objectives, is outdated and no longer aligned with DHS' Cybersecurity Strategy.

TSA Strategy for 2018 through 2026. This strategy defines its overarching goals and objectives for carrying out the agency's mission and vision. None of the goals and supporting objectives explicitly describe the agency's plan for cybersecurity. Nonetheless, the strategy notes that cyber-physical interdependency creates a risk of intrusion or disruption from state and non-state actors to critical transportation infrastructure.

Administrator's Intent 3.0. This document is intended to help implement the TSA Strategy by outlining objectives that define how the agency will work toward its strategic priorities. The Administrator's Intent 3.0 describes an objective for improving TSA's ability to anticipate cyber risks and other emerging threats through greater understanding of their impact on the TSA mission. The document notes that Operations Support is to lead this objective with a targeted outcome of integrating and sharing insightful intelligence products using analysis capabilities that adjust to changing threats and reduces risk. However, the document does not

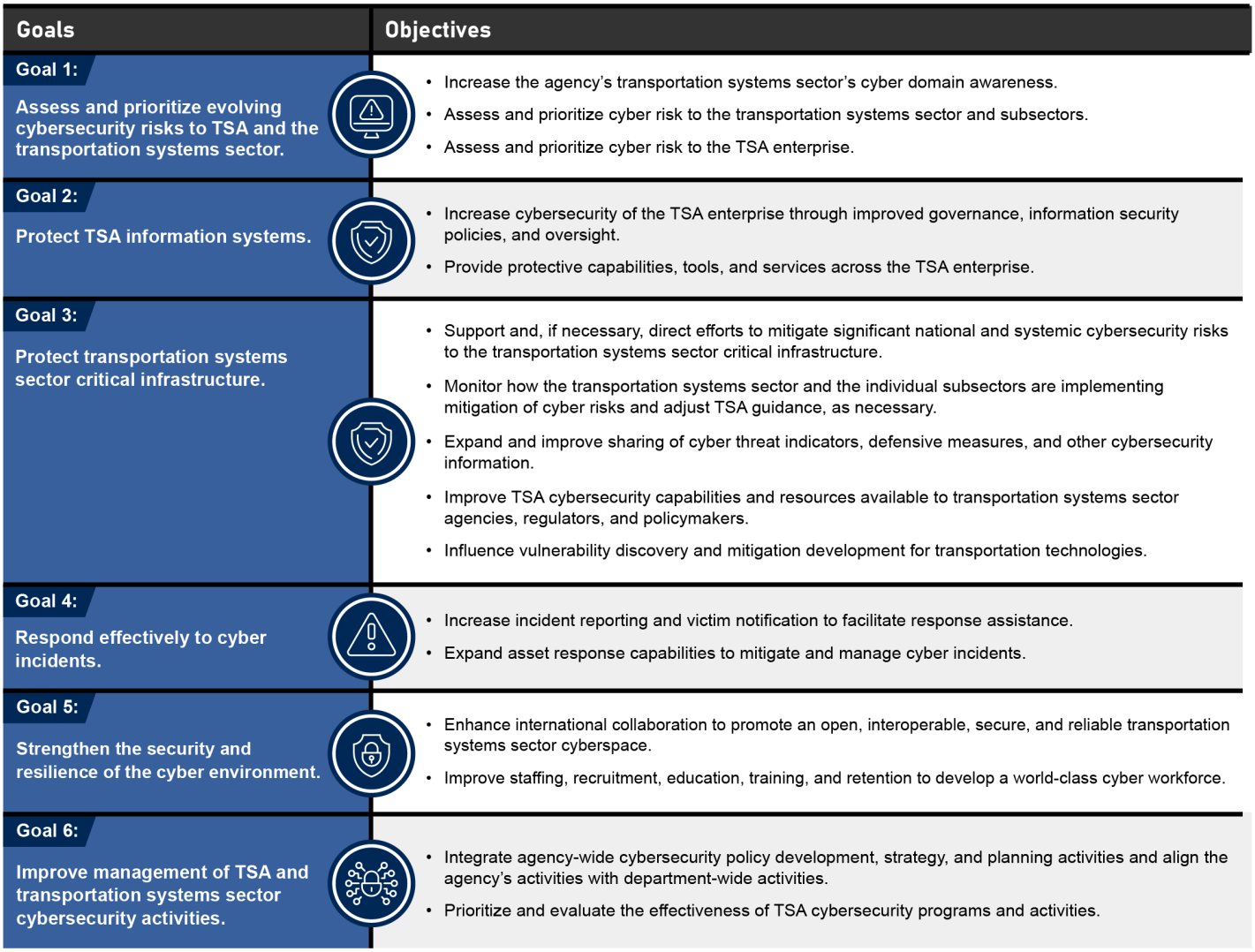
[29]GAO-04-408T.

[30]National Institute of Standards and Technology, *The NIST Cybersecurity Framework.*

specify if this objective and outcome are related to TSA's aviation cybersecurity efforts.

2018 TSA Cybersecurity Roadmap. This roadmap outlines the goals and objectives for prioritizing cybersecurity measures within TSA and in the transportation systems sector. Figure 7 outlines the goals and supporting objectives described in the 2018 TSA Cybersecurity Roadmap.

Figure 7: The 2018 Transportation Security Administration (TSA) Cybersecurity Roadmap Goals and Supporting Objectives



Sources: GAO analysis of TSA's 2018 Cybersecurity Roadmap; warmworld/stock.adobe.com (icons). I GAO-26-107693

Based on the 2018 TSA Cybersecurity Roadmap, the agency has responsibilities for

- assisting with steady-state and incident response activities, in coordination with DHS and the other sector risk management agencies;

- supporting comprehensive planning for a secure cyberspace in the aviation subsector; and
- providing security and mitigation guidance through outreach and information sharing activities, such as the Aviation Cyber Initiative.

However, the 2018 TSA Cybersecurity Roadmap does not describe the agency's cybersecurity-related roles and responsibilities for overseeing airport and aircraft operator security programs or identify the TSA entities responsible for implementing the goals and objectives it outlines.[31] The roadmap is also no longer aligned with the latest DHS Cybersecurity Strategy. According to the Administrator's Intent 3.0, TSA was to update its roadmaps, including the one for cybersecurity, between 2018 and 2026.

In interviews with 11 selected aviation stakeholders, some of the stakeholders expressed concerns about the clarity of TSA's role and responsibilities for aviation cybersecurity. Specifically, three of the aviation stakeholders—one avionics manufacturer, one airline, and one industry group—told us that they were challenged in understanding TSA's role in aviation cybersecurity. Representatives from the same airline mentioned above informed us that they felt that the agency lacked the resources, authority, and expertise to properly regulate cybersecurity. Additionally, three other stakeholders—one avionics manufacturer, one airline, and one industry group—stated that TSA's issuance of cybersecurity requirements through a Joint Emergency Amendment in March 2023 created confusion among the stakeholders who presumed that the issuance of such requirements fell under FAA's oversight role. Specifically, TSA's March 2023 Joint Emergency Amendment required the security programs for covered airports and aircraft operators to include cybersecurity measures intended to prevent the disruption and degradation of critical systems, which TSA defined as any IT, OT, or business support services that, if compromised or exploited, could result in an operational disruption.

TSA has taken some action in response to the aviation stakeholders' concerns with TSA's role in addressing aviation cybersecurity. For example, TSA worked closely with FAA to clarify the applicability of its March 2023 Joint Emergency Amendment addressing cybersecurity

[31]TSA mandates airport operators and air carriers to adopt and carry out a security program approved by TSA in accordance with requirements set forth in regulation at 49 C.F.R. part 1542 (airport operators), part 1544 (domestic air carriers), and part 1546 (foreign air carriers).

threats to certain aviation stakeholders.[32] This coordination resulted in the February 2024 Frequently Asked Questions for the emergency amendment, which noted that any logical or physical resources that are internal or external to an aircraft and contribute to its airworthiness are excluded from the scope of the emergency amendment. Additionally, according to the aviation stakeholders we interviewed, the FAA Reauthorization Act of 2024's provision that grants FAA exclusive authority to regulate the cybersecurity of civil aircraft helped to provide some clarity.

As previously mentioned, FAA has clearly defined its role and responsibilities for the cybersecurity of avionics and the ground systems it operates in the NAS. While both FAA and TSA agree that TSA does not have a role or responsibilities for avionics and ground systems, the interconnectivity between these systems and others operating in the aviation ecosystem creates the appearance of overlapping roles and responsibilities among these two agencies. Until TSA defines its roles and responsibilities for carrying out its cybersecurity goals and objectives, including those related to airports and aircraft operators, the aviation stakeholders may continue to lack clarity on the applicability of emergency amendments or other security requirements issued by the agency pursuant to its statutory authority. Ambiguity in TSA's roles and responsibilities—and in turn, stakeholders' requirements for cybersecurity—could potentially increase the risk of covered systems being exploited. Further, TSA may be challenged in holding relevant entities accountable or enabling continuous improvements to its related efforts.

FAA and TSA Addressed Leading Practices for Collaborating on Aviation Cybersecurity

FAA and TSA fully addressed all eight of GAO's leading practices for interagency collaboration while serving in leadership roles for collaborative aviation cybersecurity efforts. GAO developed these eight practices and associated key considerations to provide guidance to improve collaboration between agencies, or within components of the same agency.[33] Figure 8 lists each leading practice and associated key considerations for collaborating.

[32]Air carriers are responsible for implementing TSA security requirements predominantly through TSA-approved security programs. TSA may impose additional requirements in the form of security directives or emergency amendments when more immediate action on behalf of air carriers is necessary. See 49 C.F.R. §§ 1544.105(d), 1544.305, 1546.105(d).

[33]GAO-23-105520.

Figure 8: GAO's Leading Interagency Collaboration Practices and Examples of Associated Key Considerations

Leading Interagency Collaboration	Key Considerations
Define Common Outcomes	• Have the crosscutting challenges or opportunities been identified? • Have the short- and long-term outcomes been clearly defined? • Have the outcomes been reassessed and updated, as needed?
Ensure Accountability	• What are the ways to monitor, assess, and communicate progress toward the short- and long-term outcomes? • Have collaboration-related competencies or performance standards been established against which individual performance can be evaluated? • Have the means to recognize and reward accomplishments related to collaboration been established?
Bridge Organizational Cultures	• Have strategies to build trust among participants been developed? • Have participating agencies established compatible policies, procedures, and other means to operate across agency boundaries?
Identify and Sustain Leadership	• If leadership will be shared between one or more agencies, have roles and responsibilities been clearly identified and agreed upon? • How will leadership be sustained over the long term?
Clarify Roles and Responsibilities	• Have the roles and responsibilities of the participants been clarified? • Has a process for making decisions been agreed upon?
Include Relevant Participants	• Have all relevant participants been included? • Do the participants have the appropriate knowledge, skills, and abilities to contribute? • Do participants represent diverse perspectives and expertise?
Leverage Resources and Information	• How will the collaboration be resourced through staffing? • How will the collaboration be resourced through funding? If interagency funding is needed, is it permitted? • Are methods, tools, or technologies to share relevant data and information being used?
Develop and Update Written Guidance and Agreements	• If appropriate, have agreements regarding the collaboration been documented? • Have ways to continually update or monitor written agreements been developed?

Sources: GAO analysis of leading interagency collaboration practices and key considerations; warmworld/stock.adobe.com (icons). I GAO-26-107693

FAA and TSA have collaborated on aviation cybersecurity through the Aviation Cybersecurity Initiative (ACI). ACI is a task force led by three chairs designated from DOT, DHS, and the Department of Defense.[34] DOT and DHS assigned a chair from FAA and TSA to represent those departments' interests and missions. Collectively, these three chairs are referred to as Tri-Chairs. Through ACI, FAA and TSA fully addressed all eight of the leading practices for interagency collaboration. Figure 9 illustrates our assessment of how FAA and TSA implemented the leading practices.

