United States Government Accountability Office

Report to Congressional Committees

September 2026

AVIATION CYBERSECURITY

Enhanced Air Safety Requires FAA to Better Mitigate Threats to Aircraft Communications

GAO-26-108439

GAO Highlights

AVIATION CYBERSECURITY

Enhanced Air Safety Requires FAA to Better Mitigate Threats to Aircraft Communications

GAO-26-108439 September 2026

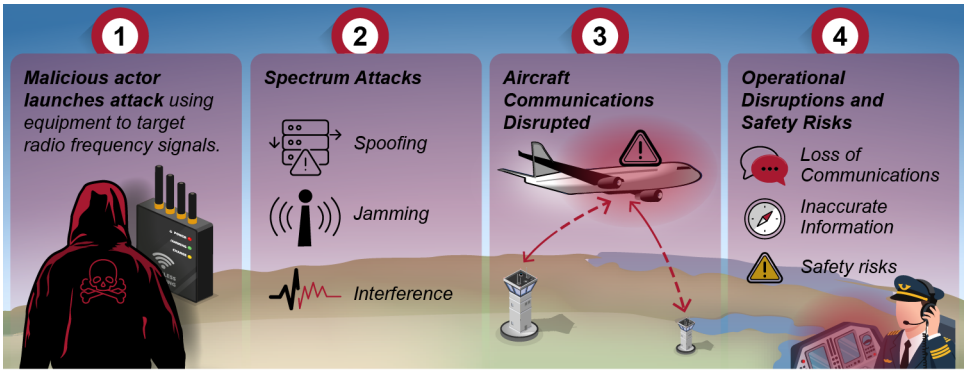
A report to congressional committees

Contact: Jennifer Franks at franksj@gao.gov

What GAO Found

The Federal Aviation Administration (FAA) has identified electromagnetic spectrum-related threats, including spoofing and jamming, to the National Airspace System (NAS) and international flight routes. However, FAA has not completed risk and mitigation assessments, and updated security documentation needed to address these threats. Additionally, FAA did not have a defined, real-time monitoring and detection capability for all spectrum-related threats. Without comprehensive risk and mitigation assessments, complete security documentation, and real-time monitoring capabilities, FAA may not have sufficient information to identify, prioritize, and respond to evolving spectrum-related threats. As a result, spoofing, jamming, and other attacks could disrupt aviation communications, degrade situational awareness, and increase the risk of operational disruptions.

Potential Cyberattacks Impacting Aircraft Communications



Sources: GAO analysis of FAA and other documentation; GAO (malicious actor, airplane, background); TarikVision/stock.adobe.com (jammer, towers); Cetacons/stock.adobe.com (icons); gentutgajah/stock.adobe.com (pilot illustration). | GAO-26-108439

FAA participates in multiple collaborative efforts with other federal agencies as well as non-federal aviation industry stakeholders regarding cybersecurity. FAA's collaborative efforts fully addressed two of the eight leading practices and partially addressed six. While FAA has defined roles and responsibilities within interagency groups, it has not established policies or procedures for information sharing, reporting, and coordination with non-federal partners outside those groups. Fully implementing leading collaboration practices could strengthen FAA's ability to effectively coordinate with key partners to mitigate cybersecurity threats affecting the aviation sector and thereby avoid fragmented and inefficient responses to incidents.

The communication applications that FAA, pilots, and aviation stakeholders use to exchange text-based information are vulnerable to cyber threats, including interception and spoofing, due to limitations related to authentication, encryption, and protocol design. For example, a malicious actor could transmit fraudulent clearance cancellations, possibly leading to flight delays or safety issues. Until FAA develops and implements a plan to strengthen authentication and data protection for these applications, malicious actors could exploit weaknesses and increase the risk of disrupted flight operations, aviation accidents, or safety incidents.

Why GAO Did This Study

Commercial flight operations rely on interconnected systems that reside onboard an aircraft and on the ground in the NAS. These systems use radio frequency signals transmitted through the electromagnetic spectrum to communicate. The Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025 includes a provision for GAO to review the vulnerability of the NAS to spectrum attacks and to assess efforts to prevent and prepare for such attacks.

This report examines, among other objectives, the extent to which FAA has identified and mitigated spectrum-related cybersecurity threats; the extent to which FAA has collaborated with federal partners to defend against cybersecurity threats; and what specific cybersecurity vulnerabilities exist in key communication applications.

To address these objectives, GAO analyzed FAA vulnerability assessments to identify spectrum-related threats to the NAS. GAO selected eight spectrum-dependent systems and assessed them against National Institute of Standards and Technology guidance. GAO also assessed key FAA collaboration mechanisms against leading practices. In addition, GAO reviewed FAA documentation to identify vulnerabilities with communication applications. GAO interviewed FAA officials and federal and non-federal stakeholders.

What GAO Recommends

GAO is making nine recommendations to FAA to strengthen its management of spectrum cybersecurity risks, enhance collaboration, and improve the security of aviation communication applications. The Department of Transportation, responding on behalf of FAA, concurred with the nine recommendations.

Contents

Letter		1
	Background	4
	FAA Has Identified Cybersecurity Threats to the NAS and International Flight Routes; However, Gaps Remain in Assessing and Addressing Risks	11
	FAA Partially Addressed Interagency Collaboration Leading Practices, but Implementation is Inconsistent	20
	Vulnerabilities Exist in Key Aircraft Communication Applications; FAA Faces Challenges Addressing Them	29
	FAA Requires Cybersecurity Measures for New Aircraft Technologies Through Certification and Operational Approval Processes	37
	Conclusions	41
	Recommendations for Executive Action	42
	Agency Comments	43
Appendix I	Objectives, Scope, and Methodology	47
Appendix II	Comments from the Department of Transportation	51
Appendix III	GAO Contact and Staff Acknowledgments	52
Tables		
	Table 1: Federal Agency Responsibilities for Aviation Cybersecurity	8
	Table 2: Examples of Spectrum-Related Threats to the National Airspace System Communications Links	12
Figures		
	Figure 1: Interconnected Systems That Support the National Airspace System	5
	Figure 2: Leading Interagency Collaboration Practices and Selected Key Considerations	10
	Figure 3: Cyberattacks Impacting Aircraft Communications	13

Figure 4: Identified Global Navigation Satellite System Spoofing and Jamming Hotspots 15
Figure 5: Extent to Which the Federal Aviation Administration Addressed Leading Practices for Interagency Collaboration 21
Figure 6: Example of a Spoofed Message that Could Disrupt Flight Operations Cancellation Messages 32
Figure 7: Example of a Spoofed Message that Could Result in an Unsafe Flight 34
Figure 8: Process of Establishing Cybersecurity Standards for New Aviation Technologies 40

Abbreviations

ACARS	Aircraft Communications Addressing and Reporting System
ACI	Aviation Cyber Initiative
ANSP	Aircraft Network Security Programs
ASH	Office of Security and Hazardous Materials Safety
ATC	air traffic control
CPDLC	Controller Pilot Data Link Communications
DHS	Department of Homeland Security
DOD	Department of Defense
DOT	Department of Transportation
FAA	Federal Aviation Administration
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
GPS/GNSS	Global Positioning System/Global Navigation Satellite System
HF	High Frequency
IPS	Internet Protocol Suite
IRAC	Interdepartmental Radio Advisory Committee
NAS	National Airspace System
NIST	National Institute of Standards and Technology
NTIA	National Telecommunications and Information Administration
OMB	Office of Management and Budget
PIRT	Purposeful Interference Response Team
RF	Radio Frequency
RTCA	Radio Technical Commission for Aeronautics
SDR	software-defined radio
VHF	Very High Frequency

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

September 21, 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 National Airspace System (NAS).[1] FAA also employs over 14,000 air traffic controllers and maintains over 100 ground navigation facilities to ensure passengers and flights get to their destinations safely.

Commercial flight operations rely on interconnected systems located both onboard aircraft and throughout the NAS. These systems exchange information using radio frequency (RF) signals transmitted through the electromagnetic spectrum (spectrum).[2] At the same time, cyber-based threats to federal information systems, including those FAA uses to provide air traffic control (ATC) services and data communications, continue to evolve. Of these, spectrum-related threats can disrupt, degrade, manipulate, or deny the RF signals used for aviation communication, navigation, and surveillance. As aviation systems become increasingly interconnected and dependent on spectrum-based technologies, disruptions to the RF signals can affect the availability and reliability of systems that support flight operations.

The Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025[3] includes provisions for GAO to, among other things, review the vulnerability of the NAS and international

[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]Radio frequency (RF) signals are wireless transmissions that operate within the electromagnetic spectrum. The electromagnetic spectrum is the range of frequencies used to transmit information through technologies such as radios, radar, GPS, cellular networks, and satellite communications.

[3]Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025, Pub. L. No. 118-159, title LV, § 5501, 138 Stat. 1773, 2452 (2024).

flight routes to electromagnetic spectrum attacks and to assess the federal government's efforts to prevent and prepare for such attacks.[4]

Our objectives were to determine (1) the extent to which FAA has identified and mitigated spectrum-related cybersecurity threats to the NAS and international flight routes; (2) the extent to which FAA has collaborated with federal partners to strengthen defenses against cybersecurity threats; (3) what specific cybersecurity vulnerabilities exist in key communication applications, including the Aircraft Communications Addressing and Reporting System (ACARS) and the Controller Pilot Data Link Communications (CPDLC), and to what extent FAA has addressed them; and (4) what cybersecurity measures FAA requires for new aircraft technologies to reduce potential vulnerabilities.

To address our first objective, we analyzed threat and vulnerability assessments for relevant FAA data communications links to identify spectrum-related threats to the NAS and international flight routes and how FAA was mitigating the threats. We also assessed FAA system authorization-to-operate documents for eight NAS systems[5] against selected cybersecurity controls from the National Institute of Standards and Technology (NIST) and against FAA's Security Authorization Handbook to identify gaps in security controls.[6]

To address the second objective, we evaluated aviation cybersecurity coordination among multiple federal agencies and non-federal stakeholders by analyzing documentation of key FAA collaboration mechanisms against GAO's eight leading practices for enhancing collaborative efforts.[7]

[4]NIST defines electromagnetic interference, whether intentional or unintentional, as something that disrupts, degrades, or limits the performance of communications, navigation, surveillance, or other electronic systems.

[5]We did not include the names of the eight systems due to sensitivity concerns. We selected the eight systems based on spectrum dependent systems that are critical to the NAS.

[6]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, SP 800-53, Rev. 5 (Gaithersburg, MD: Sept. 2020).

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

To address the third objective, we assessed outage and incident reports, FAA documentation, and academic publications to identify cybersecurity risks and vulnerabilities of ACARS and CPDLC. We interviewed FAA officials to see how they were mitigating these vulnerabilities.

To address the fourth objective, we reviewed FAA's certification process, aircraft-specific regulatory requirements called (special conditions), and other FAA policy documents and guidance to describe how the agency develops certification requirements for new aviation technologies.[8]

For all four objectives, we either met with or received written responses from FAA officials responsible for cybersecurity, communications systems, spectrum management, incident response, and aviation safety. We also interviewed officials from the Department of Defense (DOD), Department of Commerce (DOC), Department of Homeland Security (DHS), and Federal Communications Commission (FCC). These officials provided information on the RF threats posed to the NAS, collaboration efforts, ACARS and CPDLC vulnerabilities and mitigations, and cybersecurity requirements for new aviation technologies. Finally, we conducted site visits to the Air Route Traffic Control Center in Leesburg, Virginia and the Air Traffic Control System Command Center in Warrenton, Virginia to interview staff and tour the facility to understand the operations of these systems and how threats are mitigated.

We also discussed cybersecurity threats to the NAS, including ACARS and CPDLC, existing mitigations, FAA's coordination with aviation stakeholders, and how FAA and selected aviation stakeholders identify cybersecurity requirements.[9] We conducted a content analysis of the aviation stakeholders' interview responses to identify key themes related to each objective. For more information on our objectives, scope, and methodology, see appendix I.

We conducted this performance audit from April 2025 to September 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain

[8]FAA special conditions are aircraft-specific regulatory requirements issued when existing regulations do not contain adequate or appropriate safety standards for an unusual design feature.