Figure 9: Extent to Which the Federal Aviation Administration and Transportation Security Administration Addressed Leading Practices for Interagency Collaboration

GAO's Leading Practices for Interagency Collaboration	GAO Assessment
Define common outcomes	●
Ensure accountability	●
Bridge organizational cultures	●
Identify and sustain leadership	●
Clarify roles and responsibilities	●
Include relevant participants	●
Leverage resources and information	●
Develop and update written guidance and agreements	●

● Fully addressed ◐ Partially addressed ○ Not addressed

Source: GAO analysis of the Aviation Cybersecurity Initiative's documentation. | GAO-26-107693

ACI leadership, including FAA and TSA, fully addressed all of the eight leading practices for interagency collaboration to address cybersecurity threats against the aviation ecosystem through ACI. For example:

Define common outcomes. ACI leadership documented the group's purpose, mission, and key goals in a charter. Specifically, the charter

[34]While the Department of Defense is an active member of ACI, Section 396 of the FAA Reauthorization Act of 2024 includes a provision for us to review how TSA and FAA differentiate and manage their roles and responsibilities for the cybersecurity of aircraft and ground systems.

notes that ACI was established to provide a forum for coordination and collaboration on activities aimed at cyber risk reduction within the aviation ecosystem. The ACI charter states that the group's long-term goal is to reduce cybersecurity risks and improve cyber resilience to support safe, secure, and efficient operations of the Nation's aviation ecosystem. This long-term goal is to be implemented through short-term goals that are addressed in the priorities and projects established for the group. Examples of short-term goals identified for the group in 2024 include cyber risk mitigation initiatives, conducting aviation cyber tabletop exercises, and holding aviation cyber summits.

Clarify roles and responsibilities. The ACI charter documents the roles and responsibilities of the group's members. For example, the charter defines the Executive Committee as the main leadership body for ACI that is responsible for providing guidance and support to the Tri-Chairs in achieving the group's objectives. Additionally, the charter states that the Tri-Chairs will lead ACI's activities and, in doing so, are responsible for representing the interests and mission of their respective department, along with coordinating relevant partners on ACI's programs and projects.

Include relevant participants. FAA and TSA ensured that ACI included relevant participants in ACI's activities. The charter states that ACI may invite other federal departments and agencies to contribute to the work of the collaborative group and meet specific objectives. Additionally, according to the ACI Communications Plan, the initiative collaborates with a diverse group of aviation stakeholders, including industry and commercial organizations, federal departments and agencies, affiliated entities, and state, local, territorial and tribal governments.[35] Six of the eleven aviation stakeholders we interviewed—five industry groups and one avionics manufacturer—stated that they participated in ACI. Four stakeholders—two airlines, one industry group, and one research organization—stated that they do not actively participate in ACI. One of these airlines informed us that they received information from ACI, although they are not an active participant. The remaining stakeholder—an avionics manufacturer—provided written responses and did not mention any involvement in ACI.

[35]Some of the aviation organizations participating in ACI includes Airlines for America, Airports Council International-North America, Aerospace Industries Association, Airline Pilots Association, General Aviation Manufacturers Association, Garmin, and MITRE.

For a full description of FAA and TSA efforts to address GAO's leading interagency collaboration practices through ACI, see appendix II.

As a result of FAA and TSA's collaborative efforts through ACI, the agencies are better positioned to reach the group's goal to provide a forum for coordination and collaboration on activities aimed at cyber risk reduction within the aviation ecosystem.

FAA Entities with Cybersecurity Responsibilities Had Varying Budget Requests from Fiscal Years 2024 to 2026 and Did Not Report All Spending to OMB

Seven FAA entities are responsible for implementing the agency's Cybersecurity Strategy.[36] According to the President's budget requests, the amounts requested for these seven entities varied across fiscal years 2024 through 2026.

OMB instructs agencies to report their cybersecurity activity spending to inform the annual President's Budget each year. This process is known as OMB's cyber budget data request. The President's budget request for FAA described programs and costs associated with the agency's Cybersecurity Strategy for fiscal years 2024 through 2026. However, FAA did not report the cost of all these cybersecurity programs as part of OMB's cyber budget data request process.

FAA Entities That Implemented the Cybersecurity Strategy Had Varying Budget Requests from Fiscal Years 2024 Through 2026

As previously discussed, there are seven FAA entities responsible for implementing the Cybersecurity Strategy. The President's budget requests for these entities varied across fiscal years 2024 through 2026.[37] Table 1 illustrates the budget requests for the FAA entities during this time period.

[36]In March 2026, FAA finalized an update to its Cybersecurity Strategy. The updated strategy outlines strategic objectives and associated key initiatives. While some of the strategic objectives and key initiatives are similar to the goals and objectives of the previous Cybersecurity Strategy that was the focus of our review, some of them differ.

[37]The fiscal year 2024 through 2026 President's budget requests for FAA included actual funding for the prior fiscal year, enacted (or annualized continuing resolution) funding for the current year, and requested funding for the next year. We used the requested funding for fiscal years 2024 through 2026 to ensure current and consistent budget data across these years.

Table 1: Fiscal Year 2024 Through 2026 President's Budget Requests for the Federal Aviation Administration Entities Responsible for Implementing the Cybersecurity Strategy

Federal Aviation Administration entity	Fiscal year (FY) 2024 budget request (in thousands)	FY 2025 budget request (in thousands)	FY 2026 budget request (in thousands)
Air Traffic Organization	$9,898,941	$10,616,510	$10,873,540
Aviation Safety	$1,759,115	$1,844,532	$1,888,485
Commercial Space Transportation	$42,018	$57,130	$42,179
Finance & Management	$998,903	$1,057,640	$1,038,355
NextGen Office[a]	$181,334	$186,660	$176,172
Security and Hazardous Materials Safety	$164,731	$177,745	$164,469
Airports	$157,475	$163,624	$160,000

Source: GAO analysis of the fiscal year 2024 through 2026 President's budget requests for the Federal Aviation Administration. | GAO-26-107693

[a]Section 206 of the FAA Reauthorization Act of 2024 required FAA to terminate the Next Gen Office on December 31, 2025, and transfer residual functions for the NextGen program to the Airspace Modernization Office. Section 207 of the act gives the Airspace Modernization Office responsibility for research and development, systems engineering, enterprise architecture, and portfolio management for the continuous modernization of the national airspace system. On January 26, 2026, FAA announced the reorganization of the agency's structure. With the reorganization, the NextGen Office is to be replaced and functions divided across several internal entities, to include the new Airspace Modernization Office.

FAA Entities Did Not Report All Cybersecurity Spending to OMB

Each year, OMB instructs agencies to report their cybersecurity activity spending to inform the annual President's Budget. OMB's December 2023 instructions for responding to its budget data request instructed agencies to report spending to reflect fiscal year 2023 actuals, fiscal year 2024 estimates, and fiscal year 2025 budget request.[38] Additionally, the instructions requested agencies to report cybersecurity activity funding data at the capability level. Most of these capabilities are associated with one of the five NIST Cybersecurity Framework functions—identify, protect, detect, respond, and recover.[39] Within the protect function, agencies are to report funding for research and development related to

[38]Office of Management and Budget, *Government-wide Tracking of Resources for Cyber Activities*, Budget Data Request No. 23-29, Addendum 1 (Washington, D.C. Dec. 12, 2023).

[39]Outside of the NIST Cybersecurity Framework functions, there are capabilities associated with Human Capital and Sector Risk Management functional areas.

cybersecurity and information assurance intended to protect systems and their data from actions that compromise, or threaten to compromise, authentication, availability, integrity, and confidentiality. Additionally, the agencies are to report funding that has not been accounted for in any of the defined capabilities.

The fiscal year 2024 through 2026 President's budget requests for FAA described programs and costs associated with the agency's implementation of its Cybersecurity Strategy. For example, according to these budget requests:

- Office of Financial Management's (AFN) Cybersecurity Program funds FAA's security operations center, which operates as a shared service provider of network security services to the DOT. Additionally, it supports FAA's plans to implement public key infrastructure to provide authentication, encryption, and integrity needed for a zero-trust model. It is also responsible for enhancing FAA's existing cybersecurity program to ensure that defined technical requirements and mandates are met.
- Information Systems Security Enhancement is intended to improve the cybersecurity posture across FAA and strengthen the security of aviation through collaboration with public and private entities, and the intelligence community. The program funds NAS critical infrastructure cybersecurity enhancements that improve the security and resiliency of FAA systems.
- The NAS Critical Infrastructure Cyber Enhancement Program provides services and capabilities to enhance air traffic control and ensures the NAS remains secure and resilient. The program includes network and access control, enterprise tools, evolving threat protection, and secure remote access.
- The Information Security/Cybersecurity Program conducts research, analysis, demonstration, evaluation, and protype development of cybersecurity data science tools and technologies. This program also develops methods to detect, prevent, and mitigate the effects of cyber-attacks on elements of the aviation ecosystem. The goal of the program is to mitigate safety risks to aircraft operations that derive from cyber vulnerabilities. Table 2 shows the President's budget requests for these FAA programs for fiscal years 2024 through 2026.

Table 2: Fiscal Year 2024 Through 2026 President's Budget Requests for Federal Aviation Administration Cybersecurity Programs

Cybersecurity program	Fiscal year 2024 budget request	Fiscal year 2025 budget request	Fiscal year 2026 budget request
Office of Financial Management Cybersecurity Program	0	4 million	35 million[a]
Information Systems Security Enhancement	12 million	12 million	0
National Airspace System Critical Infrastructure Cyber Enhancement Program	20 million	26.7 million	27million[b]
Information Security/ Cybersecurity Program	6.4 million	5.9 million	4.6 million

Source: GAO analysis of the fiscal year 2024 through 2026 President's budget requests for the Federal Aviation Administration. | GAO-26-107693

[a]FAA planned to modernize the entire AFN Cybersecurity program in fiscal year 2026 to include updating on-premises data centers, increasing network boundary protection, and implementing zero trust requirements, among other things.

[b]In fiscal year 2026, the Information Systems Security Enhancement program was combined with the NAS Critical Infrastructure Cyber Enhancement program.

However, we found that the agency did not include spending data for its Information Security/Cybersecurity Program that supports its research and development activities as part of its budget data request reporting. According to FAA officials, the agency included the cost for this program in its most recent cyber budget data request reporting that it submitted to DOT on September 24, 2025, for the President's budget request for fiscal year 2027. However, as of April 2026, the agency had not provided evidence that it included cost for the Information Security/Cybersecurity Program in its cyber budget data reporting submission to DOT, or what the spending level was.

FAA did not report its Information Security/Cybersecurity Program as part of its cyber budget data request reporting because the agency's Cyber Budget Data Request Process does not require the agency to report all cybersecurity spending data.[40] Specifically, FAA's process only accounts for cybersecurity spending data for investments

[40]FAA's Cyber Budget Data Request Process outlines procedures for the agency to gather and report information to inform policy officials and Congress on their cybersecurity activity spending. The process requires FAA to provide cybersecurity spending data to support the Department of Transportation's response to OMB's cyber budget data request.

pre-populated in the data call spreadsheet used by the agency to collect data for OMB's budget data request. Additionally, the process does not specify that the program offices can add additional cybersecurity activity spending data to the data call spreadsheet.

Until FAA can comprehensively report its cybersecurity activities and costs for OMB's cyber budget data request, the agency increases the risk that policy officials and Congress will not have a complete understanding of FAA's cybersecurity activity spending, including its research and development activities. These activities play a significant role in the agency's NAS modernization efforts, as overall progress will rely on testing technologies and capabilities, such as artificial intelligence and machine learning. This could also impact the policy officials and Congress decisions regarding future cybersecurity funding.

FAA's Cybersecurity Strategy Aligned with Most Key Mitigation Practices for Avionics and Ground Systems in the NAS

FAA's Cybersecurity Strategy, as of February 2026, and associated processes for ensuring the security of avionics and the ground systems it operates in the NAS aligned with key risk and vulnerability mitigation practices.[41] Additionally, the strategy included the agency's plans to implement zero trust architecture capabilities to better protect its networks and systems. However, FAA's Zero Trust Implementation Plan that describes the agency's approach for transitioning its operating environments to a zero trust architecture did not fully align with related NIST guidance.[42]

[41]As discussed earlier, in March 2026, FAA finalized an update to its Cybersecurity Strategy. The updated strategy outlines strategic objectives and associated key initiatives. While some of the strategic objectives and key initiatives are similar to the goals and objectives of the previous Cybersecurity Strategy that was the focus of our review, some of them differ. The strategy states that FAA will develop a centralized implementation plan to guide the agency's achievement of the strategic objectives outlined within it.

[42]According to NIST, zero trust architecture is an enterprise's cybersecurity plan that uses zero trust concepts that are designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. National Institute of Standards and Technology, *Zero Trust Architecture*.

FAA's Strategies for Securing Avionics and Ground Systems Align with Key Federal and Industry Cybersecurity Risk Mitigation Practices

FAA's processes for ensuring the security of avionics and the ground systems it operates in the NAS align with the key federal and industry cybersecurity risk mitigation practices that we identified. Those key practices are to

- define the characteristics of the system, to include its intended purpose;
- determine the appropriate level of security for the system based on identified risks and threats;
- identify the security measures to achieve the appropriate level of security;
- implement the security measures;
- assess the effectiveness of the implemented security measures;
- document the security activities and make a determination about authorizing/certifying the system to operate, to include accepting any remaining risks; and
- monitor the effectiveness of the security measures and re-assess security impacts as modifications are made to the system.[43]

FAA's Cybersecurity Strategy, as of February 2026, described the aircraft certification and safety oversight responsibilities of the Office of Aviation Safety (AVS), to include applying special conditions to address cybersecurity risks to airplane systems and networks. We described FAA's use of special conditions to address cybersecurity risks to avionics in a prior GAO report.[44] Special conditions apply to a specific aircraft design when existing regulations do not adequately address a novel or unusual design feature, such as onboard computer networks or avionics.

[43]We identified these key federal and industry cybersecurity risk mitigation practices by compiling common themes outlined in the following. National Institute of Standards and Technology, *Risk Management Framework*; American Society for Testing and Materials, *Standard Practice for Protection of Aircraft Systems from Intentional Unauthorized Electronic Interactions* (Feb. 1, 2022*);* and Radio Technical Committee for Aeronautics, *Airworthiness Security Process Specification* (Washington D.C.: August 6, 2014).

[44]GAO-21-86.

During the certification process for aircraft with special conditions, the applicant proposes a means of compliance that FAA reviews for consistency with its certification basis and applicable FAA policies.[45] The means of compliance is demonstrated through design data, interfaces, risk assessments, and other documentation needed to show compliance with the certification basis and applicable special conditions. FAA reviews this documentation and any proposed mitigations to determine whether the applicant has met the applicable requirements for certification. For instance, during the certification of an aircraft with special conditions related to the cybersecurity of avionics, the applicant develops and provides FAA with a risk assessment for the individual special condition. FAA engineers are to review the aircraft's architecture and determine how to address the risks to avionics. Any potential risks must be mitigated to FAA's satisfaction prior to certification of an aircraft.

When the applicant believes it has fulfilled all the regulations that apply to the aircraft's certification, including means of compliance for special conditions, they assemble a protoype aircraft with all systems in place. Testing is performed to show that required protections and mitigations are in place and are functioning as intended. This may include the internal networking and cybersecurity controls needed to ensure that mitigations are in place and functioning properly. FAA approves the test plans and reviews the testing results and certification package to decide whether to issue the certification approval for the aircraft.

Aircraft that have been certified with special conditions that requires operator action to mitigate electronic security risks are required to have an aircraft network security program.[46] In this situation, the design approval holder provides network security guidance and, where applicable, instructions for continued airworthiness that the operator uses

[45]FAA deems aircraft cybersecurity standards that have been issued by aviation standards development organizations, such as RTCA and the American Society for Testing and Materials, as accepted means of compliance for applicable special conditions. A certification basis identifies the applicable standards and amendment levels that the applicant must show compliance with. For example, a type certification is the approval of the design of the aircraft and all its components and signifies that the aircraft design is in compliance with all applicable standards.

[46]The aircraft network security program includes instructions on maintenance of the aircraft's internal networks and external connections, a forensic analysis process to address safety-related cybersecurity incidents, and requirements for incident reporting. These instructions to the aircraft operator may be in addition to the design approval holder's instructions that were created to meet the special conditions.

to develop and maintain the aircraft network security program.[47] The aircraft network security program is intended to ensure

- sufficient data security protection to prevent unauthorized access by external devices and personnel;
- identification and assessment of security threats;
- implementation of mitigation strategies to ensure the continued airworthiness of the aircraft;
- prevention of inadvertent or malicious changes to the aircraft network, systems, and software; and
- prevention of unauthorized access from sources onboard the aircraft.

Components of the aircraft network security program include a description of the security environment and plans and procedures for access control to networks, systems, and software and event identification, response, and recovery, among other things. The agency monitors implementation of the aircraft network security program as part of its oversight of fleet safety.

In August 2024, FAA issued a notice of proposed rulemaking that would add type certification and continued airworthiness requirements to protect transport category airplanes, engines, and propellers from intentional unauthorized electronic interactions that could create safety hazards.[48] According to the proposed rule, the continued airworthiness requirements are primarily based on past special conditions that FAA issued to address cybersecurity. FAA's current use of special conditions, together with the proposed rule, if finalized in its current state, aligns with the key federal and industry practices that we identified for cybersecurity risk mitigation, as described in appendix III.

For NAS systems operated by FAA, the agency's information security program is intended to address cybersecurity risk to those systems. According to the FAA Cybersecurity Strategy as of February 2026, the agency's information security controls, policies, and processes need to be

[47]The design approval holder is an entity, such as a manufacturer, that has FAA authorization for an aircraft product's design.

[48]Intentional unauthorized electronic interaction is defined as a circumstance or event with the potential to affect the aircraft due to human action resulting from unauthorized access, use, disclosure, denial, disruption, modification, or destruction of information and/or aircraft system interfaces. This includes malware and the effects of external systems, but does not include physical attacks, such as electromagnetic jamming.

aligned with NIST standards and guidelines.[49] FAA's supplemental implementing directive on Information Security and Privacy Governance requires the agency to use its Security Authorization Handbook for the initial authorization and continuous monitoring assessment of systems.[50]

FAA's Security Authorization Handbook is intended to guide the agency in applying the NIST risk management framework. The handbook outlines the agency's risk management and security authorization process for all its systems, including those operating in the NAS. Additionally, the agency's Air Traffic Organization (ATO) Information Security Continuous Monitoring (ISCM) Plan aligns with the Security Authorization Handbook and outlines FAA's approach for performing continuous monitoring in support of ongoing authorization decisions for NAS systems. The handbook and ATO ISCM Plan address the key federal and industry practices that we identified for cybersecurity risk mitigation, as described in appendix III.

FAA's Strategy for Ensuring Cybersecurity Aligns with Some, but Not All, Zero Trust Migration Practices

FAA's Cybersecurity Strategy includes the agency's plans to better protect its networks and systems by developing and implementing zero trust architecture capabilities.[51] However, FAA's Zero Trust Implementation Plan that is intended to guide development of the agency's zero trust architecture capabilities partially aligns with NIST's Zero Trust Architecture guidance.[52] NIST's guidance on Zero Trust Architecture provides a roadmap for organizations migrating to a zero trust design. In doing so, the guidance notes that the specific steps for migrating to a zero-trust architecture are to:

- **Identify actors** on the enterprise, to include both human and possible non-person entities.

[49]The updated March 2026 strategy does not outline a strategic objective or key initiative for aligning with NIST standards and guidelines. However, it describes a desired end state for doing so.

[50]FAA's supplemental implementing directive on governance supports and provides more details on the requirements set forth in the agency's overarching Information Security and Privacy Policy, which establishes the core management policies and responsibilities for its related programs.

[51]The updated March 2026 strategy includes a strategic objective for developing a strong foundation for maintaining a robust defensive posture through implementation of key initiatives related to zero trust capabilities.

[52]National Institute of Standards and Technology, *Zero Trust Architecture.*

- **Identify and manage assets** owned by the enterprise, to include hardware components and digital artifacts.
- **Identify and rank key processes and data flows** and the risk associated with them in relation to their impact on the organization's mission.
- **Determine the set of criteria or confidence level weights** that the trust algorithm will used to grant, deny, or terminate access to assets and workflows.[53]
- **Develop a list of zero trust architecture solutions** that are appropriate for the organization's assets and workflows.
- **Start initial deployment of the zero trust solutions** and monitor them for effectiveness.
- **Expand the zero-trust architecture** and implement a steady operational phase for the enterprise that consists of monitoring networks and assets, logging traffic, obtaining feedback from relevant stakeholders, and reevaluating any changes to the workflow.

According to FAA's Cybersecurity Strategy as of February 2026, the agency plans to better protect its networks and systems by developing and implementing zero trust architecture capabilities.[54] To this end, FAA's August 2023 Zero Trust Implementation Plan includes timelines for transitioning its Administrative, Mission Essential, and Mission Critical operating environments to a zero-trust architecture. The plan addresses changes in the Mission Essential and Mission Critical operating environments that will occur as a result of NAS modernization. However, the plan does not include details on the Research and Development operating environment's transition to a zero-trust architecture. Instead, the plan notes that the Research and Development operating environment will install and deploy a combination of the tools and technologies planned for each of the other operating environments. Given the Research and Development operating environment interfaces with

[53]The trust algorithm is the process used by the policy engine to ultimately grant or deny access to a resource. A criteria-based trust algorithm assumes a set of qualified attributes that must be met before access is granted to a resource or an action is allowed. A score-based trust algorithm computes a confidence level based on values for every data source and enterprise-configured weights. If the score is greater than the configured threshold value for the resource, access is granted or the action is performed. If the score is lower, access is denied or access privileges are reduced.

[54]In March 2026, FAA finalized an update to its Cybersecurity Strategy. The updated strategy outlines strategic objectives and associated key initiatives. While some of the strategic objectives and key initiatives are similar to the goals and objectives of the previous Cybersecurity Strategy that was the focus of our review, some of them differ.

other agencies and aviation partners, also addressing the transition to zero trust capabilities for this operating environment in the FAA Zero Trust Implementation Plan would enable more comprehensive plans for managing risks.

Additionally, FAA's Zero Trust Implementation Plan fully aligns with three of the seven practices NIST outlined for migrating to a zero-trust architecture. The plan partially aligns with the remaining four practices. Specifically, while FAA's plan fully describes the agency's efforts to determine a set of criteria that the trust algorithm will use to grant, deny, or terminate access, develop a list of zero trust architecture solutions, and expand its zero-trust architecture, it does not do the following:

- Outline how FAA is to identify the actors that will interact with the agency's resources within its Administrative, Mission Critical, and Research & Development operating environments.
- Describe FAA's efforts to identify and manage assets within the Research & Development operating environment.
- Define how the agency is to identify data flows, business processes, and workflows in the Administrative and Research and Development operating environments. It also does not describe how the agency is to identify workflows within the Mission Critical operating environment.
- Describe the agency's efforts to monitor implementation of the zero-trust algorithm that is used to inform access decisions in the Administrative, Mission Essential, Mission Critical, and Research and Development operating environments.

Appendix III provides more details on our assessment of the extent to which FAA's Zero Trust Implementation Plan addresses NIST's seven steps for migrating to a zero-trust architecture.

FAA officials acknowledged that its Zero Trust Implementation Plan did not fully align with all NIST best practices for migrating to a zero-trust architecture. The officials stated that they will address those practices in their fiscal year 2026 update to the plan, which is currently ongoing.