[9]We identified a non-generalizable sample of 21 aviation stakeholders based on our knowledge of prior GAO work and recommendations from stakeholders. Of those 21 stakeholders, 13 responded to our meeting request. The remaining eight either did not respond or stated that they were unable to assist us.

sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

FAA, an agency of the Department of Transportation (DOT), is responsible for civil aviation safety oversight. It is also responsible for the safe and efficient management of the navigable airspace of the United States and of international airspace delegated to the United States for the purpose of providing air traffic services under relevant regional air navigation agreements. Its stated mission is to provide the safest, most efficient aerospace system in the world. This system, known as the NAS, includes ATC systems, ATC procedures, operational facilities, aircraft, and the people who certify, operate, and maintain them. According to FAA, the NAS includes more than 19,000 airports, and over 500 ATC facilities across the United States.

Systems Supporting National Airspace System Communications

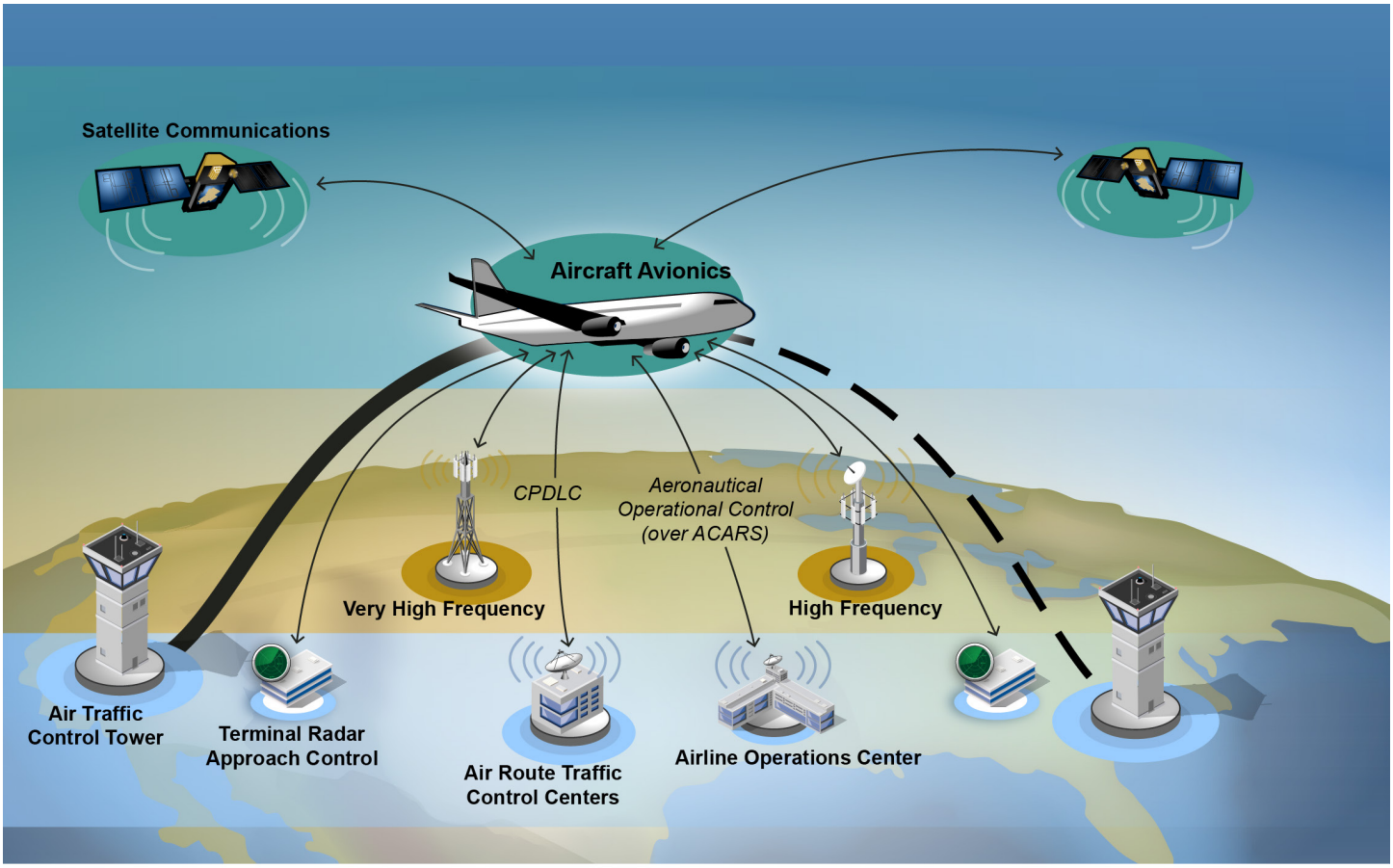
FAA's ability to fulfill its mission depends on the capability and reliability of its vast network of computer hardware and software that supports its ability to provide air navigation services. The agency relies on more than 100 systems to process and track flights around the world. These complex and highly automated systems process a wide range of information, including communication, navigation, surveillance, automation and processing, flight information, air traffic flow management, air traffic control systems, infrastructure, and systems used by airport authorities—all of which are required to support the agency's mission. In order to successfully carry out ATC operations, it is essential that these systems interoperate, functioning both within and across facilities as one integrated system of systems.

Aircraft avionics systems[10] enable communication through satellite communication systems, as well as Very High Frequency (VHF), High Frequency (HF), Ultra High Frequency, and Super High Frequency radio systems. These systems support applications such as ACARS and

[10]Avionics systems are generally considered one of the most vital components of an airplane due to their criticality for safe flight operations. They include engine controls, flight control systems, navigation, communications, flight recorders, lighting systems that provide interior and exterior illumination, fuel systems, weather radar, performance monitors, and systems that carry out hundreds of other mission and flight management tasks.

CPDLC for message exchanges.[11] These avionic systems interface with ground stations and service providers to exchange information between the aircraft, Airline Operations Centers, and ATC facilities, including airport control towers, Terminal Radar Approach Control, and Air Route Traffic Control Centers (see figure 1).

Figure 1: Interconnected Systems That Support the National Airspace System



CPDLC = Controller Pilot Data Link Communications, ACARS = Aircraft Communications Addressing and Reporting System

⟷ Data communication (data includes CPDLC and ACARS) Projected flight path

Sources: GAO analysis based on Federal Aviation Administration information; GAO (airplane, background); AlexZel/stock.adobe.com (buildings); TarikVision/stock.adobe.com (towers). | GAO-26-108439

[11]ACARS is digital messaging application that enables aircraft and ground personnel to exchange operational information. CPDLC is one of several applications used to exchange safety-related messages between pilots and air traffic controllers.

The Aeronautical Operational Control transmits a significant portion of ACARS messages and supports the exchange of aircraft status, flight plans, weather, and other operational information between an aircraft, airlines, and service partners at the Airline Operations Centers. ATC-related ACARS messages include clearances, route changes, and position reports. Flight plans received through these communication systems can be uploaded into the flight management system, an avionics system that manages an aircraft's navigation routes.

CPDLC is an ATC application that operates over data link communications systems. CPDLC allows air traffic controllers to transmit digital text messages to an aircraft and vice versa as an alternative to voice communications. Examples of CPDLC messages may include clearance and instructions, reports and requests, aircraft position and estimated time of arrival, and acknowledgements, among other messages. Messages from ATC normally follow a standard format and require a response from the aircraft. CPDLC messages, formatted by their respective systems, should follow strict standard format in most cases, especially safety-critical messages. Free text is available and permitted for certain situations, such as for clarifications or operational remarks. However, FAA discourages CPDLC free text in most cases.

In 2024, we reported that a large majority of FAA's ATC systems were unsustainable or potentially unsustainable. We also found that FAA was not moving fast enough to modernize its systems.[12] Consistent with our findings, in May 2025 FAA announced a new initiative to accelerate the modernization of its outdated systems—referred to as the Brand New Air Traffic Control System initiative. This new initiative intends to, among other things, replace outdated infrastructure including radars, radio systems, software, hardware, and telecommunications lines to manage modern travel by December 2028.[13]

Cybersecurity Supports the Safe and Reliable Operation of Air Traffic Control Systems

Safeguarding federal computer systems and the systems supporting the nation's critical infrastructures, including the NAS, are essential to

[12]GAO, *Air Traffic Control: FAA Actions Are Urgently Needed to Modernize Aging Systems*, GAO-24-107001 (Washington, D.C.: Sept. 23, 2024).

[13]We have an ongoing review assessing FAA's progress in implementing the Brand New Air Traffic Control System initiative.

protecting national and economic security and public health and safety.[14] For government organizations, information security is also a key element in maintaining public trust. Inadequately protected systems may be vulnerable to insider threats, as well as the risk of intrusion by individuals or groups with malicious intent who could use their illegitimate access to obtain sensitive information, disrupt operations, or launch attacks against other computer systems and networks. Accordingly, since 1997, we have designated information security as a government-wide High Risk area.[15] In 2003, we expanded this High Risk area to include protecting systems supporting our nation's critical infrastructure.[16]

Laws and Guidance Supporting Federal Cybersecurity

Federal laws and guidance specify requirements for protecting the security of federal information and systems, including FAA systems.

Federal Information Security Modernization Act of 2014 (FISMA).[17] FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over federal operations and assets. FISMA assigns responsibility to each agency head for providing information security protections commensurate with the risk and magnitude of the harm. Security risks include unauthorized access, use, disclosure, disruption, modification, or destruction of information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. The law also requires each agency

[14]The term "critical infrastructure" refers to systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters. 42 U.S.C. § 5195c(e). Federal policy identifies 16 critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems. In addition, several sectors have subsectors (e.g., the aviation and freight rail subsectors within the transportation sector).

[15]GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: Feb. 1, 1997).

[16]GAO, *High-Risk Series: An Update*, GAO-13-283 (Washington, D.C.: Feb. 14, 2013).

[17]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), Title III of Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2014 and those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect. This act provides a comprehensive framework for ensuring the effectiveness of information security controls over federal agency operations and assets.

to develop, document, and implement an agency-wide information security program to provide risk-based safeguards for the information and information systems that support the operations and assets of the agency.

NIST guidance. FISMA requires agencies to comply with information security standards developed by NIST, including minimum information security requirements as described in NIST Special Publication (SP) 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*.[18] This publication provides a catalog of security and privacy controls for federal information systems and a process for selecting controls to protect organizational operations and assets. For example, the publication calls for vulnerabilities to be remediated according to organization-defined time frames based on an assessment of risk.

Federal Agency Roles Supporting Aviation Cybersecurity

Three agencies have distinct roles and responsibilities regarding aviation cybersecurity. The agencies responsible for supporting aviation security are FAA, DHS, and DOD. The responsibilities of each agency are outlined in table 1 below.

Table 1: Federal Agency Responsibilities for Aviation Cybersecurity

Agency	Aviation Cybersecurity Responsibilities
Federal Aviation Administration (FAA)	The FAA is responsible for civil aviation safety oversight, as well as for the safe and efficient management of the navigable airspace of the United States and of international airspace delegated to the United States for the purpose of providing air traffic services under relevant regional air navigation agreements. The agency serves as co-lead with the Transportation Security Administration (TSA) for the aviation subsector of the transportation systems critical infrastructure sector, including airports and ground support systems not otherwise overseen by FAA, for which the Department of Transportation and the Department of Homeland Security are co-Sector Risk Management Agencies. To the extent that cybersecurity risks could threaten the safety of civil aviation, FAA is responsible for overseeing efforts to mitigate those risks. For example, FAA is responsible for developing the national airspace system cyber threat management process and has also been directed by Congress to promote safe flight of civil aircraft through minimum standards required in the interest of cybersecurity of aircraft.

[18]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*.

Department of Homeland Security (DHS)	DHS is the lead federal agency for cybersecurity protection. With regard to aviation, DHS, through the TSA, is responsible for coordinating federal government activities addressing aviation security. DHS, through TSA, conducts these activities by identifying conflicting procedures, identifying vulnerabilities and consequences, and coordinating corresponding interagency mitigation actions. Further, DHS, through TSA, is responsible for overseeing transportation security activities, such as airport security. The Cybersecurity and Infrastructure Security Agency (CISA), a component within DHS, is responsible for identifying cybersecurity vulnerabilities and coordinating mitigation actions across the federal government, including aviation cybersecurity research efforts.
Department of Defense (DOD)	DOD conducts its missions within the National Airspace System (NAS) as both an aircraft operator and, as delegated by FAA, a provider of air traffic control (ATC) and other air navigation services. DOD has the authority to certify its own aircraft, manage delegated airspace, and provide ATC-related services in accordance with FAA requirements. DOD is also responsible for aviation security programs and initiatives that support national security.