Without fully aligning FAA's Zero Trust Implementation Plan with NIST best practices for migrating to a zero-trust architecture across all four of its operating environments, the agency cannot ensure that it is effectively managing cybersecurity risks, including during the NAS modernization effort. More specifically, until FAA fully identifies the actors, assets, key processes, and data flows across its entire enterprise, the agency cannot

establish a baseline to inform plans to migrate to a zero trust architecture. This could in turn cause gaps in the agency's implementation of zero trust capabilities. Additionally, without monitoring the zero-trust algorithm used to inform access decisions, FAA cannot ensure that the algorithm is effective and working properly to protect the assets on its network from unauthorized access.

FAA Partially Implemented Its Cybersecurity Strategy to Mitigate Risks to Its Networks and Systems

In our review of FAA's Cybersecurity Strategy as of February 2026, the agency had not fully implemented all of the objectives supporting its goal to protect and defend the agency's networks and systems. The second goal outlined in the FAA Cybersecurity Strategy was to protect and defend FAA networks and systems to mitigate risks to the agency's missions and service delivery. The strategy described seven objectives that outline the agency's plans for achieving the goal:

- Improve cyber threat intelligence 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 internal and external threats.
- Leverage cybersecurity research and development across FAA operating environments and systems.
- Ensure FAA information security controls, policies, and processes are aligned with current NIST standards and guidelines.
- Develop and implement zero trust architecture capabilities.

FAA fully implemented three of the objectives supporting its goal to protect and defend the agency's networks and systems and partially implemented the other four objectives. Table 3 describes our assessment of FAA's progress in implementing the seven objectives supporting its goal.

Table 3: Assessment of Federal Aviation Administration's Efforts to Implement its Cybersecurity Strategy Goal to Protect and Defend its Networks and Systems, as of February 2026

Goal objective	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 operating environments 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	◐

● = fully implemented ◐ = partially implemented ○ = did not implement.

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

The sections below describe how FAA addressed the seven objectives supporting its goal to protect and defend the agency's networks and systems.

Improve Cyber Threat Intelligence Collection, Processing, Dissemination, and Reporting—fully implemented. According to the FAA Cybersecurity Strategy, the agency planned to improve its capabilities and use of commercial and government sources, as well as open-source intelligence, to drive improvements in the protection and defense of FAA networks and systems. To do this, the agency's Office of Security and Hazardous Materials Safety (ASH) is responsible for leading the development and improvement of processes for the dissemination of cyber threat intelligence within FAA and to external partners.

FAA has developed process-based improvements that establish and enhance information sharing for cyber threat intelligence and assessments, cyber risk trends, and ongoing collaboration efforts across the agency. FAA's whitepaper on standard operating procedures for process-based improvements in cyber threat intelligence sharing outlines the agency's approach for doing so. The whitepaper lists the mechanisms ASH uses to share classified and open-source cyber threat intelligence,

such as briefings, reports, flyers, notes, bulletins, and assessments. According to ASH's Homeland Security Information Network homepage, the entity shares cyber reports, open-source library resources, and notices.[55] The whitepaper also summarizes recent and process-based information sharing processes, such as an updated email distribution system, a plan that outlines ASH's priority intelligence products for the fiscal year, and guides for sharing unclassified information and formatting intelligence products. For example, ASH developed an information note template to describe the contents, grammar, and style that should be included in the notes. ASH's Intelligence & Threat Analysis Division also developed a grammar, style, and product formatting guide to promote consistency across its information sharing products.

Additionally, FAA officials stated that ASH partnered with other government agencies to coordinate, collaborate, and facilitate intelligence and information sharing on cybersecurity threats to the civil aviation ecosystem and national and international airspace.

Improve FAA Cyber Monitoring, Detection, and Response Capabilities—partially implemented. The strategy states that FAA planned to improve cyber monitoring, detection, and response capabilities through the adoption of new technologies. In April 2025, FAA stated that they had improved cyber monitoring, detection, and response through capabilities, such as continuous diagnostics and mitigations (CDM) tools and logging maturity. A 2024 Department of Transportation (DOT) Office of the Inspector General (OIG) report that assessed the department's continuous monitoring tools for detecting, preventing, and reporting cyber threats found that FAA is not using tools to provide near real-time monitoring on all mission-critical NAS systems.[56] Specifically, while DOT used continuous monitoring tools to support essential CDM requirements, FAA had not performed near real-time cyber monitoring activities on 62 of 85 NAS Cyber Management Systems due to air traffic and safety concerns.

[55]The Homeland Security Information Network is DHS's official system for trusted sharing of sensitive but unclassified information between federal, state, local, territorial, tribal, international and private sector partners.

[56]Department of Transportation Office of the Inspector General, *DOT Uses Continuous Monitoring Tools to Automate Cybersecurity Monitoring But Needs to More Effectively Detect, Prevent, and Report Cybersecurity Threats*, No. IT2024041 (Washington, D.C.: Sept. 30, 2024).

The DOT OIG recommended that FAA implement procedures to perform near real-time cyber monitoring activities. FAA agreed with the recommendation but had not implemented the recommendation, as of June 2026. According to FAA officials, 20 of the 62 NAS Cyber Management Systems that were found to not be undergoing real-time cyber monitoring now have capabilities in place. Additionally, they informed us that one of the systems was decommissioned, and six were not applicable for onboarding monitoring due to technical constraints or upcoming decommissioning plans. FAA officials stated that they were currently working to implement near real-time cyber monitoring capabilities for the remaining 35 systems.

Improve Privileged User Control, Monitoring, and Visibility—partially implemented. According to the strategy, the agency planned to develop standards and processes to improve identity and access management, multifactor authentication, and privileged accounts.[57] FAA has implemented tools to improve identity and access management, multifactor authentication, and privileged accounts. According to the Fiscal Year 2024 DOT Federal Information Security Modernization Act of 2014 (FISMA) report, FAA achieved more than 99 percent compliance with mandatory multifactor authentication usage.[58] The FISMA report further states that FAA was able to accomplish this increased compliance as a result of DOT's efforts to prioritize improvements in phishing-resistant multifactor authentication across the department's networks and systems.

Regarding privileged accounts, FAA officials stated that a third-party service manages the agency's privileged access process, which includes provisioning of privileged and non-personal entity accounts. Nevertheless, the fiscal year 2024 independent audit of DOT's information security

[57]Identity and access management includes implementing controls that are intended to limit or detect inappropriate access to computer resources to protect them from unauthorized modification, loss, and disclosure. Multifactor authentication requires more than one distinct authentication factor (e.g., password, PIN, token, or biometric) to successfully authenticate a user. Privileged user accounts are a system account for users authorized to perform security-relevant functions that ordinary users are not authorized to perform.

[58]FISMA requires agencies to report annually to the heads of OMB and DHS, certain congressional committees, and GAO on the adequacy and effectiveness of their information security policies and procedures. OMB and DHS work with interagency partners to develop the Chief Information Officer FISMA metrics, which are intended to be used by the agencies, OMB, and DHS to track agencies' progress in implementing cybersecurity capabilities.

program and practices found that FAA had not enabled audit logging of privileged user activities for three systems.[59] Specifically, the agency had not conducted periodic reviews of privileged user accounts on one of these systems and had not conducted a privileged account recertification for two of the systems. Further, according to the audit report, FAA could not provide evidence demonstrating that it reviewed and monitored logs captured for privileged user account activities on two systems. In March 2026, FAA provided a risk acceptance memo stating that the related controls were low risk, the systems could not be configured to implement the controls, and there were compensating controls in place. The memo, dated March 2025, notes that the risk acceptance is applicable for one year and will be reviewed annually by ATO and the Authorizing Official. However, FAA did not provide documentation showing that it had reviewed the risk acceptance within the one-year requirement.

Improve Capabilities for Detection and Mitigation of Internal and External Threats—fully implemented. The FAA Cybersecurity Strategy states that the agency planned to continue to improve its ability to identify cybersecurity vulnerabilities and risks by using Cybersecurity Test Facility (CyTF) and Secure Enterprise Cyber Test Range (SECTR) capabilities. These capabilities are intended to facilitate the assessment and testing of new systems and services, including technologies developed by other federal partners. According to the strategy, CyTF and SECTR are also to be used to support cybersecurity exercises and evaluations at both unclassified and classified levels.

FAA has used CyTF to conduct cyber exercises intended to evaluate incident response plans and new cyber tools to improve the security of the NAS, and to conduct research with government agencies.[60] In May 2024, FAA facilitated a tabletop exercise intended to (1) assess the operational resilience of the agency's mission essential function in the event of a cybersecurity incident that compromised multiple NAS systems; (2) identify agency-level coordination requirements and considerations; and (3) analyze the effectiveness of the agency's cyber incident response crisis coordination. The exercise resulted in

[59]Department of Transportation Office of the Inspector General, *Quality Control Review of the Independent Auditor's Report on the Assessment of DOT's Information Security Program and Practices*, Report QC2024042, (Washington, D.C.: Sept. 30, 2024).

[60]According to security authorization documentation for CyTF, it serves as an independent research and development environment to facilitate cybersecurity testing and evaluation activities across the agency's operating environments. The test facility operates out of the William J. Hughes Technical Center and consists of replicas of selected FAA systems.

observations and associated recommendations that informed the development of a Cyber Resiliency High-Fidelity test that was performed in September 2024.

The Cyber Resiliency High Fidelity Test that FAA conducted in September 2024 was intended to validate the operational resilience of FAA in the event of a cybersecurity incident that compromised multiple NAS systems and services and to identify the minimal operational capabilities and configurations needed to operate the NAS safely. As with the May 2024 tabletop exercise, the test resulted in findings and associated recommendations. In December 2024, FAA released an after-action report that provided a summary of the test and identified key findings and recommendations, based on the test data analyzed. According to FAA officials, starting in fiscal year 2025, the agency would conduct research activities to promote the safety of aircraft operations as it relates to cyber threat detection and protection, and response and recovery.

Further, as of September 2024, FAA had used CyTF to conduct penetration testing on 21 high value asset systems that support the agency's mission critical operations. According to FAA officials, the agency used SECTR to conduct classified research and analysis activities with other government agencies. Additionally, FAA officials informed us that it has not performed classified work with any industry aviation partners but stated that it is an option if the partners have the appropriate security clearance.

Leverage Cybersecurity Research and Development Across FAA Operating Environments and Systems—fully implemented. According to the strategy, FAA planned to work collaboratively with appropriate partners to understand the potential positive and negative impacts that new technologies have on cybersecurity. FAA's Research and Development Plan for 2020 through 2025 described projects related to developing tools and methods to enhance FAA and industry's ability to prevent, detect, and respond to cyberattacks. For example, the plan describes aircraft systems information security protection research that consists of FAA working with stakeholders to address potential safety vulnerabilities and risks that could affect the continued operational airworthiness of aircraft. This research resulted in FAA developing the *Aircraft Systems Information Security/Protection Safety Risk Assessment Methodology* that focused on identifying and assessing cyber safety risks, identifying controls that can address weaknesses in the system, evaluating those controls, and recommending mitigations for the risks.

In addition to the research above, FAA's Research and Development Plan for 2020-2025 describes a project related to NextGen information security that is conducted through FAA's Cybersecurity Data Science (CSDS) research program.[61] This project is intended to prevent and predictively determine the potential for cyber events, such as denial of service and unauthorized access, destruction, disclosure, or modification of information or data. The NextGen information security project included research on how artificial intelligence and machine learning could be leveraged throughout the aviation ecosystem. It also included research that can be used by aviation standards bodies, such as the Aeronautical Radio, Incorporated and Radio Technical Commission for Aeronautics, to inform the development of industry standards. FAA developed the CSDS *Aviation Architecture Framework* to describe how artificial intelligence and machine learning could be leveraged by industry partners to address key aviation cybersecurity challenges.

Ensure FAA Information Security Controls, Policies, and Processes are Aligned with Current NIST Standards and Guidelines—partially implemented. According to the strategy, the agency planned to improve its implementation of NIST standards and guidelines, including the adoption of the latest versions of these standards and guidelines, across the agency. FAA's Security Authorization Handbook documents the agency's process for aligning its security authorization process with the NIST Risk Management Framework.[62] The handbook requires FAA to perform an initial security assessment on all systems before they are placed into operation. After initial operation, systems must undergo an annual assessment and be reauthorized every three years. The annual assessments are to be a partial assessment, and the reauthorization is to be a complete assessment.

However, FAA has not consistently implemented its Security Authorization Handbook for the eight systems we selected for review. Specifically, one of the eight systems—a moderate-impact, mission

[61]NextGen is an FAA initiative that is intended to transition the nation's current ground-based radar air-traffic control system to a system based on satellite navigation, automated position reporting, and digital communications.

[62]National Institute of Standards and Technology, *Risk Management Framework*.

essential system—had a current security authorization assessment.[63] Of the other seven systems:

- Two of the systems—one moderate-impact, non-mission critical system and one unsustainable, mission essential system—had not undergone an initial authorization, even though these systems are in operation.[64]
- Four systems had not undergone an annual assessment. Of these systems, one is a high-impact, mission essential system; two are high-impact, mission critical systems; and the remaining system is an unsustainable, non-mission critical system.[65]
- One system—a moderate-impact, mission critical system—had not undergone an annual assessment or been reauthorized after the three-year authorization period since at least fiscal year 2022.

Develop and Implement Zero Trust Architecture Capabilities—partially implemented. The FAA strategy states that the agency plans to implement a zero trust architecture to strengthen the agency's resiliency and security posture. In doing so, FAA will require all users, devices, and applications—whether in or outside the organization's network—to be authenticated, authorized, and continuously validated before being granted or sustaining access to applications and data.

As previously mentioned, FAA developed a Zero Trust Implementation Plan to guide the development of zero trust architecture capabilities. The FAA Cybersecurity Strategy describes issues that the agency must overcome to comply with federal zero trust architecture guidance. Those issues are related to executive sponsorship and funding; integration of security capabilities; modifications to legacy applications, infrastructure, systems, and protocols; and a multi-year budget line to support a phased

[63]Systems with a moderate-impact security categorization would have a serious adverse impact if compromised.

[64]Systems with a high-impact security categorization would have a severe or catastrophic adverse impact if compromised. Mission critical systems are vital to the operation of air travel, such as automation, communications, navigation, surveillance, and weather. Mission essential systems are vital to the operation of services indirectly supporting the safety and efficiency of air traffic operations, such as grant applications, airman and aircraft certification and regulatory services, and airport services. The selected unsustainable system had significant shortages in spare systems, shortfalls in sustainment funding, and little or no technology funding.

[65]The selected unsustainable system had significant shortfalls in sustainment funding or capability.

approach to implementing a zero trust architecture. FAA informed us that its Cybersecurity Steering Committee has been closely monitoring FAA's enterprise zero trust architecture efforts.

However, the summaries of the committee's 15 meetings held between February and October 2024 and January and July 2025 did not consistently include agenda items or discussions related to the agency's zero trust architecture efforts. In the summaries for the meetings held in 2025, one FAA entity mentioned that they were looking for funding for the zero trust initiative, framework, and pilot program. Additionally, during two other meetings, the attendees discussed the status of zero trust deployments and, during one other meeting, presented on zero trust activities and accomplishments at one FAA entity. Further, FAA has not updated its Zero Trust Implementation Plan since August 2023. The plan notes that the agency will perform a comprehensive update and refresh of the entire document, to include updated planned implementation activities. In January 2026, FAA officials informed us that they were working to update the Zero Trust Implementation Plan by the end of fiscal year 2026.

FAA had not fully implemented its Cybersecurity Strategy, in part, because the agency lacked a comprehensive process to monitor and track its implementation of the strategy. The NIST Cybersecurity Framework states that cybersecurity risk management outcomes should be reviewed to inform and adjust strategic direction, and that performance should be evaluated and updated as necessary.[66] Although FAA has reported on challenges it has faced in implementing its Cybersecurity Strategy, the agency did not have a comprehensive process to monitor implementation of the strategy. Specifically, in the report required by Section 1029 of the FAA Reauthorization Act of 2024, the agency noted the following challenges:[67]

- **Resource Allocation.** Planning for specific cyber risks or requirements within the federal budget cycle.

[66]National Institute of Standards and Technology, *The NIST Cybersecurity Framework*.

[67]Section 1029 of the FAA Reauthorization Act requires the agency to report on the status of its implementation of the FAA Cybersecurity Strategy, to include, at a minimum, (1) a description of the progress in developing, implementing, and updating the strategy; (2) an overview of completed and planned research and development projects and a description of planned research and development activities that have been prioritized for the most needed improvements to safeguard the NAS; and (3) an explanation for any delays or challenges in implementing the strategy.

- **IT workforce.** Filling and retaining specialized cybersecurity positions.
- **Infrastructure modernization.** Supporting and securing aging technology.
- **Agency-specific challenges.** Minimizing risks to operational technology and assuring mission execution.

Nonetheless, FAA lacked a comprehensive performance monitoring process to track its implementation of the strategy. According to the strategy, each line of business, or FAA entity, is to have a business plan that aligns with the objectives described within it. AIS was the one entity able to provide a business plan. The business plan included AIS cybersecurity initiatives that tracked back to the strategy's objectives and listed target milestone dates for completing them. While FAA provided documentation of its efforts to monitor AIS' progress towards targeted milestone dates, the agency did not provide the business plans for the other entities involved in implementing goal 2 of the Cybersecurity Strategy, such as ASH, ATO, and ANG. Additionally, FAA did not provide documentation of its efforts to monitor implementation of the other goals described in the strategy.

Further, the summaries of the Cybersecurity Steering Committee meetings discussed cybersecurity initiatives, such as security compliance and vulnerability management, and upcoming projects—they did not indicate any monitoring of the strategy's implementation. During one meeting in April 2025, the committee discussed developing an implementation plan to show progress on meeting the strategy's goals; however, the summary for the June 2025 meeting included a discussion on revising those plans to focus on a comprehensive rewrite of the Cybersecurity Strategy due to resource constraints. FAA informed us that it does not have any processes in place to monitor or track its implementation of its strategy. As discussed earlier in March 2026, FAA finalized an update to its Cybersecurity Strategy that outlines strategic objectives and associated key initiatives. The updated strategy describes the agency's plans to assess implementation and evaluate progress towards its cybersecurity goals. To do this, FAA 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.

While FAA has developed plans to evaluate its implementation of the updated Cybersecurity Strategy, as previously mentioned, the agency did not consistently use business plans to monitor implementation of the

previous strategy. Even though the previous strategy states that each FAA entity was to develop a business plan that aligned with the objectives described within it, the agency did not provide business plans that monitored implementation across all the FAA entities involved in carrying out the goals and objectives of the previous strategy. 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.

Conclusions

Aircraft depend on avionics and ground systems to get from one place to the next safely. The growing interconnectivity of these aviation systems to support flight operations has increased their exposure to cyber-based threats. As a result, cybersecurity remains a fundamental consideration for FAA and TSA leadership in the aviation subsector.

FAA has taken steps to define its roles and responsibilities for aviation cybersecurity, to include overseeing avionics and managing ground systems in the NAS. However, TSA's Cybersecurity Roadmap does not describe the agency's cybersecurity-related roles and responsibilities for overseeing airport and aircraft operator security programs or identify the TSA entities responsible for implementing the goals and objectives it outlines. Without clearly defined roles and responsibilities, TSA may be challenged in holding relevant entities accountable or enable continuous improvements to its related efforts.

As part of FAA's annual reporting of its cyber spending to OMB, FAA did not report spending data for its Information Security/Cybersecurity Program that supports its research and development activities. This is because FAA's Cyber Budget Data Request process does not include all cybersecurity spending from program offices. 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.

Further, FAA's current and proposed aircraft certification and system security authorization processes meet key federal and industry practices to mitigate cybersecurity vulnerabilities and risks to avionics and ground systems. However, FAA's plan for transitioning its operating environments

to a zero trust architecture, did not include details of the planned transition for its Research and Development operating environment. Additionally, the plan fully aligned with three of the seven NIST practices for migrating to zero trust architecture. Without fully aligning its zero trust implementation plan with NIST's best practices across all operating environments, FAA cannot ensure that it is effectively managing cybersecurity risks, including during NAS modernization.

Lastly, FAA had not fully implemented the objectives supporting its Cybersecurity Strategy's goal to protect and defend its networks and systems. This is because the agency lacked a process to monitor and evaluate the implementation of any of the goals or objectives in the FAA Cybersecurity Strategy at the time. In March 2026, FAA updated its Cybersecurity Strategy, which now describes the agency's intention to 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 is better able to ensure its plans to mitigate cybersecurity risks are effective, identify challenges, make adjustments, and prioritize resources to address identified risks to its missions and service delivery.

Recommendations for Executive Action

We are making a total of five recommendations, including one to TSA and four to FAA. Specifically:

The Administrator of TSA should update the TSA Cybersecurity Roadmap to define the roles and responsibilities for the TSA entities responsible for carrying out the goals and objectives described within it, including for the aviation subsector, and align the roadmap with the DHS Cybersecurity Strategy. The TSA Administrator should communicate its Cybersecurity Roadmap to appropriate non-federal stakeholders (recommendation 1).

The Administrator of FAA should update the agency's cyber budget data request process to ensure that it includes all cybersecurity spending from program offices. (recommendation 2)

The Administrator of FAA should ensure that the agency's updated Zero Trust Implementation Plan includes detailed steps for transitioning all operating environments to a zero trust architecture. (recommendation 3)

The Administrator of FAA should ensure that the agency's updated Zero Trust Implementation Plan fully aligns with NIST best practices for migrating to a zero trust architecture. (recommendation 4)

The Administrator of FAA should direct the agency's Cybersecurity Steering Committee to take steps, as the agency implements its revised Cybersecurity Strategy, to ensure it carries out monitoring as planned and incorporates lessons learned from its past experiences. (recommendation 5)

Agency Comments

We provided a draft of this report to DHS and DOT for review and comment. We received written comments from DHS and DOT—reprinted in appendix IV and V. DHS agreed with our recommendation to TSA, and DOT agreed with our recommendations to FAA. DHS stated that the recommendation to TSA will be implemented after the department's effort to align its Cybersecurity Strategy with the President's Cyber Strategy for America. DHS also discussed how the updated TSA Cybersecurity Roadmap will address our recommendation, and its plan to communicate with non-federal stakeholders during development of the updated roadmap. Both DHS and DOT provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Administrators of the Federal Aviation Administrator and Transportation Security Administration, Director of the Cybersecurity and Infrastructure Security Agency, these agencies' inspectors general, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at FranksJ@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix VI.

//SIGNED//

Jennifer R. Franks
Director, Center for Enhanced Cybersecurity
Information Technology and Cybersecurity

List of Committees

The Honorable Ted Cruz
Chairman
The Honorable Maria Cantwell
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Rand Paul, M.D.
Chairman
The Honorable Gary C. Peters
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Sam Graves
Chairman
The Honorable Rick Larsen
Ranking Member
Committee on Transportation and Infrastructure
House of Representatives

The Honorable Andrew Garbarino
Chairman
The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Troy E. Nehls
Chairman
The Honorable Steve Cohen
Ranking Member
Committee on Transportation and Infrastructure
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our specific objectives were to determine (1) the extent to which the Federal Aviation Administration (FAA) and the Transportation Security Administration (TSA) defined their current roles and responsibilities for aviation cybersecurity, and collaborated to manage them; (2) the budget requests for the FAA entities responsible for implementing its Cybersecurity Strategy and to what extent are they meeting relevant Office of Management and Budget (OMB) reporting requirements; (3) the extent to which the FAA 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 has implemented its Cybersecurity Strategy to mitigate cybersecurity risks to its systems and networks.