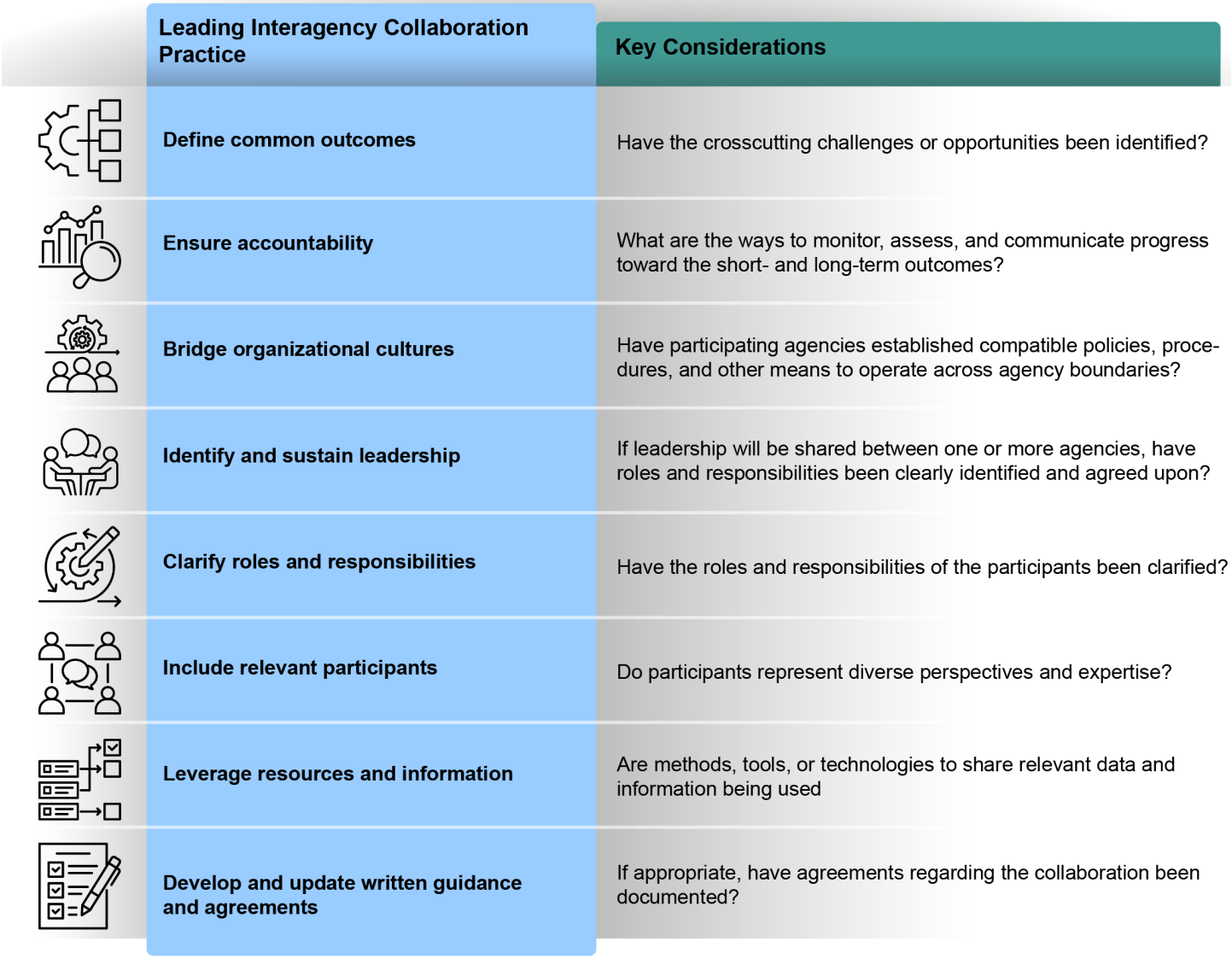
Source: GAO analysis based on FAA, DHS and DOD information. | GAO-26-108439

GAO Guidance on Collaboration

In 2023, GAO updated the leading interagency collaboration practices to help agencies collaborate to address crosscutting challenges facing the federal government.[19] GAO identified eight leading interagency collaboration practices for achieving important interagency outcomes, as well as key considerations for those practices. These practices help to provide valuable insight and guidance to improve collaboration between agencies. Figure 2 lists each leading practice and an associated key consideration.

[19]GAO-23-105520.

Figure 2: Leading Interagency Collaboration Practices and Selected Key Considerations



Sources: GAO; *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges;* Cetacons/stock.adobe.com (icons). | GAO-26-108439

FAA Has Identified Cybersecurity Threats to the NAS and International Flight Routes; However, Gaps Remain in Assessing and Addressing Risks

FAA has identified emerging spectrum-related cybersecurity threats to the NAS and international flight routes. Such threats could disrupt, degrade, or deceive critical systems within the NAS required for communication, navigation, and surveillance services resulting in operational disruptions that increase flight safety risks, erode ATC effectiveness, and cause significant flight delays. However, FAA has not fully implemented key elements of a risk-based cybersecurity program. As a result, FAA may not have sufficient information to identify, assess, and address cybersecurity risks affecting critical aviation communications systems.

FAA Has Identified Cybersecurity Threats to the NAS and International Flight Routes

FAA, alongside other agencies such as CISA and DOD, has identified cybersecurity threats to the NAS and international flight routes. Three key spectrum-related threats to the NAS are spectrum interference, spoofing, and jamming. Spectrum interference could degrade or block communications between ground systems and the aircraft, which rely on these communication links to send and receive time-sensitive ATC instructions and operational data such as surveillance and navigation data. Similarly, spoofing can transmit false signals or information that may cause aircraft or ground systems to receive inaccurate data, while jamming can overwhelm legitimate signals and deny access to critical communications or navigation services. If successful, these attacks can negatively impact the safety, security, and efficiency of air traffic operations. These spectrum-related threats and how they may affect the NAS are identified in table 2 below.

Table 2: Examples of Spectrum-Related Threats to the National Airspace System Communications Links

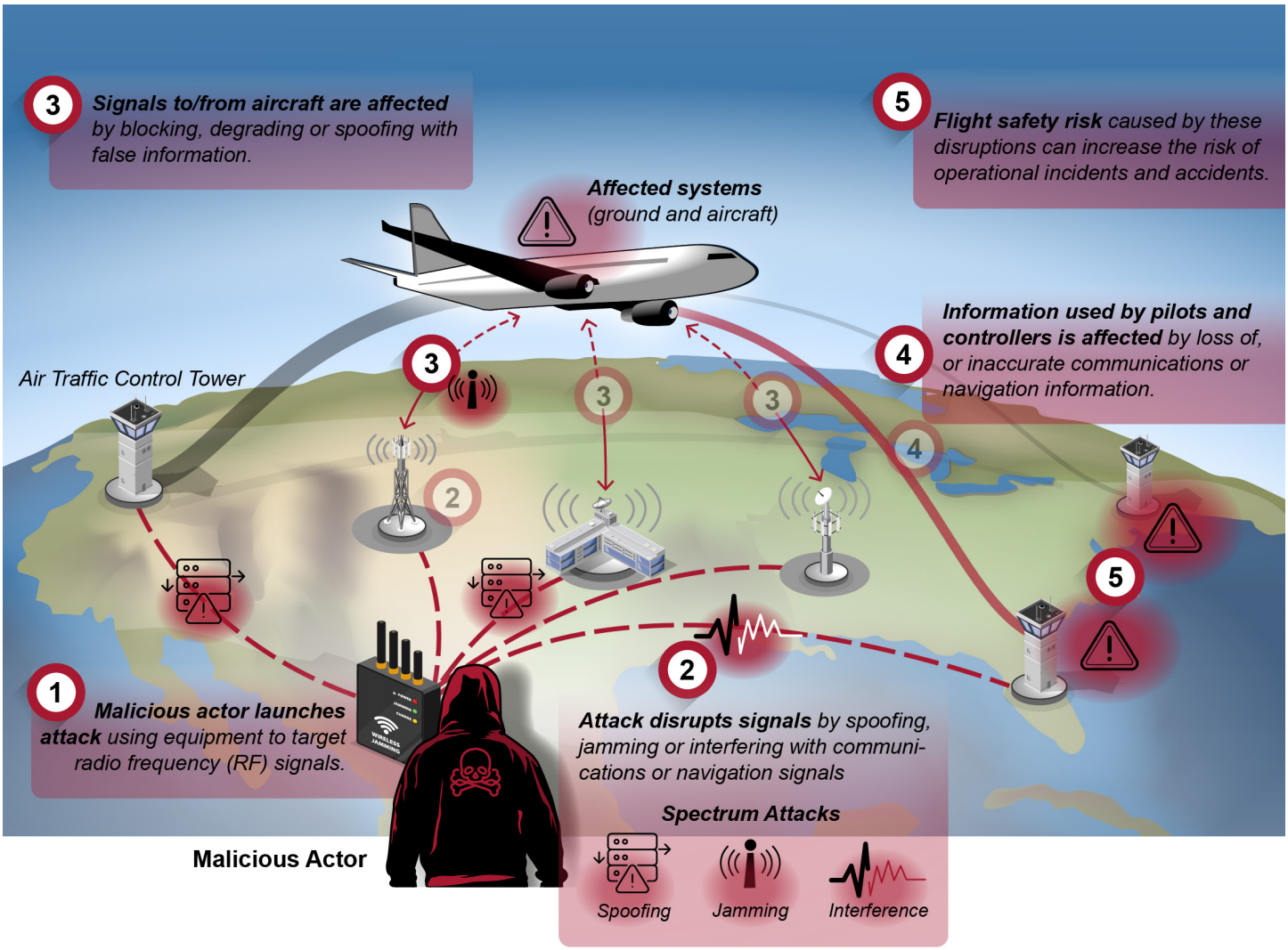
Threat	Definition	Examples of Effects
Spectrum Interference	Occurs when unwanted radio frequency energy that disrupts wireless communication or navigation systems causes degraded performance or signal loss. It results from systems using the same frequency channel or an adjacent band in the same geographic area.	In 2012, Newark Airport experienced harmful interference during pre-deployment testing of a ground-based augmentation system. This was caused by an individual who operated a device jamming GPS transmissions. This interference degraded a system that leverages GPS positioning accuracy to improve aircraft approach, departure, and terminal area operation.
Spoofing	Involves emissions of GPS/ Global Navigation Satellite System (GNSS)-like signals that may be acquired and tracked in combination with or instead of the intended signals by public GPS receivers. Spoofing can result in false and potentially confusing, or hazardously misleading position, navigation, and/or date and time information in addition to loss of GPS/GNSS service.	In 2022, the area around a Dallas airport experienced GPS/GNSS interference with signs of spoofing that affected arriving aircraft. This caused confusion for air traffic control (ATC) and led to over 230 departure delays. Pilots had to rely on ground-based navigation and radar guidance to adjust their routes.
Jamming	Involves emissions that interfere with the civil receiver's ability to acquire and track GPS/GNSS signals. Jamming can result in denial of GPS/GNSS navigation, positioning, timing, and aircraft dependent functions.	In 2022, an unauthorized transmitter broadcasting on the GPS/GNSS frequency within the vicinity of the Denver International Airport affected civil flights, ATC, and other GPS/GNSS dependent systems. This resulted in disrupted navigation accuracy and impacted onboard safety systems.

Source: GAO analysis of FAA and other documentation. | GAO-26-108439

Note: These are examples of spectrum-related threats to the NAS and do not represent a comprehensive list of all potential threats.

Figure 3 shows how a malicious actor could potentially use spectrum-related attacks (e.g., spectrum interference, spoofing, and jamming) to disrupt communications and navigation signals exchanged among ground infrastructure, ATC facilities, and aircraft. For example, spoofing could transmit false position, velocity, or timing data to an aircraft, while jamming could block or degrade communications or navigation signals. These disruptions could affect the availability or integrity of information used by pilots and air traffic controllers, increasing operational and flight safety risks.

Figure 3: Cyberattacks Impacting Aircraft Communications



Sources: GAO analysis of Federal Aviation Administration and other documentation; GAO (airplane, malicious actor, background); AlexZel/stock.adobe.com (buildings); TarikVision/stock.adobe.com (towers, jammer); Cetacons/stock.adobe.com (icons). | GAO-26-108439

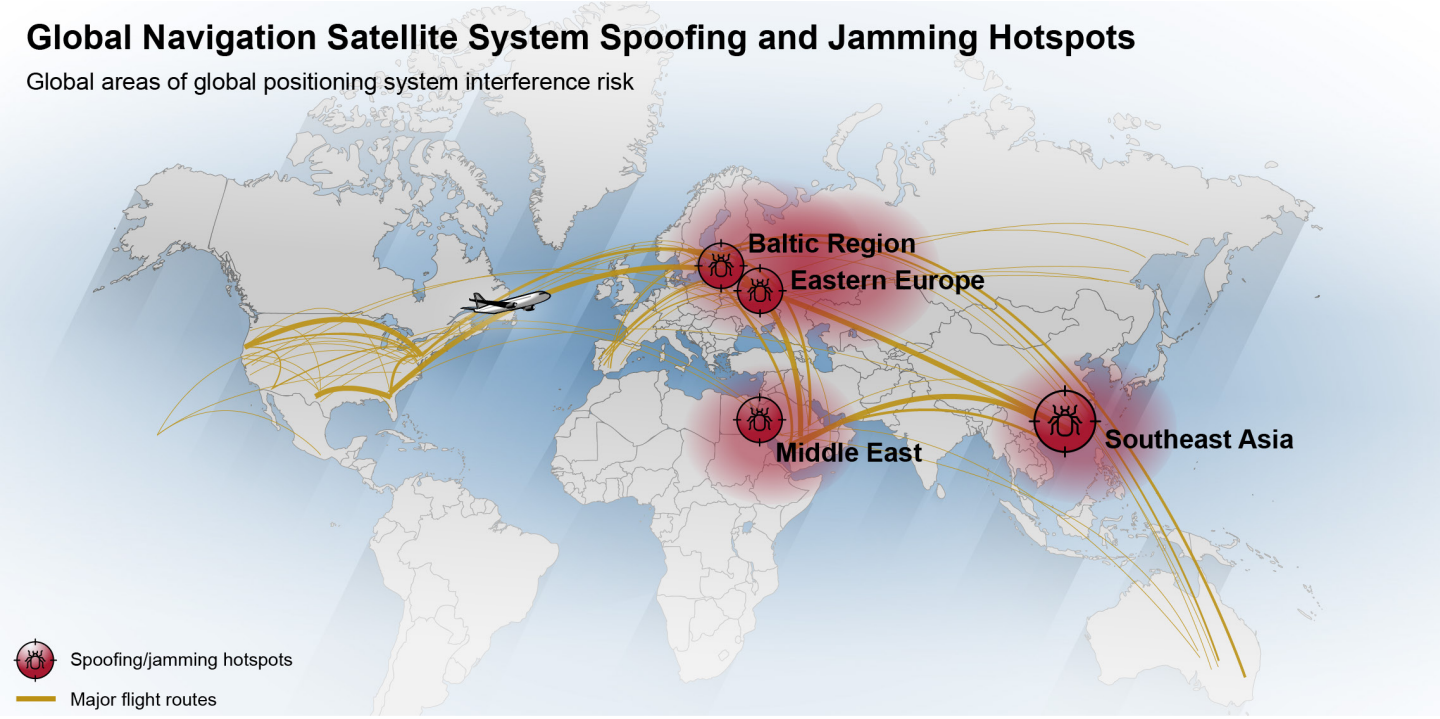
In addition to threats to the NAS, FAA has identified several international flight routes where GPS/Global Navigation Satellite System (GNSS) interference is increasing, particularly in conflict areas such as the Middle East, Eastern Europe, Southeast Asia, and the Baltic region. These disruptions often originate from military jammers and counter-unmanned

aircraft systems operating in conflict zone areas.[20] These conditions create safety risks for international flights, as GPS/GNSS signal interference can degrade or cause loss of data communications and increase the voice communications workload. In addition, false signals from spoofing can potentially cause a mismatch and mislead pilots and ATC of the aircraft's GPS/GNSS position. This can potentially cause the aircraft to enter restricted airspace without the knowledge of pilots and ATC.

For example, an Azerbaijan Airlines flight was shot down in December 2024 amid heightened GPS/GNSS disruptions linked to the ongoing Russia-Ukraine conflict, causing the approach to become more complex than usual and resulting in multiple pilot and ATC miscommunications. In 2025, the International Air Transport Association also reported that incidents of GPS/GNSS signal loss—from interference, space weather, or onboard issues—increased from 28.1 to 60.1 per 1,000 aircraft since 2021, indicating a growing risk. To combat these risks, in addition to advising against or restricting operations in certain areas, FAA, foreign civil aviation authorities, and international organizations are working together to detect and advise on jamming and spoofing, as well as working with industry to make detection and mitigation procedures available to pilots. Figure 4 illustrates hotspots for spoofing and jamming of GPS/GNSS signals, primarily in conflict zones.

[20]Counter-unmanned aircraft systems—also frequently referred to as a counter-drone system—are a suite of technologies and procedures designed to mitigate a credible threat that an unmanned aircraft system or unmanned aircraft poses.

Figure 4: Identified Global Navigation Satellite System Spoofing and Jamming Hotspots



Sources: GAO analysis based on Federal Aviation Administration documentation; GAO (airplane, world map illustrations); Cetacons/stock.adobe.com (icons). | GAO-26-108439

FAA Has Not Developed Sufficient Threat Risk Assessment or Mitigation Reports

Risk assessments evaluate threats, vulnerabilities, likelihood, and potential impacts to organizational operations and assets. They also assess existing security controls and mitigations to determine whether they effectively reduce risk to an acceptable level. NIST SP 800-53 Rev. 5 recommends agencies perform a risk assessment to identify threats, vulnerabilities, likelihood, and impact. The results of these assessments are intended to support risk response decisions and mitigations. Additionally, FAA Order 1370.121B and its supplemental implementation directives require FAA systems to identify cybersecurity risks and implement controls to mitigate those risks based on their importance to the agency's mission.[21]

For seven of the eight spectrum-dependent NAS systems we reviewed, FAA did not produce separate, detailed risk assessment reports, as called

[21]Federal Aviation Administration, *FAA Information Security and Privacy: Policy*, Order 1370.121B (Apr. 25, 2022).

for in NIST SP 800-53 Rev. 5. FAA officials stated they did not develop separate risk assessments because the agency maintains a general spectrum risk assessment that addresses risks across systems. However, FAA's general spectrum risk assessment does not satisfy the NIST recommendation for system-specific risk assessments because it assesses spectrum risks at a broad level and does not evaluate how specific threats and vulnerabilities affect individual systems. For example, different systems may face varying levels of exposure to threats such as interference, spoofing, jamming, or other weaknesses in authentication and data protection.

Without assessments tailored to individual systems, FAA cannot demonstrate that they evaluated spectrum-related threats, vulnerabilities, impacts, and residual risks in the context of each system's unique mission, architecture, and controls. As a result, FAA may not make informed risk-based decisions regarding security controls and mitigations, increasing the risk that communications systems could experience disruptions that affect the efficiency of air traffic controllers and safety of the NAS.

FAA Security Documents Are Not Aligned with Current NIST Standards, Required Controls, or Consistent System Impact Levels

FISMA requires federal agencies to maintain security policies and procedures aligned with information security standards developed by NIST, such as SP 800-53 Rev. 5, which was revised on September 2020, and superseded Rev. 4. NIST SP800-53 Rev. 5 expanded security and privacy controls to address evolving cybersecurity threats, including supply chain risks, privacy protections, and increased emphasis on resilience and risk management.[22] Agencies are expected to align their security programs and system documentation with Rev. 5 standards. In addition, NIST Federal Information Processing Standards (FIPS) Publication 199 requires federal agencies to categorize information systems based on the potential impact of a security breach, while NIST FIPS 200 requires agencies to implement appropriate security controls for high-impact systems.[23] FAA's Air Traffic Organization Information

[22]Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073, 3078 (2014) (44 U.S.C. § 3554) and National Institute of Standards and Technology, SP 800-53, Rev. 5.

[23]National Institute of Standards and Technology, *Minimum Security Requirements for Federal Information and Information Systems*, FIPS 200 (Washington, D.C., March 2006). FIPS 199 establishes the method for categorizing federal information system as high, medium, and low impact while FIPS 200 establishes minimum information security requirements for federal information systems corresponding to the system's FIPS 199 categories.

Security Continuous Monitoring Plan also requires FAA systems to regularly update security documentation to reflect current standards.[24]

Also, NIST FIPS 199 and the NIST Risk Management Framework, call for federal systems to have a clearly defined and consistently documented security categorization across authorization artifacts.[25] The categorization determines the appropriate control baseline from NIST SP 800-53 Rev. 5.

Further, FAA's Security Authorization Handbook outlines the agency's process for aligning with the NIST Risk Management Framework.[26] It requires an initial security assessment before a system begins operation, followed by annual partial assessments and full reauthorization every 3 years.

FAA has established policies and procedures for managing the security authorization process for NAS systems. However, our review identified several weaknesses in the implementation and documentation of security controls in the eight NAS systems we reviewed, as follows:

- Four systems still referenced the outdated NIST SP 800-53 Rev. 4, which was superseded in 2021.
- Five systems did not include all required baseline security controls for high-impact systems. Specifically, there were missing key security controls in the system security plans that do not fully reflect the system's implemented high baseline controls, such as contingency planning and protection against denial-of-service. This results in documentation inconsistency and lack of alignment between the system security plan and control implementation artifacts.
- One system had inconsistencies in system categorization. For example, some documents (e.g., executive summary and security assessment report) classified the system as high impact, while others (e.g., system security plan and contingency plan) classified it as

[24]Federal Aviation Administration, *Air Traffic Organization Information Security Continuous Monitoring Plan*, Version 24.0. The plan describes the strategy, approach, and implementation of continuous monitoring in support of Ongoing Authorization decisions.

[25]National Institute of Standards and Technology SP 800-37, Revision 2: *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (Gaithersburg, Md.: December 2018).

[26]Federal Aviation Administration, *Fiscal Year 2024 (FY24) Security Authorization Handbook*, (Oct. 2023).

moderate. This inconsistency affects how security requirements are defined and assessed.

- One system had not completed its required annual security assessment since 2023.

After we completed our review of the eight NAS systems, FAA completed the required annual security assessment for one system and updated system documents to reference NIST SP 800-53 Rev. 5 for three of the four systems. Similar issues were reported by the DOT Office of Inspector General, which found that FAA systems continue to rely on outdated NIST standards and lack required controls for high-impact systems.[27] The Office of Inspector General recommended that FAA address these gaps to reduce risk. FAA officials stated they follow NIST guidance for the 3-year authorization cycle and that, although some documents had not been signed since fiscal year 2023, they are updated annually. However, this response does not fully address the deficiencies identified during our review. While FAA completed corrective actions for some systems after our review, one system still did not reflect current NIST guidance, several systems had incomplete control baselines, one system had inconsistent categorization, and one system had an overdue assessment at the time of our review.

Until FAA fully aligns system documentation, security controls, system categorizations, and assessment activities with current federal requirements, the agency may lack complete and reliable information to make risk-based cybersecurity decisions for critical NAS systems. As a result, security weaknesses may go unidentified, inadequately assessed, or insufficiently mitigated, increasing the risk of disruption to aviation operations.

FAA Lacks Real-Time Monitoring and Response Capabilities for Spectrum-Related Cyber Threats

Continuous monitoring involves maintaining ongoing awareness of system security, including vulnerabilities, threats, and the effectiveness of security controls to support risk management decisions. NIST SP 800-53 Rev. 5 calls for covered organizations to implement a continuous monitoring strategy to regularly assess security controls, track changes to the system and its environment, identify emerging risks, and report security status to appropriate officials. Additionally, FAA Order 1370.121B and its supplemental implementing directives require FAA systems to

[27]Department of Transportation, Office of Inspector General, *FAA Does Not Effectively Secure Its High-Impact Systems Supporting the National Airspace System*, FI2026023 (April 1, 2026). This public version of the report did not disclose the specific systems or security controls.

identify cybersecurity risks and implement controls based on their importance to the agency's mission.