To address our first objective, we compared FAA and TSA's roles and responsibilities for aviation cybersecurity, as defined in relevant strategies, to identify any duplication, overlap, or fragmentation.[1] This included identifying and comparing the offices within FAA and TSA that have responsibilities in aviation cybersecurity. Further, we compared the agencies' strategies against the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 guidance on roles, responsibilities, and authorities.[2] We also interviewed or collected written responses from aviation stakeholders, such as industry groups, avionics manufacturers, and airlines, to obtain their perspectives on FAA and TSA roles and responsibilities for aviation cybersecurity.[3]

Additionally, we assessed the group that FAA and TSA used to collaborate on aviation cybersecurity—the Aviation Cybersecurity

[1]GAO, *Fragmentation, Overlap, and Duplication: An Evaluation and Management Guide*, GAO-15-49SP, (Washington, D.C.: Apr. 2015).

[2]National Institute of Standards and Technology, *The NIST Cybersecurity Framework, Version 2.0 (Gaithersburg, MD: February 2024).*

[3]We identified a non-generalizable sample of 18 stakeholders based on our review of prior GAO work, a literature search, and recommendations from stakeholders that were obtained during interviews from the prior GAO Aviation Surveillance Technology engagement. Of those 18 stakeholders, eight responded to our meeting request and three provided written responses to our questions. The remaining seven either did not respond or stated that they were unable to assist us. The responding 11 entities represent industry groups, avionics manufacturers, domestic airlines, and a research organization.

Initiative (ACI)—against leading practices that we previously identified for interagency collaboration.[4] Those leading practices include the following:

- Defining common outcomes
- Ensuring accountability
- Bridging organizational cultures
- Identifying and sustaining leadership
- Clarifying roles and responsibilities
- Including relevant participants
- Leveraging resources and information
- Developing and updating written guidance and agreements

Specific documentation that we compared against these leading practices included the ACI charter and Communications Plan; meeting minutes and presentations; tabletop exercise presentations and after-action reports; and FAA and TSA budget information. We compared this documentation to the leading practices for interagency collaboration to determine the extent to which FAA and TSA collaborative efforts addressed them. We also interviewed the selected aviation stakeholders mentioned above to obtain their perspectives on FAA and TSA's collaborative efforts for aviation cybersecurity.

To address the second objective, we reviewed and described the fiscal year (FY) 2024 through 2026 President's budget requests for relevant FAA entities to describe their requested budgets for that time period. We also summarized the costs associated with cybersecurity activities outlined in the FAA Cybersecurity Strategy. Further, we assessed FAA's Cyber Budget Data Request Process to determine the extent to which it facilitated comprehensive reporting of its cybersecurity activities and costs to OMB.

To address the third objective, we evaluated standards and guidance issued by NIST and aviation industry standards bodies, such as Radio Technical Commission for Aeronautics (RTCA) and American Society for Testing and Materials, to identify key practices for mitigating cybersecurity

[4]GAO, *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges*, GAO-23-105520 (Washington, D.C.: Mar. 2023).

risks and vulnerabilities to avionics and ground systems.[5] Specifically, we compiled and synthesized the processes outlined in the standards and guidance mentioned above to identify common themes. Our assessment resulted in the following key practices for mitigating cybersecurity risks and vulnerabilities to those systems:

- Define the characteristics of the system, to include its intended purpose.
- Determine the appropriate level of security for the system based on identified risks and threats.
- Identify security measures to achieve the appropriate level of security.
- Implement the security measures.
- Assess the effectiveness of the implemented security measures.
- Document the security activities and make a determination about authorizing/certifying the system to operate, to include accepting any remaining risks.
- Monitor the effectiveness of the security measures and re-assess security impacts as modifications are made to the system.[6]

We analyzed and compared FAA's Cybersecurity Strategy, as of February 2026, and associated documentation against the key practices we identified to determine the extent to which the strategy addressed them.[7] The documentation we analyzed included new and existing code of federal regulations and associated requirements regarding the approval process for aircraft with special conditions related to intentional unauthorized electronic interaction and network security programs; FAA's

[5]For purposes of our review, we considered ground systems as those that are external to an aircraft but provide information and data necessary for its safe flight. These systems are operated and managed by FAA.

[6]The specific guidance and standards that we used to identify the key risk mitigation practices are as follows. National Institute of Standards and Technology, *Risk Management Framework 800-37*, Revision 2 (December 2018); American Society for Testing and Materials, *Standard Practice for Protection of Aircraft Systems from Intentional Unauthorized Electronic Interactions* (Feb. 1, 2022); and Radio Technical Commission for Aeronautics, *Standards on Airworthiness Security Process Specification* (Washington D.C.: August 6, 2014).

[7]In March 2026, FAA finalized an update to its Cybersecurity Strategy that outlines strategic objectives and associated key initiatives. According to the updated strategy, FAA will develop a centralized implementation plan to guide the agency's achievement of the strategic objectives outlined within it. Our review primarily focused on the strategy as of February 2026 given the timing of our review and FAA's update.

Monitor Safety Analyze Data process; and the agency's Information Security and Privacy Policy, Security Authorization Handbook, Air Traffic Organization Information Security Continuous Monitoring Plan, and Zero Trust Implementation Plan.[8]

To address the fourth objective, we analyzed the FAA Cybersecurity Strategy, as of February 2026, to identify and describe the agency's goal and supporting objectives to mitigate cybersecurity risks to its systems and networks. We then assessed agency policies, procedures, plans, and exercise, and testing documentation to determine the extent to which FAA had fully implemented its goal. As part of this assessment, we analyzed security authorization documentation, such as system security plans, security assessment reports, plans of action and milestones, and executive summaries, for eight selected systems. Using this documentation, we determined the extent to which FAA was consistently implementing its Security Authorization Handbook, which is intended to align the agency with NIST standards and guidance—an objective supporting the agency's goal to mitigate cybersecurity risks to its systems and networks.

To select the eight systems for our review, we used FAA's inventory of mission critical systems that were categorized as high- and moderate-impact.[9] For these systems operating in the mission support and national airspace system domains, we randomly selected one high-impact and one moderate-impact system using a computerized random function. Since the research and development domain did not have any mission critical systems, we judgmentally selected the one system categorized as high-impact and randomly selected a moderate-impact system using a computerized random function. Further, we used FAA's inventory of unsustainable systems to select one mission essential system with

[8]Intentional unauthorized electronic interaction is defined as a circumstance or event with the potential to affect the aircraft due to human action resulting from unauthorized access, use, disclosure, denial, disruption, modification, or destruction of information and/or aircraft system interfaces. This includes malware and the effects of external systems, but does not include physical attacks, such as electromagnetic jamming.

[9]Mission critical systems are vital to the operation of air travel, such as automation, communications, navigation, surveillance, and weather. Systems with a high-impact security categorization would have a severe or catastrophic adverse impact if compromised. Systems with a moderate-impact security categorization would have a serious adverse impact if compromised.

sustainability rating A and one with sustainability rating B.[10] We also randomly selected these systems using a computerized random function. The eight systems that we selected for review were the following:

1. Safety Assurance System
2. Enterprise Service Center Middle-Tier and Enterprise Support Applications
3. Central Altitude Reservation Function
4. Aeronautical Communications System
5. Cybersecurity Test Facility
6. NextGen Office (ANG)-A Business Applications
7. Juneau Airport Wind System
8. Enterprise Information Display System

We supplemented our analysis for each objective with interviews of relevant FAA officials in the offices of Financial Management, NextGen, and Aviation Safety. We also interviewed TSA officials in the offices of Security Operations, Policy Plans, and Engagement, and Strategy, Policy, Coordination, and Innovation. These interviews assisted in corroborating evidence and providing additional context to the actions taken by FAA and TSA to carry out its roles, responsibilities, strategies, policies, procedures, and plans regarding aviation cybersecurity.

We conducted this performance audit from August 2024 to July 2026 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.

[10]Mission essential systems are vital to the operation of services indirectly supporting the safety and efficiency of air traffic operations, such as grant applications, airman and aircraft certification and regulatory services, and airport services. Sustainability rating of A means that the system has significant shortages in spare systems, shortfalls in sustainment funding, and little or no technology funding. Sustainability rating B means that the system has significant shortfalls in sustainment funding or capability.

Appendix II: Evaluation of FAA and TSA Collaborative Efforts for the Aviation Cyber Initiative

We assessed the Federal Aviation Administration's (FAA) and Transportation Security Administration's (TSA) collaborative efforts performed through the Aviation Cyber Initiative (ACI) against the eight leading practices for interagency collaboration that we identified in prior GAO work.[1] ACI is a task force led by three chairs designated from the Department of Transportation (DOT), Homeland Security (DHS), and Defense.[2] DOT and DHS assigned a chair from FAA and TSA to represent those departments' interests and missions. We determined that FAA and TSA, in collaborating through ACI, addressed all of the leading practices for interagency collaboration, as shown in table 4.

[1]GAO, *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges*, GAO-23-105520 (Washington, D.C.: May 24, 2023).

[2]While the Department of Defense is an active member of ACI, Section 396 of the FAA Reauthorization Act of 2024 includes a provision for us to review how TSA and FAA differentiate and manage their roles and responsibilities for the cybersecurity of aircraft and ground systems.

Table 4: Assessment of Federal Aviation Administration (FAA) and Transportation Security Administration's (TSA) Collaborative Efforts through Aviation Cyber Initiative (ACI) Against GAO's Leading Practices for Interagency Collaboration

Leading practice	GAO assessment	Summary
Define common outcomes	●	ACI leadership defined common outcomes for the group in a charter, which states that ACI was established to provide a forum for coordination and collaboration on activities aimed at cyber risk reduction within the aviation ecosystem. The charter defines ACI's long-term outcome to reduce cybersecurity risks and improve cyber resilience to support safe, secure, and efficient operations of the Nation's aviation ecosystem. The charter also identified how it will achieve the long-term outcome through three strategic objectives: 1. Identify, assess, and analyze cyber threats, vulnerabilities, and consequences within the aviation ecosystem through research, development testing, and evaluation initiatives, 2. Engage with aviation ecosystem stakeholders on activities for reducing cyber risk, and 3. Seek potential improvement opportunities and risk mitigation strategies. ACI's short-term outcomes are carried out through projects and initiatives associated with annual priorities established to achieve the group's long-term outcome. For example, during the January 2024 ACI Executive Committee (ExCom) meeting, participants discussed annual priorities and supporting projects and initiatives related to cyber risk mitigation, tabletop exercises, and risk assessments.
Ensure accountability	●	FAA and TSA have processes to ensure accountability within ACI by monitoring the group's progress towards achieving the short- and long-term outcomes. For example, the Tri-Chairs met weekly between June 2020 and April 2025 to discuss and monitor the status of the projects and initiatives undertaken by ACI. FAA and TSA also recognized the accomplishments of ACI by tracking the completion status of annual priorities and the supporting projects and initiatives during biannual ExCom meetings held in January and August of 2024.
Bridge organizational cultures	●	FAA and TSA addressed differences in their organizational cultures by establishing a process to ensure that communication is unified among its members. Specifically, the ACI Communications Plan outlines the group's strategy to achieve unity of messaging and describes how information is to be disseminated to ACI membership and stakeholders to ensure appropriate protections are established. For example, the Communications Plan requires that ACI members use the August 2014 Department of Homeland Security (DHS) Security Classification Guide to protect classified national security information.[a] As an example of how this guide has been used in ACI products, the after-action reports for tabletop exercises were designated as sensitive and were shared with the participating organizations on a need-to-know basis. Additionally, the ACI charter states that the group's programs and projects should be carried out in accordance with each department's policies, procedures, and authorities.