According to FAA officials, the Security and Hazardous Materials Safety organization oversees the FAA's Counterintelligence Program and coordinates with interagency partners to identify and mitigate foreign, domestic, and insider threats to FAA systems, facilities, information, missions, and personnel. These efforts include sharing threat information, leveraging classified and open-source intelligence to inform leadership, and coordinating with the FAA Security Operations Center to investigate suspicious activity and potential security incidents. Additionally, the Security and Hazardous Materials Safety organization monitors security policies and plans for FAA systems to proactively identify and mitigate risks and threats. FAA officials stated that in some cases, these efforts have led to the identification and prosecution of individuals attempting unauthorized access to FAA systems. However, these activities are focused on broader security and counterintelligence efforts and do not provide real-time monitoring of spectrum-related threats.

According to FAA's Information System Continuous Monitoring plan, security posture monitoring consists of real-time activities conducted by the NAS Cyber Operations office in collaboration with other organizations and offices that assist in cyber threat intelligence support.[28] These activities include monitoring systems and network event logs to identify unusual or unauthorized activity. For example, FAA officials stated that the NAS Cyber Operations has tools and dashboards that identify all network traffic traversing the NAS, which plays a crucial role in identifying potential security threats in real-time.

However, FAA's Spectrum Engineering office has limited capability to monitor spectrum-related threats (e.g., spectrum interference, jamming, or spoofing) in real-time. Instead, it primarily relies on investigating incidents after they have been reported. Officials stated they do not have a continuous, 24/7 monitoring capability and lack specialized tools needed to detect certain threats, such as signal interference or spoofing, as they occur. Although technologies exist that can continuously monitor spectrum-related activity, detect anomalous signals, analyze potential threats, and generate alerts, FAA does not currently have comparable capabilities. FAA's Wide Area Augmentation System monitors GPS signal

[28]Department of Transportation, Federal Aviation Administration, Air Traffic Organization, *Information Security Continuous Monitoring (ISCM) Plan, Version 24* (Washington, D.C.).

integrity and issues alerts when GPS performance is degraded.[29] However, the Wide Area Augmentation System is designed to support navigation performance rather than detect cyber or spectrum-related threats. It can identify signal degradation but does not detect spoofing or determine the source of interference. FAA officials stated that a large portion of the RF signals used by aviation communication systems are managed by other entities and therefore falls outside of FAA's direct control or monitoring authority. They also said they lack total visibility in key data service providers. For example, FAA has very limited ability to monitor data service providers and no monitoring of satellite providers due to the nature of the arrangements between the providers and FAA as the customer. These gaps limit FAA's ability to detect and respond to spectrum-based threats.

FAA officials also cited funding constraints as a key challenge which have limited the rollout of certain monitoring tools for high-risk systems. Without on-site deployment of these tools, FAA cannot proactively monitor for interference, spoofing, or jamming activities. As a result, the agency's ability to quickly detect and respond to these types of threats is limited. Until FAA implements real-time detection capabilities, the NAS remains vulnerable to disruptions that could affect aviation communications and safety.

FAA Partially Addressed Interagency Collaboration Leading Practices, but Implementation is Inconsistent

FAA has collaborated with a range of federal and non-federal partners to address aviation cybersecurity risks. Key collaboration efforts include participation in interagency groups such as the Aviation Cybersecurity Initiative (ACI), Purposeful Interference Response Team (PIRT)/CRUCIBLE, the Interdepartmental Radio Advisory Committee (IRAC), as well as coordination with other government agencies and industry stakeholders on cybersecurity, communications, and spectrum-related issues.

Regarding the eight leading interagency collaboration practices, FAA has fully incorporated two and partially incorporated six of the practices when working with interagency groups, federal partners, and non-federal partners. Figure 5 illustrates our assessment of FAA's implementation of the eight leading interagency collaboration practices.

[29]Wide Area Augmentation System is a system operated by FAA to improve GPS accuracy, integrity, and reliability for aviation.

Figure 5: Extent to Which the Federal Aviation Administration Addressed Leading Practices for Interagency Collaboration

Source: GAO analysis of FAA and other documentation. | GAO-26-108439

FAA Has Fully Met Two of Eight Leading Interagency Collaboration Practices

Define Common Outcomes. GAO's leading collaboration practices state that participants should develop a shared understanding of the crosscutting challenges or opportunities to effectively coordinate efforts and build buy-in among internal and external stakeholders.

FAA has defined common outcomes by working with a variety of federal and non-federal partners to coordinate efforts and address crosscutting challenges. For example:

- FAA is one of three lead agencies in ACI which is a tri-chaired federal task force established in 2019 by DOT, DHS, and DOD. Representing DOT, FAA works with government and industry partners to identify aviation cybersecurity vulnerabilities, improve resilience, and coordinate efforts to reduce cyber risks across the aviation ecosystem.
- The agency participates in PIRT/CRUCIBLE alongside the DOD's Space Force, Coast Guard, CISA, and FCC. PIRT is a collaborative interagency group with subgroups responsible for investigating and addressing different types of interference. As part of PIRT, CRUCIBLE is the name for designated federal operations centers that coordinate responses to GPS disruptions in the NAS. Through designated operations centers, these agencies coordinate responses to GPS disruptions by sharing information, assessing reported incidents, and determining appropriate response actions.
- FAA is a member of IRAC, which advises the National Telecommunications and Information Administration (NTIA) on federal spectrum allocation, management, and frequency assignments. FAA coordinates with other federal agencies through IRAC's committee structure, subcommittees, and working groups on spectrum-related issues.

FAA and its partners share information outside formal coordination structures through direct communication among officials and subject matter experts. For example, FCC and DOD officials stated that they routinely exchange information with FAA outside interagency forums. In addition, it works alongside multiple non-federal aviation industry partners to communicate and conduct research on spectrum-related issues.

Leverage Resources. GAO's leading collaboration practices state that successfully addressing crosscutting challenges and opportunities requires collaborating agencies to effectively leverage technological resources, including methods, tools, and technologies used to share relevant data and information.

FAA has leveraged resources by employing a range of methods, tools, and technologies to share relevant data and information. For example, officials stated that the agency uses multiple reporting systems and analytic tools supported by cyber analysts who provide technical

expertise and issue alerts and warnings to FAA and DOT staff. According to officials, they conducted risk assessments, performed trend analyses, and developed spot reports and other products, which are shared across the agency. The agency also developed a crisis management handbook which provides senior leaders and supporting personnel with guidance to address cyber disruptions affecting electronic systems.

In addition, FAA officials stated that it used both classified and unclassified tools to track and monitor GPS interference incidents. For example, FAA, DOD's Space Force, and Coast Guard provided detection sensors, while DOD integrated the data into a shared operational picture. The information was shared with U.S. Customs and Border Protection, DOD, and the Texas Department of Public Safety, which helped agencies locate and stop a malicious counter-drone system. Further, North American Aerospace Defense Command officials stated that they collaborated with FAA primarily through information sharing, threat analysis, and contingency planning.

FAA Has Partially Met Six of Eight Leading Collaboration Practices

Ensure Accountability. GAO's leading collaboration practices state that establishing accountability helps agencies encourage participation, track progress, and make needed adjustments. This includes monitoring, assessing, and communicating progress towards shared short- and long-term outcomes.

FAA has partially ensured accountability by monitoring, assessing and communicating progress toward security and operational outcomes related to spectrum cybersecurity affecting the NAS. For example, interagency groups such as CRUCIBLE, ACI, and IRAC have policies and processes that facilitate coordination, information sharing, and in some cases, progress tracking. CRUCIBLE directs operation centers to initiate coordination calls for significant events, designate an incident lead, share information, and provide a unified federal response—supporting real-time monitoring and communication during incidents. FAA officials stated that they evaluate after-action reports and outcomes in different ways depending on factors such as whether the impact was traced back to a service provider and whether the root cause of an incident is known or still under investigation. CISA officials provided an after-action report of a GPS interference event from January 2022 that detailed the event, the response, and additional insight from the investigation. Officials also provided a tabletop exercise from January 2026 on GPS interference run for internal agency components. Similarly, ACI requires executive committee meetings to review accomplishments and conducts regular coordination calls and tabletop exercises to assess progress and identify

improvements. IRAC also directs its subcommittees to coordinate spectrum-related activities, develop guidance, and support emergency preparedness efforts, which contribute to ongoing oversight of activities.

However, FAA's efforts partially align with the leading practice, because certain elements of accountability—particularly consistent monitoring and assessing of outcomes—are missing. Specifically, not all interagency groups have established policies or procedures to assess progress against defined short- or long-term outcomes. For example, although IRAC outlines roles and responsibilities for its subcommittees, its charter does not specify how decisions or outcomes should be monitored or assessed over time.

As a result, FAA lacks comprehensive mechanisms to monitor, assess, and communicate results across all collaborative efforts. Without fully implementing these accountability mechanisms, it may face challenges in assessing progress, making informed adjustments, and effectively managing interagency efforts, increasing the risk of fragmentation and reduced effectiveness in achieving intended outcomes.

Bridge Organizational Cultures. GAO's leading collaboration practices state that addressing differences between diverse organizational cultures can create mutual trust among collaborating participants that is critical to enhancing and sustaining the collaborative effort. Specifically, participating agencies should establish compatible policies, procedures, and other means to operate across agency boundaries.

FAA has partially bridged organizational cultures by establishing compatible policies, procedures, and other means to operate across agency boundaries which can help address differences in organizational cultures and build mutual trust among collaborating partners. Specifically, the agency's participation in groups such as CRUCIBLE, ACI, and IRAC reflects the use of structured policies and procedures that promote consistent communication and coordination. CRUCIBLE has standardized protocols for communication, including required email formats, defined call structures, and designated leadership roles—such as FAA initiating calls and CISA leading them. Similarly, ACI has implemented a communications plan to support unified messaging and timely information sharing among members, while IRAC's bylaws established clear roles, responsibilities, and procedures for subcommittee operations, including meeting conduct and decision-making processes. These efforts demonstrate alignment across agencies within formal collaboration structures.

However, compatible policies and procedures are not consistently established outside these formal interagency groups. For example, DOD and FCC officials stated that information is shared with FAA outside of formal interagency forums, but neither agency had documented policies and procedures defining information-sharing expectations, reporting processes, or coordination protocols. FAA officials similarly stated that there are no formal policies governing information sharing outside of interagency groups. Although FAA officials said the agency's System Operations office is developing a standard operating procedure to address GPS loss-of-service and interference events, they did not provide documentation of this effort.

Without fully established and compatible policies, procedures, or other means of operating across agency boundaries outside of interagency groups, FAA and its partners may face challenges in overcoming organizational differences, thereby reducing the effectiveness and sustainability of interagency collaboration.

Identify and Sustain Leadership. GAO's leading collaboration practices state that strong and sustained leadership provides the authority, support, and decision-making capabilities that allow interagency efforts to function and to facilitate oversight and accountability. This includes establishing shared leadership among one or more agencies, with clearly defined and agreed-upon roles and responsibilities.

FAA has partially identified and sustained roles and responsibilities in interagency groups. For example, within IRAC, the agency is represented on all subcommittees, chairs the Aeronautical Advisory Group, and serves as a member of the Military Advisory Group of the Frequency Assignment Subcommittee. Additionally, IRAC requires member agencies to designate primary representatives and member agencies may appoint alternatives to ensure continuity of participation. Similarly, ACI establishes shared leadership by designating the DOT, DOD, and DHS as tri-chairs of ACI and requires that DHS and DOT appoint representatives from TSA and FAA, respectively. In addition, CRUCIBLE designates FAA's Wide Area Augmentation System Operations Center as its representative, reflecting an identified role within that collaboration. These efforts demonstrate that the agency has taken steps to define leadership roles and responsibilities consistent with the leading practice.

However, mechanisms to sustain leadership over time are not consistently established. For example, while CRUCIBLE identifies the Wide Area Augmentation System Operations Center as FAA's

representative, its policies and procedures do not clearly define leadership roles within that center or establish processes for designating alternates or successors in the event of absence due to the multi-faceted roles these personnel occupy. As a result, leadership continuity and decision-making authority during critical situations may be unclear.

Without clearly defined and sustained leadership structures—including processes for maintaining continuity—interagency groups may face challenges in providing consistent oversight, ensuring accountability, and maintaining effective collaboration over time.

Clarify Roles and Responsibilities. GAO's leading collaboration practices state that by clarifying roles and responsibilities agencies can identify and leverage their strengths, resources, and authorities while helping overcome barriers when working across agency boundaries. Agencies should work together to define and agree on their respective roles and responsibilities, including leadership responsibilities, agency-specific tasks, decision-making processes, and how joint efforts will be coordinated.

FAA has partially clarified roles and responsibilities of participants. Within formal interagency groups such as CRUCIBLE, ACI, and IRAC, FAA and its partners have established specific roles and responsibilities. Specifically, CRUCIBLE designates FAA as being primarily responsible for determining the severity of an event that could impede flight operations, including those that may trigger a Traffic Management Initiative, affect satellite or ground-based augmentation systems, or result in the loss of area navigation at airports without alternative precision navigational aids. Additionally, CRUCIBLE directs members to initiate coordination by contacting FAA's Wide Area Augmentation System Operations Center.

Similarly, ACI establishes shared leadership by designating TSA, FAA, and DOD's lead component as tri-chairs, responsible for representing their respective agencies and providing consensus input to DHS, DOD, and DOT. ACI also defines the role of an executive committee composed of senior officials from these departments, which meets regularly to review progress and coordinate actions. The executive committee is required to represent the interests and missions of their respective departments, coordinate with the relevant Transportation Systems Sector Risk Management Agencies on issues related to their roles and responsibilities, as well as coordinate and collaborate to provide consensus input to DHS, DOD, and DOT. In IRAC, FAA is assigned to

specific subcommittees and chairs the Aeronautical Advisory Group, while the charter outlines the functions and responsibilities of each subcommittee.

However, FAA has not defined roles, responsibilities, or information-sharing expectations outside of formal interagency groups. For example, some non-federal partners reported uncertainty regarding which FAA offices are responsible for addressing spectrum-related issues and the appropriate channels for communicating concerns. FAA officials confirmed that no formal policies exist to define roles and responsibilities outside of interagency groups. Without clearly defined roles and responsibilities across all collaborative efforts, FAA and its partners may face challenges coordinating activities and addressing issues that cross organizational boundaries.

Include Relevant Participants. GAO's leading collaboration practices state that including relevant participants helps ensure that agencies engage not only relevant organizations but also individuals with a stake in the collaborative effort, recognizing that no single entity has the authority, resources, or skills necessary to address crosscutting challenges. This also involves ensuring that participants reflect diverse perspectives and areas of expertise.

FAA includes some diverse perspectives and areas of expertise on spectrum cybersecurity. Interagency groups such as CRUCIBLE, ACI, and IRAC, have established policies and procedures to incorporate stakeholder input. For example, CRUCIBLE allows escalation to a group 2 call, which expands the participation to include subject matter experts, team leaders, or other stakeholders. ACI enables its tri-chairs to invite representatives from member agencies and partners to share information, report on progress, and provide input on emerging issues while also facilitating engagement with non-federal partners. Similarly, IRAC's bylaws permit assistants, consultants, advisors, visitors, or federal and non-federal guests to attend subcommittee and working group meetings when sponsored by a member.

However, FAA has not consistently engaged all relevant stakeholders. For example, FCC officials reported that the agency has not been engaged for continued participation in ACI following the conclusion of an interagency taskforce in 2021. In addition, aviation partners reported challenges with engagement, including limited information sharing, inconsistent communication regarding issue resolution, and a lack of clarity regarding FAA points of contact for addressing spectrum issues.

Aviation partners also noted differences between the data they use and FAA's data, as well as concerns about the agency's incident reporting priorities. Some aviation partners further indicated a desire for greater inclusion in coordination mechanisms, such as CRUCIBLE calls. The lack of aviation partners' participation in CRUCIBLE calls can impact critical and time-sensitive information sharing between industry and government entities, including when organizations have information that can help address new and ongoing disruptions.

FAA officials stated that they include relevant participants through the rulemaking process and interagency groups. According to the officials, the agency incorporates input from agency experts, other federal agencies, and the public through the rulemaking process. Proposed rules are published for public comment through the Federal Register and Regulations.gov. However, FAA does not provide other opportunities for all relevant stakeholders to provide input outside the rulemaking process, such as by ensuring relevant stakeholders are engaged in appropriate interagency groups.

Without consistently engaging all relevant federal and non-federal partners, FAA may not fully incorporate diverse perspectives needed to address crosscutting cybersecurity challenges, increasing the risk of fragmentation and limiting its ability to achieve intended outcomes.

Develop and Update Guidance. GAO's leading collaboration practices state that documenting agreements in formal guidance can strengthen participants' commitment to work collaboratively and enhance accountability for results. This includes establishing and maintaining written agreements that clearly define how the collaboration will operate.

FAA has partially developed and updated written guidance and agreements that defined how collaboration will operate. Interagency groups such as CRUCIBLE, ACI, and IRAC all have established written charters or bylaws to guide their collaborative efforts. For example, the CRUCIBLE charter includes standardized templates for information sharing and call agendas to support consistent coordination. ACI's charter outlines the mission, strategic objectives, scope, and governance structure of the initiative. In addition, ACI has developed the ACI Communications Plan to provide a consistent approach to messaging and engagements within its scope of responsibilities. Similarly, IRAC's bylaws describe the membership, structure, and functions of the committee.

However, FAA does not have formal information sharing agreements with DOD and FCC. DOD officials stated that while they do share information with FAA within the ACI framework, they do not have formal information-sharing agreements outside of ACI or other structured forums. DOD officials added that they were uncertain if there was a clearly defined channel for sharing information outside that framework. Similarly, FCC officials stated that they collaborate through the CRUCIBLE process, as well as constant communication between FCC and FAA, including classified and unclassified meetings, one-on-one and group discussions, and incident response communications. FCC officials noted that although expectations and informal guidance for information sharing exist, FAA and FCC have not established formal agreements governing how they should exchange information. FAA officials stated that there are no formal information sharing agreements outside of the interagency groups.

Without formalized guidance and agreements for collaboration outside interagency groups, FAA may have limited ability to ensure consistency; sustain collaboration over time, particularly during leadership changes; and enhance accountability for results. As a result, gaps in documented collaboration mechanisms may weaken FAA's ability to effectively coordinate with partners and could lead to inefficiencies in information sharing.

Vulnerabilities Exist in Key Aircraft Communication Applications; FAA Faces Challenges Addressing Them

ACARS and CPDLC, two key aircraft communication applications, face cybersecurity threats from interception, spoofing, and denial-of-service attacks through communications resources due to a lack of authentication, unencrypted communication, and protocol design limitations. Further, since ACARS and CPDLC transmit over RF datalinks, they are also vulnerable to spectrum denial attacks including jamming and other forms of interference. FAA has taken some actions to mitigate these vulnerabilities, but challenges remain. Some of these challenges will require actions by industry and other external stakeholders, in coordination with FAA, to fully address.

Cybersecurity Vulnerabilities Exist in ACARS and CPDLC

ACARS and CPDLC are text-based data communication applications used in commercial aircraft and business aviation. ACARS is a data communications messaging service application that delivers messages between pilots and airlines using VHF, HF, and Satellite Communications data links. CPDLC is a data communication application that transmits messages to and from FAA networks and carried over ACARS-based communication service provider networks. It primarily uses VHF Data Link

Mode 2 communication links.[30] Over oceanic routes and remote areas where VHF is unavailable, CPDLC messages are typically transmitted via Satellite Communications using ACARS-based datalink services. This helps reduce voice traffic by delivering text communications between pilots and ATC.

However, ACARS and CPDLC were not initially designed with strong cryptographic protections, and therefore cybersecurity vulnerabilities exist. Communications are generally not encrypted and lack authentication, meaning messages can be intercepted by anyone with the right equipment. In addition, VHF data link communications lack significant and robust security controls; as a result, individuals using devices such as a software-defined radio (SDR) paired with freely available software can transmit or receive signals.[31] These VHF data links also have throughput constraints due to limited channel capacity, making them susceptible to congestion and transmission delays in spectrum dense airspace. VHF data links are also vulnerable to spectrum denial attacks such as jamming.

Because ACARS and CPDLC communications generally lack encryption and authentication, they are vulnerable to interception, spoofing, and flood-based denial-of-service attacks that could disrupt aviation operations.

Interception: Unauthorized users can capture ACARS or CPDLC messages without altering them. While this may not immediately disrupt operations, information—such as flight plans or operational data—could be used to support further attacks. Researchers have observed large volumes of such messages, some containing sensitive information.

Spoofing: A malicious actor can send fraudulent messages that appear to come from a legitimate source, such as from ATC or the Airline Operations Center. While spoofing messages requires technical and procedural knowledge, along with specific timing for transmitting the

[30]VHF Data Link Mode 2 data links is a digital communication system that allows aircraft and ground stations to exchange data over VHF radio frequencies.

[31]An SDR is a radio communication device that uses software to perform functions such as to receive, process, analyze, and transmit radio signals across a wide range of frequencies. Instead of requiring separate hardware for different radio protocols, an SDR uses a computer and programmable software to receive, process, analyze, and transmit radio signals across a wide range of frequencies.

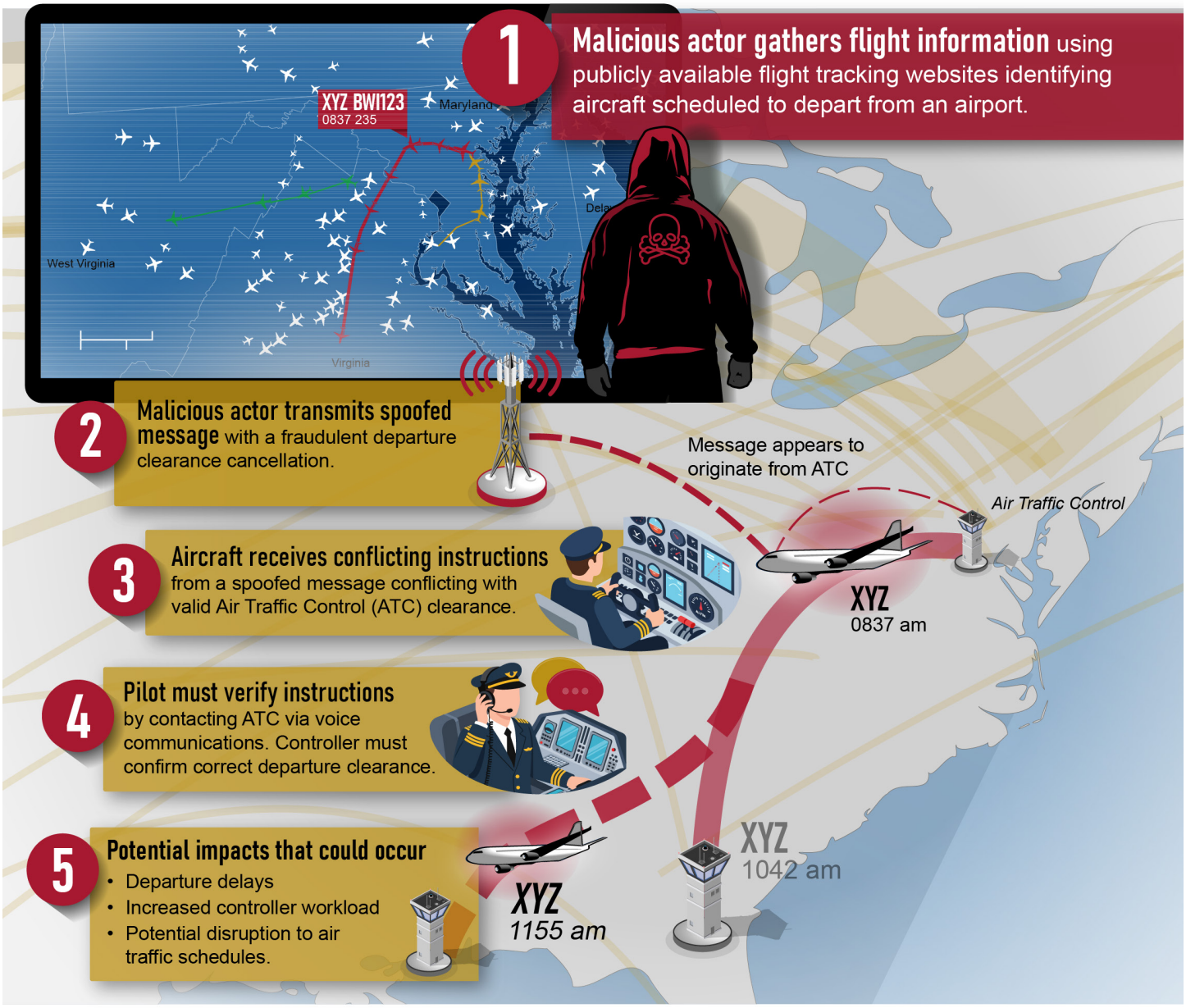
messages successfully, if accepted, these messages could provide incorrect or misleading instructions to pilots.