Identify and sustain leadership	●	The ACI charter identifies the following two leadership groups: • ExCom consists of senior-level officials from the Departments of Transportation, Homeland Security, and Defense (DOD) to guide and support ACI objectives and ensure that outreach efforts, authorities, policies, and missions for each respective department are maintained and followed. The Deputy Administrators at FAA and TSA served in this leadership role. • Tri-Chair representatives consist of delegates, typically subject matter experts, from FAA, TSA, and the lead DOD component to represent the interests and mission of their respective departments. These Tri-Chair representatives report to ExCom to ensure the authorities, policies and missions of each department are maintained. For ExCom, the FAA Chief Information Officer and TSA Deputy Executive Assistant Administrator for Security Operations were delegated to represent the agencies' Deputy Administrators during their absence. The FAA and TSA Tri-Chair representatives had consistent participation in the group's meetings and activities held between 2020 and 2025.
Clarify roles and responsibilities	●	ACI leadership identified and defined the roles and responsibilities of ACI members in the group's charter. For example, the charter describes ExCom as the main leadership body to provide support to the Tri-Chairs regarding ACI activities. In doing so, ExCom meets biannually—the first time to determine priorities and grant approval for projects and the second time to discuss the group's progress in carrying out those priorities and projects. Similarly, the Tri-Chairs are to represent their department's mission and interests in implementing the priorities determined by ExCom. In doing so, Tri-Chair representatives were present during ExCom meetings to provide their input on the projects and initiatives supporting the proposed annual priorities. For example, during the January 2024 ExCom meeting, FAA's Tri-Chair led a discussion on an ongoing initiative to educate airports on how global-positioning systems are used and operated, and the related potential threats, such as spoofing and jamming. Further, the charter describes the role of the Executive Secretariat who is to handle administrative tasks for the group. Specifically, the Executive Secretariat is responsible for sharing meeting minutes, agendas, and invites, and documenting ACI's efforts, among other things.
Include relevant participants	●	The charter states that ACI may invite other federal departments and agencies to contribute to the work of the collaborative group and meet specific objectives. According to the ACI Communications Plan, the initiative collaborates with a diverse group of aviation stakeholders, including industry and commercial organizations, federal departments and agencies, affiliated entities, and State, Local, Territorial and Tribal governments.[b] Six of the eleven aviation stakeholders we interviewed—five industry groups and one avionics manufacturer—stated that they participated in ACI. Four stakeholders—two airlines, one industry group, and one research organization—stated that they do not actively participate in ACI. One of these airlines informed us that they received information from ACI, although they are not an active participant. The remaining stakeholder—an avionics manufacturer—provided written responses and did not mention any involvement in ACI.
Leverage resources and information	●	FAA and TSA leveraged their agency resources to support ACI and defined information sharing mechanisms in its Communications Plan. The work undertaken by ACI is dependent on staffing and funding allocated by each participating department. According to FAA officials, they provided several employees to support ACI activities, with one staff member serving as the ACI Executive Secretariat. In fiscal year 2024, FAA allocated $1.6 million to support ACI and officials informed us that they allocated $1.2 million in fiscal year 2025. TSA officials informed us that they provided two employees and allocated $1.75 million to support ACI activities. Regarding information sharing among members, the ACI Communications Plan describes a standard process for doing so. Additionally, based on ACI's meeting minutes and agendas, the group uses several mechanisms to share information, such as virtual meetings, panel discussions, and conferences. Further, one of ACI's projects involved establishing an information sharing portal that the group's members would use to collaborate.

Develop and update written guidance and agreements	●	ACI leadership documented how the group is to collaborate in the charter, which was fully signed by the departments' Secretaries by May 2019. The charter describes ACI's purpose, identifies key members, and defines the meeting interval for the group. FAA officials stated that they plan to review the charter to ensure that it is aligned with the new administration's orders and legislation. TSA officials stated that the Tri-Chairs have discussed an initiative to update the charter in 2026. Further, the Communications Plan defines ACI's governance structure regarding how information, recommendations, and guidance are conveyed through ACI. Senior officials serving in ExCom signed the plan to show agreement with all associated processes.

● = fully addressed ◐ = partially addressed ○ = not addressed

Source: GAO analysis. | GAO-26-107693

[a]The August 2014 DHS Security Classification Guide governs the handling and distribution of data and information regarding identified vulnerabilities and exploits.

[b]Some of the aviation organizations participating in ACI includes Airlines for America, Airports Council International-North America, Aerospace Industries Association, Airline Pilots Association, General Aviation Manufacturers Association, Garmin, and MITRE.

Appendix III: Assessment of FAA's Cybersecurity Strategy and Associated Processes Against Key Mitigation Practices

We assessed the Federal Aviation Administration's (FAA) Cybersecurity Strategy and associated processes against key practices that we identified for mitigating cyber risk and vulnerabilities to avionics and the ground systems operating in the national airspace system (NAS).[1] Those key practices are to:

- Define the characteristics of the system, to include its intended purpose
- Determine the appropriate level of security for the system based on identified risks and threats
- Identify security measures to achieve the appropriate level of security
- Implement the security measures and assess their effectiveness
- Document the security activities and determine whether to authorize or certify the system to operate, to include accepting any risk
- Monitor the effectiveness of the security measures and re-assess security impacts as modifications are made to the system

Further, the National Institute of Standards and Technology (NIST) outlines best practices for organizations migrating to a zero trust architecture.[2]

We determined that FAA's current process for certifying aircraft with special conditions and August 2024 new proposed rule for imposing new design standards to address cybersecurity threats for transport category airplanes, engines, and propellers (if finalized in its current state) aligns with the key practices we identified.[3] Additionally, we determined that FAA's Security Authorization Handbook and Air Traffic Organization

[1]In March 2026, FAA finalized an update to its Cybersecurity Strategy. The updated strategy outlines strategic objectives and associated key initiatives. While some of the strategic objectives and key initiatives are similar to the goals and objectives of the previous Cybersecurity Strategy that was the focus of our review, some of them differ.

[2]National Institute of Standards and Technology, *Zero Trust Architecture*, Special Publication 800-207, (Gaithersburg, MD: August 2020). Zero trust architecture is an enterprise's cybersecurity plan that uses zero trust concepts and encompasses component relationships, workflow planning, and access policies. Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.

[3]Special conditions apply to a specific aircraft design when existing regulations do not adequately address a novel or unusual design feature, such as onboard computer networks or avionics.

Information Security Continuous Monitoring Plan aligned with the practices. However, FAA's Zero Trust Implementation Plan did not align with NIST's best practices for migrating to a zero trust architecture. Tables 5, 6, and 7 summarize our assessment.

Table 5: Assessment of the Federal Aviation Administration's (FAA) Current and Proposed Approach for Certifying Aircraft with Information Security Protections Against Key Cybersecurity Risk and Vulnerability Mitigation Practices

Key risk mitigation practices for avionics and ground systems	GAO's assessment	FAA's current special condition[a] process and proposed approach for certifying aircraft with information security protections[b]
Define the characteristics of the system, to include its intended purpose	•	During the certification process for aircraft with special conditions, the applicant provides design data, interfaces, risk assessments, and other documentation needed to show compliance with the special condition and certification basis.[c]
Determine the appropriate level of security for the system based on identified risks and threats	•	FAA's current process for certifying aircraft with special conditions related to the cybersecurity of an aircraft requires the certification applicant to develop and provide FAA with a risk assessment for the special condition. FAA engineers are to review the aircraft's architecture and determine how the risks identified in the risk assessment should be addressed. The agency's proposed rule, if finalized in its current state, would require certification applicants to perform a cybersecurity risk analysis for intentional unauthorized electronic interactions to:[d] • identify all threat conditions associated with the system, architecture, and external or internal interfaces, • assess the severity of the impact of those threat conditions on associated assets (system, architecture, etc.), and • analyze related vulnerabilities for the likelihood of exploitation.
Identify security measures to achieve the appropriate level of security	•	As a part of FAA's current special condition process, the applicant proposes a means of compliance for FAA's review.[e] The means of compliance defines the steps necessary to meet the special condition and address any associated potential risks. The proposed rule, if finalized in its current state, would require applicants to adequately mitigate the cybersecurity risks for safety, functionality, and continued airworthiness by showing that the design: • protects against unauthorized access from inside or outside of the aircraft, and • prevents malicious changes to, and adverse impacts on, the aircraft, equipment, systems, and networks required for safe operation.
Implement the security measures and assess the effectiveness of the implemented security measures	•	In FAA's existing special condition process, once the applicant has met all applicable certification requirements, including compliance with special conditions, they are to assemble a prototype aircraft with all systems in place. Then final testing is performed, which may include networking and cybersecurity controls needed to ensure that mitigations are in place and functioning properly. According to the proposed rule, if finalized in its current state, each applicant would be required to identify and assess the security risks posed by intentional unauthorized electronic interactions and mitigate the vulnerabilities identified in the cybersecurity risk analysis through the practice above through installation and assessment of single or multilayered protection mechanisms or process controls.

Document the security activities and make a determination about authorizing/certifying the system to operate, to include accepting any remaining risks		During FAA's current special condition process, the agency reviews testing results and the certification package to determine whether to approve certification of the aircraft. If the approved aircraft has special conditions that require operator action to mitigate electronic security risks, FAA's existing process requires that the design approval holder develop a network security guidance document.[f] This document contains instructions for continued airworthiness of the aircraft and informs the aircraft network security program.[g]
	●	The proposed rule would require applicants to document their procedures for maintaining the protections against intentional unauthorized electronic interactions in their instructions for continued airworthiness. Additionally, any maintenance-related procedures for security protections that extend beyond what is typically included in the instructions for continued airworthiness are to be documented in the aircraft network security program. FAA will make a determination as to whether the applicant sufficiently identified and mitigated the cybersecurity risks and include that in its decision to certify the aircraft.
Monitor the effectiveness of the security measures and re-assess security impacts as modifications are made to the system		In general, as part of FAA's existing special condition process, operators are required to conduct surveillance of their aircraft network security program to verify compliance and identify threats to the overall system. Documentation of surveillance should be included in the operator's continuing analysis and surveillance system program for technical issues, and in the annual security assessment for threat information. In addition, FAA monitors the aircraft network security program as part of its oversight of fleet safety.
	●	Further, FAA's Monitor Safety-Analyze Data process outlines how the agency is to monitor identified safety issues, including those posed by intentional unauthorized electronic interactions, and manage risk in aviation products throughout their lifecycle. This process involves the analysis of reported safety issues, identification and implementation of corrective actions, and validation of risk mitigation effects. FAA received three reports of cyber-related safety issues that were reported through this process. According to FAA officials, none of them were determined to be related to intentional unauthorized electronic interaction.

● = fully addressed ◐ = partially addressed ○ = not addressed

Source: GAO analysis. | GAO-26-107693

[a]Special conditions apply to a specific aircraft design, such as onboard computer networks or avionics.

[b]In August 2024, FAA proposed a new rule that introduces certification and continued airworthiness requirements for protecting the equipment, systems, and networks of transport category airplanes, engines, and propellers from intentional unauthorized electronic interactions that could create safety hazards.

[c]A certification basis identifies the applicable standards and amendment levels that the applicant must show compliance with. For example, a type certification is the approval of the design of the aircraft and all its components and signifies that the aircraft design is in compliance with all applicable standards.

[d]Intentional unauthorized electronic interaction is defined as a circumstance or event with the potential to affect the aircraft due to human action resulting from unauthorized access, use, disclosure, denial, disruption, modification, or destruction of information and/or aircraft system interfaces. This includes malware and the effects of external systems, but does not include physical attacks, such as electromagnetic jamming.

[e]FAA deems aircraft cybersecurity standards that have been issued by aviation standards development organizations, such as Radio Technical Commission for Aeronautics and American Society for Testing and Materials, as accepted means of compliance for applicable special conditions.

[f]The design approval holder is an entity, such as a manufacturer, that has FAA authorization for an aircraft product's design.

[g]The aircraft network security program includes instructions on maintenance of the aircraft's internal networks and external connections, forensic analysis process to address safety-related cybersecurity incidents, and requirements for incident reporting.