Flood-based denial-of-service: An attacker can overwhelm communication channels by sending large volumes of messages, potentially disrupting normal communication between the aircraft and ATC. The effects of such an attack are similar to those experienced in very busy airspace due to limited bandwidth.

Potential Attack Scenarios to Cause Flight Delays

A threat actor seeking to cause flight delays could use publicly available flight information regarding a particular aircraft from an airport. For example, the actor could potentially use an SDR to transmit fraudulent CPDLC route modifications, altitude changes, or other clearances that appear to originate from ATC. To do so, the threat actor must operate within limited windows for execution based on close physical proximity and other factors. The pilot, now facing conflicting clearances, would have to verbally confirm and resolve the discrepancy. Resolving these discrepancies could potentially delay flights, and if multiple aircraft are affected, it could increase ATC workload and disrupt airport departure schedules. Additionally, increased workload and confusion for pilots and ATC on the ground could lead to increased safety risks. Figure 6 shows how a threat actor can use an SDR to cause flight delays.

Figure 6: Example of a Spoofed Message that Could Disrupt Flight Operations Cancellation Messages

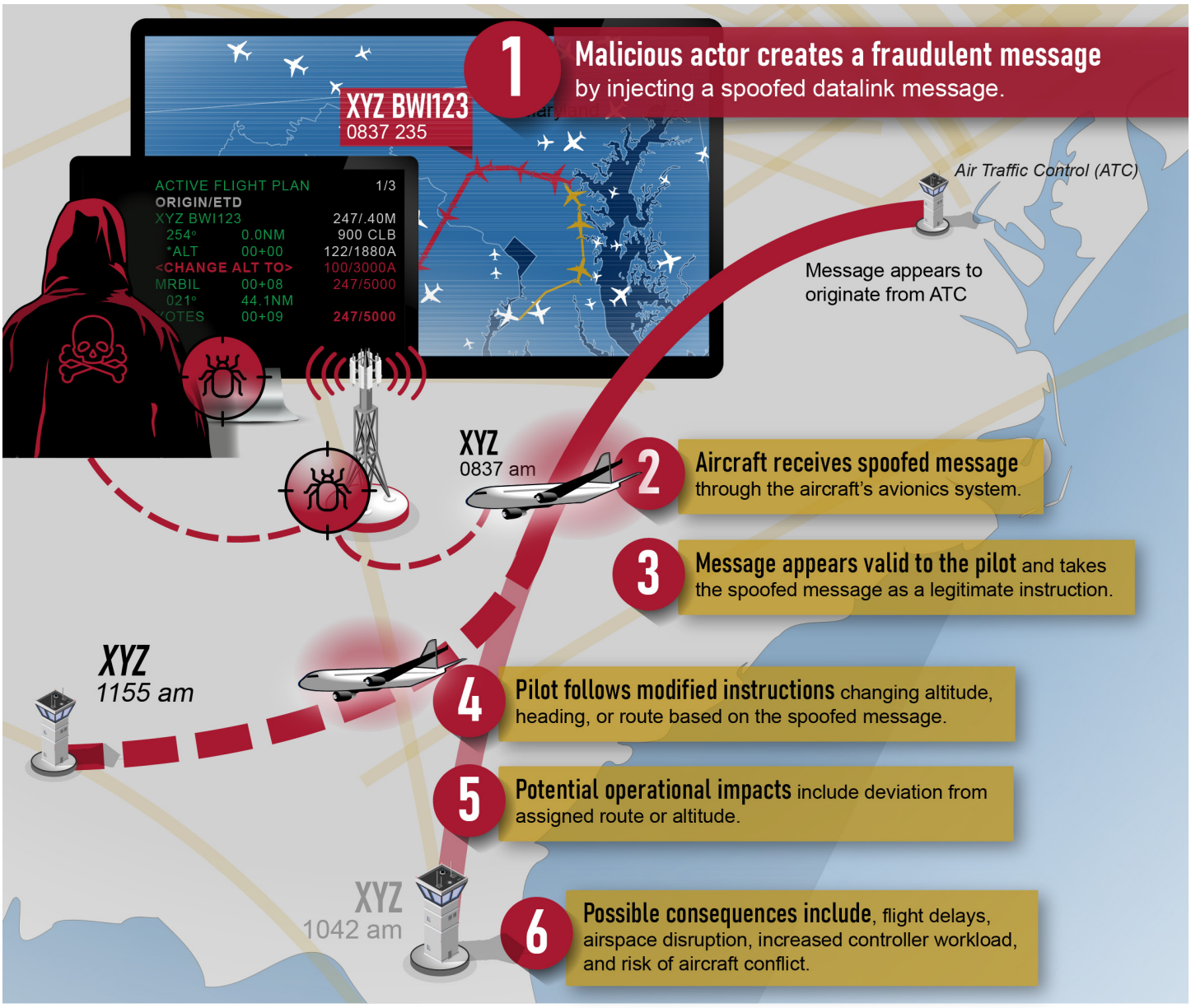


Sources: GAO analysis of Federal Aviation Administration and other documentation; GAO (map, malicious actor, monitor/flight screen, airplane illustrations); TarikVision/stock.adobe.com (towers); gentutgajah/stock.adobe.com (pilot illustrations). | GAO-26-108439

Potential Attack Scenarios to Cause Safety Issues

A threat actor could modify, replay information, or inject ACARS or CPDLC messages that appear to come from a legitimate source such as from the ATC or Airline Operations Center. If the message recipient accepts the message as valid, the pilot may follow the modified instructions or make a flight path decision based on false information resulting in unsafe circumstances for the flight. If multiple aircraft receive such messages, ATCs may need to intervene to resolve the conflicts. Even if the issue is identified quickly, these events could disrupt operations, cause delays, and increase the risk of aircraft collisions. Figure 7 shows how a threat actor could modify messages to pilots resulting in potential flight safety issues.

Figure 7: Example of a Spoofed Message that Could Result in an Unsafe Flight



Sources: GAO analysis of FAA and other documentation; GAO (map, malicious actor, monitor/flight screen, airplane illustrations); Cetacons/stock.adobe.com (icons); TarikVision/stock.adobe.com (towers). | GAO-26-108439

ACARS and CPDLC Lack Authentication and Message Integrity Protections and Rely on Procedural Safeguards to Mitigate Risks

ACARS and CPDLC were developed before modern cybersecurity safeguards became commonplace and lacks common cryptographic protections used to provide authentication, confidentiality, and message integrity. Therefore, both applications rely on a combination of operational procedures and alternative communication methods to reduce security risks. However, these measures were not designed to provide the same level of protection as modern cryptographic controls and may not fully address evolving threats.

For example, ACARS relies on operational and procedural safeguards to help mitigate security risks. For example, flight crews verify information contained in ACARS messages, including the flight identification, aircraft tail number, and message sequence number embedded in the message header before acting on the information. In addition, pilots, dispatchers, and other operational personnel may cross-check ACARS messages against flight plans, aircraft status information, and other communication channels when messages appear unusual or safety critical. Standardized message formats and established operating procedures also help reduce the risk of misinterpretation or unauthorized actions.

Like ACARS, FAA has implemented procedural measures to mitigate certain CPDLC security limitations. CPDLC is used as a supplemental communication method rather than the sole means of communication between pilots and air traffic controllers. When necessary, pilots and controllers can revert to voice communications, which provides an alternative communication path if CPDLC is unavailable or unreliable. In addition, CPDLC procedures restrict its use in time-sensitive or high-risk communications. CPDLC also includes mandatory message acknowledgement, standardized message formats, and strict pre-communication logon requirements. Further, pilots and ATCs review and verify messages before acting, providing additional layers of procedural safeguards against errors or misuse.

However, these safeguards increase operational complexity and could be supplemented by stronger authentication and message integrity protections. Several procedural controls also have inherent limitations. For example, human verification remains susceptible to human error, message correlation does not provide authentication, and syntax validation does not ensure message integrity. In addition, voice communication has limitations including VHF congestion, message misinterpretations, and limited availability in certain remote areas.

Procedural safeguards also require continuous training, rely on inconsistent international standards, and have become more difficult to implement as operational complexity grows. Future autonomous aircraft operations may require additional protection. Implementing stronger authentication and message integrity protections through policy changes, technology implementation, and international standards harmonization would strengthen the security of ACARS and CPDLC and support broader use of digital communications.

As a result, ACARS and CPDLC continue to rely primarily on procedural and multi-channel safeguards, increasing the risk of unauthorized transmissions and message manipulation. Even with additional technical protections, human factors and procedural controls will remain an important component of aviation safety and security.

FAA Has Standards for Enhanced Communication Security, but Faces Challenges in Implementing These Secure Measures

FISMA requires agencies to develop and maintain comprehensive information security programs. In addition, NIST SP 800-53 Rev. 5 calls for federal agencies to protect the confidentiality, integrity, and availability of transmitted information by implementing cryptographic mechanisms to prevent unauthorized disclosure and detect changes during transmission and storage.

FAA stated that new communication standards based on the Internet Protocol Suite (IPS) have been developed to improve the security of aircraft data communications. These standards are intended to replace older communications technologies that were developed decades ago and have limitations related to security, scalability, performance, and interoperability. According to FAA, the new IPS approach would enable aircraft and ATC systems to exchange information using more secure and reliable communications.

FAA officials stated that they are currently testing IPS implementation at select locations and are planning for future deployment; however, FAA has not provided any documented timelines for implementation. The timeline for implementing IPS depends on how quickly airlines can equip the aircraft with the technology and obtain the necessary approvals from the manufacturers and operators. FAA also uses certain existing safeguards, such as the Airline Flight Number login process, which establishes communication between the aircraft and ATC using flight number and aircraft identification. Once connected, an aircraft can send and receive ACARS and CPDLC messages. CPDLC requires both ATC input and flight crew acceptance before taking any action. These

procedures help reduce the likelihood and potential impact of unauthorized or compromised messages.

However, FAA has not fully implemented enhanced cryptographic security measures for applications like ACARS and CPDLC. FAA officials stated that deployment is constrained by the limited availability of compatible aircraft avionics and ground infrastructure that supports these technologies. FAA officials also noted the complexity and cost of coordinating implementation across multiple aviation stakeholders.

Without stronger authentication and message integrity, there is an increased risk that unauthorized parties could send or alter messages, compromising the integrity and authenticity of communication. Greater link capacity is also essential to prevent congestion-based disruptions. Until FAA develops and implements a plan to strengthen these protections, risks such as spoofing, unauthorized transmissions, and message manipulation will persist and could contribute to operational disruptions, including flight delays and potential safety concerns.

FAA Requires Cybersecurity Measures for New Aircraft Technologies Through Certification and Operational Approval Processes

FAA, in collaboration with standards organizations, industry, and other regulators, has established cybersecurity guidance for aircraft system authorization. The guidance covers the protection of information systems and data and defines requirements, roles, and responsibilities aligned with federal standards.[32] Additionally, FAA has proposed a rule for new design standards to address cybersecurity threats and to align cybersecurity requirements for the certification and continued airworthiness of transport category airplanes, engines, and propellers.[33]

FAA addresses cybersecurity measures for new aircraft technologies through its aircraft certification and operational authorization processes. The agency requires applicants to demonstrate and inform FAA of any potential design or technological threats to airworthiness, and to propose and implement mitigations to reduce threats to acceptable levels. FAA does not apply a single set of standardized cyber and technical requirements across all technologies. Aircraft and other aviation products with new designs are generally required to complete FAA's multistep design certification process before the product can be issued an

[32]Federal Aviation Administration, Advisory Circular 119-1A, *Aircraft Network Security Program (ANSP)* (Sept. 28, 2023) and FAA, *FAA Information Security and Privacy: Policy*, Order 1370.121B (Apr. 25, 2022) among others.