Table 6: Assessment of the Federal Aviation Administration's (FAA) Security Authorization Process for Systems it Operates in the National Airspace System (NAS) Against Key Cybersecurity Risk and Vulnerability Mitigation Practices

Key risk mitigation practices for avionics and ground systems	GAO assessment	FAA security authorization processes
Define the characteristics of the system, to include its intended purpose	●	The FAA Security Authorization Handbook requires system owners to document information about the system undergoing review for authorization to operate.[a] Specific information that should be documented includes a functional description of the system, the system architecture, security categorization, and future changes.
Determine the appropriate level of security for the system based on identified risks and threats	●	According to FAA's Security Authorization Handbook, all information systems must have a security categorization that is based on the impact of loss in the system's confidentiality, integrity, or availability. A low security categorization is defined as the system's loss having a limited adverse impact; a moderate categorization would have a serious adverse impact; and high categorization would be catastrophic.
Identify security measures to achieve the appropriate level of security	●	According to the Security Authorization Handbook, each system is required to have a system security plan that provides a listing of the minimum system security controls necessary to protect the system. The security categorization (e.g., low, moderate, high) provides the basis for identifying the initial high, moderate and low baseline set of security controls that should be implemented on a system undergoing authorization.
Implement the security measures and assess the effectiveness of the implemented security measures	●	The Security Authorization Handbook requires that the security controls implemented on a system undergoing authorization are independently assessed. The assessment is intended to verify that the security controls are implemented and working as intended.
Document the security activities and make a determination about authorizing/certifying the system to operate, to include accepting any remaining risks	●	According to the Security Authorization Handbook, FAA National Airspace Systems (NAS) must be granted an authority to operate before it becomes operational. The system security plan, report describing findings from the independent assessment of security controls, and any plans to remediate identified vulnerabilities are briefed to the Authorizing Official who is responsible for authorizing systems to operate. Additionally, a risk assessment that evaluates the likelihood and impact of the remaining vulnerabilities is conducted to assist the Authorizing Official in determining whether or not accept any remaining risks and grant the system an authority to operate.

Monitor the effectiveness of the security measures and re-assess security impacts as modifications are made to the system	●	According to the Security Authorization Handbook, once a NAS system has completed a security assessment and has been authorized for operation, it can undergo ongoing authorization, which implies a continued understanding and acceptance of risk. The Security Authorization Handbook states that FAA systems must repeat the steps above at least every three years and undergo an assessment annually. For NAS systems specifically, FAA's Air Traffic Organization Information Security Continuous Monitoring Plan establishes a continuous monitoring approach for those systems once they have completed initial authorization.[b] According to the plan, NAS systems are placed into tiers that define the monitoring and assessment approaches that are suited to the systems.

● = fully addressed ◐ = partially addressed ○ = not addressed

Source: GAO analysis. | GAO-26-107693

[a]FAA's Security Authorization Handbook outlines the agency's risk management and security authorization process for all its systems, including those operating in the NAS.

[b]The Air Traffic Organization Information Security Continuous Monitoring Plan aligns with the Security Authorization Handbook and outlines FAA's approach for performing continuous monitoring in support of ongoing authorization decisions for NAS systems.

Table 7: Assessment of the Federal Aviation Administration's (FAA) Zero Trust Implementation Plan Against the National Institute of Standards and Technology (NIST) Best Practices for Migrating to a Zero Trust Architecture

NIST practice	GAO assessment	Federal Aviation Administration Zero Trust Implementation Plan[a]
Identify actors	◐	FAA's Zero Trust Implementation Plan describes near-term (fiscal year 2023-2024) activities for identifying subjects in the Mission Essential operating environment. Specifically, the plan states that near-term activities for the Mission Essential operating environment includes surveying subjects associated with the current state of mission essential National Airspace Systems (NAS) functions. However, the plan does not describe these efforts for the Administrative, Mission Critical, and Research & Development operating environment.
Identify assets	◐	The plan describes near-term activities for identifying assets in the Administrative, Mission Essential and Mission Critical operating environments. For the Administrative operating environment, the plan states that efforts will focus on establishing a comprehensive inventory of assets, among other things. For the Mission Essential and Mission Critical operating environments, the plan states that near-term activities will include surveying assets associated with the current state of their defined NAS functions. However, the plan does not describe these efforts for the Research & Development operating environment.
Identify key process and data flows	◐	FAA's plan describes near-term activities for surveying data flows, business processes, and workflows in the Mission Essential operating environment. It also mentions surveying data flows and business processes in the Mission Critical operating environment. However, the plan does not describe identifying workflows for the Mission Critical environment, or any of these things for the Administrative and Research & Development operating environments.
Formulate policies	●	FAA's Zero Trust Implementation Plan describes near-term activities in the Administrative and Mission Essential operating environments related to orchestration services/policy decision point that will be used to define dynamic policy access to the agency's assets. According to the plan, the Mission Critical operating environment will define solutions to support micro-segmentation and leverage similar orchestration service/policy decision point implementation as the Mission Essential operating environment, where applicable. Further, the plan states that the Research & Development operating environment will install and deploy a combination of the tools and technologies planned for each of the other operating environments.

Identify candidate zero trust solutions	●	The plan describes the current implementation status of existing tools that can be leveraged to support zero trust capabilities and defines the agency's plans for migrating to new solutions to improve those capabilities within the Administrative, Mission Essential, and Mission Critical environment. As mentioned above, the Research & Development operating environment will install and deploy a combination of the tools and technologies planned for each of the other operating environments.
Start initial deployment and monitor	◐	FAA's Zero Trust Implementation Plan describes near-term, and mid-term (fiscal year 2025-2030) activities related to starting initial deployments of solutions in the Administrative, Mission Essential, and Mission Critical operating environments. However, the plan does not describe the agency's efforts to monitor implementation of the policy decision point to ensure that it is working according to defined policies. According to FAA officials, the effectiveness and accuracy of the policy decision point is reviewed on a real-time basis based on alerts from the FAA Security Operations Center and NAS Cyber Operations, as well as by the Life Cycle Management team within 24 to 48 hours of receiving an alert. FAA's Zero Trust Implementation Plan does not describe these efforts.
Expand the zero trust architecture	●	Far-term (FY30 and beyond) activities for FAA's migration to zero trust involve maturing implementation by fully incorporating zero trust strategies and principles and working in collaboration with the other operating environments to define a strategy, plan, and architecture, and to conduct technology pilots to implement and deploy zero trust capabilities agency-wide. The plan states that lessons learned on mission benefits and enterprise integration should be gathered from pilots to inform recommendations and implementation planning. Additionally, the agency will develop communication plans that provide details about stakeholder engagement and communication activities, including for ensuring regular coordination among the operating environments. According to the plan, this coordination will focus on successes, lessons learned, and progress against goals; alternate or adaptable solutions in use; and impacts that zero-trust implementation has had on stakeholders.

● = fully addressed ◐ = partially addressed ○ = did not address

Source: GAO analysis. | GAO-26-107693

[a]FAA's Zero Trust Implementation Plan describes the agency's approach for transitioning its operating environments to a zero-trust architecture.

Appendix IV: Comments from the U.S. Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

BY ELECTRONIC SUBMISSION

June 11, 2026

Jennifer R. Franks
Director, Center for Enhanced Cybersecurity
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to GAO-26-107693, "AVIATION CYBERSECURITY: FAA and TSA Are Collaborating on Cybersecurity but Need to Address Key Shortfalls"

Dear Ms. Franks:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS, or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

DHS leadership is pleased to note GAO's positive recognition that the Federal Aviation Administration and the Transportation Security Administration (TSA) fully addressed all eight of the auditors' leading practices for interagency collaboration while serving in leadership roles for collaborative aviation cybersecurity efforts. DHS remains committed to supporting interagency collaboration and implementing cybersecurity strategies that align with federal standards and best practices.

The draft report contained five recommendations, including one for DHS with which the Department concurs. Enclosed find our detailed response to the recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under separate cover for GAO's consideration, as appropriate.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JEFFREY M BOBICH Digitally signed by JEFFREY M BOBICH Date: 2026.06.11 12:49:50 -04'00'

JEFFREY M. BOBICH
Director of Financial Management

Enclosure

Enclosure: Management Response to Recommendation Contained in GAO-26-107693

GAO recommended that the TSA Administrator:

Recommendation 1: Update the TSA Cybersecurity Roadmap to define the roles and responsibilities for the TSA entities responsible for carrying out the goals and objectives described within it, including for the aviation subsector, and align the roadmap with the DHS Cybersecurity Strategy. The TSA Administrator should communicate its Cybersecurity Roadmap to appropriate non-federal stakeholders

Response: Concur. TSA agrees with the importance of updating the TSA Cybersecurity Roadmap, especially to include ongoing initiatives in 2022 and 2023 addressing cybersecurity in aviation security programs. Accordingly, TSA, led by the Office of Strategy, Policy, and Engagement under the direction of the TSA Deputy Administrator, will update the Cybersecurity Roadmap to align with a new DHS Cybersecurity Strategy that will be developed to align with "President Trump's Cyberstrategy for America," released March 2026.[1] This updated Cybersecurity Roadmap will designate TSA pillars responsible for implementing the objectives, with roles and responsibilities aligned to TSA Management Directive 100.0,[2] which establishes TSA's internal organizational framework, roles, and responsibilities. Further, TSA is responsible for assisting with steady-state and incident response activities in coordination with DHS and other sector risk management agencies, supporting comprehensive planning for secure cyberspace in the aviation subsector, and providing security and mitigation guidance through outreach and information sharing activities, such as the Aviation Cyber Initiative. Given the cross-cutting nature of cybersecurity activities across TSA, multiple program offices will be involved in this effort and in achieving cybersecurity goals. TSA will continue to communicate with non-federal stakeholders during development of the updated roadmap. Estimated Completion Date: May 31, 2027.

[1] "President Trump's Cyberstrategy for America," dated March 2026; See: https://share.google/ivqcRoEtG4t8DndVQ.
[2] TSA Management Directive 100.0, "TSA Roles and Responsibilities," dated My 4, 2026.

Appendix V: Comments from the U.S. Departments 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

June 22, 2026

Jennifer R. Frank
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Ms. Frank:

The Federal Aviation Administration (FAA) is committed to securing the National Airspace System by building a robust, strategic cybersecurity framework. Protecting FAA systems and strengthening government and industry partnerships is vital to safeguarding the evolving aviation ecosystem. As technological advancements introduce new challenges, FAA will continuously adapt to ensure that cybersecurity remains a core pillar of aviation safety and operational efficiency.

Upon review of GAO's draft report, we concur with the four recommendations issued to the agency to: (1) update the cyber budget data request process to ensure that it includes all cybersecurity spending from program offices; (2) update the Zero Trust Implementation Plan to include a detailed plan for transitioning all operating environments to a zero trust architecture; (3) ensure the Zero Trust Implementation Plan fully aligns with NIST best practices for migrating to a zero trust architecture; and (4) ensure the agency's Cybersecurity Steering Committee takes steps, as the agency implements its revised Cybersecurity Strategy, to ensure it carries out monitoring as planned and incorporates lessons learned from its past experiences. DOT will provide a detailed response to the recommendations within 180-days of the final GAO report issuance.

We appreciate the opportunity to respond to the GAO draft report. Please contact Gary Middleton, Director, Audit Relations and Program Improvement, at gary.middleton@dot.gov with any questions or if GAO would like to obtain additional details about these comments.

Sincerely,

Anne Byrd

Dr. Anne Byrd
Assistant Secretary for Administration

Appendix VI: GAO Contact and Staff Acknowledgments

GAO Contact

Jennifer R. Franks, FranksJ@gao.gov

Staff Acknowledgments

In addition to the contact named above, the following staff made key contributions to this report: Di'Mond Spencer-Pearson (Assistant Director), Douglas O. Harris, Jr. (Analyst-in-Charge), Donna Epler, Smith Julmisse, Anh-Thi Le, Julia Munroe, Cassaundra Pham, India Sharpe, Darron Smallwood, and Walter Vance.

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 X, LinkedIn, Instagram, and YouTube.
Subscribe to our 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/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

David A. Powner, Acting Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us