[33]89 Fed. Reg. 67564 (Aug. 21, 2024).

airworthiness certificate to safely operate in the NAS.[34] Through this certification process, FAA applies cybersecurity requirements according to the specific risks associated with each technology's design and integration.

FAA evaluates new aircraft technologies through FAA's established aircraft certification processes to ensure they meet safety requirements before being approved for use. This process is risk-based and relies on aircraft manufacturers to identify potential safety and security issues. According to FAA officials in the Aviation Safety office, they incorporate cybersecurity into the broader airworthiness certification process when cyber-related conditions could affect the safe operation of the aircraft. FAA officials further stated that the certification process evaluates whether aircraft systems can continue to operate safely when faced with conditions such as signal loss, degradation, delay, misleading data, electromagnetic interference, or other external disruptions. According to FAA, some risks related to jamming, spoofing, and broader spectrum threats may involve external infrastructure or signal environments outside the aircraft applicant's control and are addressed through other government and industry efforts, such as spectrum protection, navigation resiliency initiatives, and operational mitigations.

During the certification process, aircraft manufacturers submit design information, system architectures, safety assessments, aircraft and system level security risk assessments, and other technical documentation for FAA to review. FAA officials stated that manufacturers are responsible for identifying potential safety and security concerns as part of the certification process, while FAA evaluates whether the proposed design includes appropriate safeguards, resilience, monitoring, and fallback capabilities to maintain safe operations. As part of the Technical Standards Order process, FAA engineers and technical specialists also review to determine whether the proposed design complies with applicable regulations and guidance, which may include FAA policies and procedures as well as other aviation standards such as those issued by the Radio Technical Commission for Aeronautics (RTCA), the International Civil Aviation Organization, and the European

[34]See 49 U.S.C. § 44704.

Organization for Civil Aviation Equipment.[35] For example, FAA's AC 119-1A[36] describes an acceptable means of obtaining operational authorization for aircraft with a special condition related to the security of the on-board network, while RTCA's DO-355 is also accepted as an alternative, depending upon the authorization being sought.[37] FAA may also require additional analyses, testing, or mitigations if the new technologies introduce risks or system interactions.

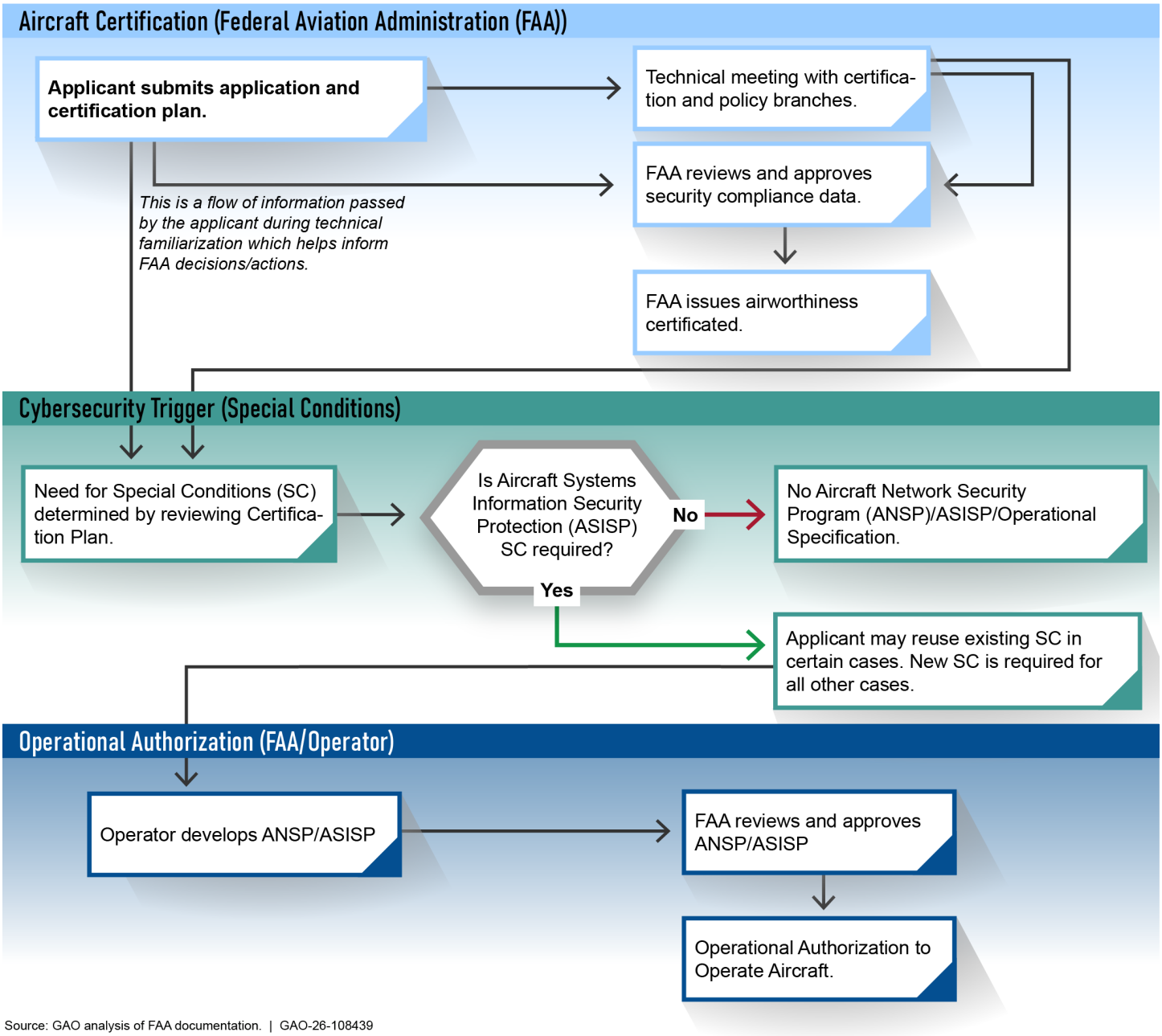
When existing rules do not fully address the characteristics of new technology, such as when systems connect to external or untrusted networks, FAA may impose additional requirements during certification. This process involves evaluating Aircraft Systems Information Security Protection risks associated with the new technology. FAA may establish additional certification requirements, including issuing special conditions, that require applicants to implement design-specific cybersecurity mitigations. These mitigations are based on the system's architecture, connectivity, and defined cybersecurity risks and are evaluated during the certification process. Mitigations may include additional architectural protections, separating critical systems, adding monitoring capabilities, or implementation of other tailored safeguards. Figure 8 illustrates the process of establishing cybersecurity standards for new aviation technologies.

[35]RTCA is a private, nonprofit association comprised of civil aviation authorities and aviation industry stakeholders that develops technical standards often used to demonstrate compliance with government regulations. The International Civil Aviation Organization is a specialized agency of the United Nations that promotes safe, orderly, and efficient development of international civil aviation. International Civil Aviation Organization member nations (i.e., contracting states) agree to cooperate to implement standardized global aviation safety and security measures. The European Organization for Civil Aviation Equipment is the European leader for the development of aviation industry standards.

[36]Federal Aviation Administration, Advisory Circular 119-1A, *Operational Authorization of Aircraft Network Security Program*, (Sept. 28, 2023).

[37]RTCA DO-326, *Airworthiness Security Process Specification* and DO-355A (Aug. 6, 2014), *Information Security Guidance for Continuing Airworthiness* (Sept. 10, 2020).

Figure 8: Process of Establishing Cybersecurity Standards for New Aviation Technologies



Source: GAO analysis of FAA documentation. | GAO-26-108439

In some cases, certification actions may prompt the implementation of Aircraft Network Security Programs (ANSP) as part of the operational authorization process. ANSPs may be needed when cybersecurity-related special conditions require the applicant manufacturer to establish procedures that ensure the continued airworthiness of the aircraft over its lifetime, including against cybersecurity risks. These programs are primarily based on manufacturer guidance and applicable special conditions, with some manufacturers assisting operators in developing ANSPs for more advanced connectivity.[38] FAA reviews the ANSP documentation, and if it is sufficient, approves and monitors the program over time. Cybersecurity measures and requirements for new aircraft technologies vary depending on the system's design, level of connectivity, and risks identified during the certification review process, rather than being based on a single, standardized set of requirements. Under this approach, FAA accounts for cybersecurity measures and mitigations to the specific risks and characteristics of each technology.

Conclusions

The NAS relies on a complex network of aviation systems and communications links to support the safe and efficient movement of aircraft. As these systems become increasingly interconnected, cybersecurity risks have the potential to affect critical aviation communications and operations. Although FAA has not experienced a successful cyberattack resulting in safety impacts, evolving threats increase the importance of protecting these systems.

FAA has identified spectrum-related threats to the NAS and international flight routes, including spectrum interference, spoofing, and jamming. However, gaps in risk assessments, mitigation planning, security documentation, and real-time monitoring capabilities limit FAA's ability to fully understand, detect, and respond to these threats. As a result, disruptions to aviation communications could go undetected or unaddressed, increasing the risk of operational delays, degraded situational awareness, and impacts to air traffic operations.

FAA has undertaken efforts to collaborate with federal and non-federal partners to strengthen defenses against cyber threats. However, shortcomings in interagency coordination and information sharing may reduce the effectiveness of efforts to identify emerging threats, share

[38]Operator refers to a FAA certificated air carrier or commercial operator authorized to conduct operations under 14 CFR Part 119.

threat intelligence, and develop coordinated responses to cybersecurity incidents affecting aviation systems.

In addition, vulnerabilities in ACARS and CPDLC communications remain, and while FAA has identified potential mitigation approaches, they have not yet been consistently implemented. Consequently, these communications may be susceptible to threats such as spoofing and jamming. Exploitation of these vulnerabilities could result in misleading information, increased controller and pilot workload, flight delays, other operational disruptions, and risks to flight safety.

Recommendations for Executive Action

We are making the following nine recommendations to FAA:

The Administrator of FAA should develop a formal risk assessment report that addresses, analyzes, and documents specific risks to the seven of eight identified NAS systems arising from but not limited to threats such as spectrum attacks, spoofing, and jamming. (Recommendation 1)

The Administrator of FAA should conduct a review of system categorization for the one system we reviewed to ensure all system documents are consistent and align with the appropriate system impact level. (Recommendation 2)

The Administrator of FAA should implement capabilities to continuously monitor threats such as interference, spoofing, and jamming to aviation communications links within the National Airspace System. (Recommendation 3)

The Administrator of FAA should, in coordination with partner agencies, develop methods to monitor and assess progress toward short- and long-term outcomes in interagency groups to ensure accountability. (Recommendation 4)

The Administrator of FAA should, in conjunction with partner agencies, develop formal guidance on information sharing outside of interagency groups. (Recommendation 5)

The Administrator of FAA should, in conjunction with interagency partners, describe how leadership roles in interagency groups will be sustained over the long-term, including in the event of resignation, reassignment, or retirement of the individual serving in that leadership role. (Recommendation 6)

The Administrator of FAA should work to clarify the roles and responsibilities for information sharing with non-federal partners outside of interagency groups. (Recommendation 7)

The Administrator of FAA should work with federal and non-federal partners to ensure that all relevant stakeholders are included in FAA's collaborative efforts both within, and outside of, interagency groups. (Recommendation 8)

The Administrator of FAA should, in conjunction with federal and non-federal partners, develop and implement a plan to strengthen authentication and data protection for ACARS and CPDLC communications to mitigate risks of spoofing, unauthorized transmissions, and message tampering. (Recommendation 9)

Agency Comments

We provided a draft of this report to DOT, DHS, DOD, Commerce, and FCC for their review and comment. DOT, the agency to which we made recommendations, provided written comments which are reprinted in appendix II. DOT concurred with all nine of our recommendations. DOT stated the agency is strengthening its risk assessment process to ensure it reflects the current threat landscape and leverages relevant guidance. The agency also noted that the Aviation Cyber Initiative will seek to enhance outreach efforts across the aviation ecosystem and added FAA will continue collaboration across industry and government to identify and mitigate emerging risks to the NAS.

Of the four agencies to which we did not make recommendations, DOD, Commerce, and FCC did not have any comments on the report. DHS and DOT provided technical comments, which we have incorporated as appropriate. In addition, each of the agencies conducted a sensitivity review of the information contained in this report and did not identify any sensitivity concerns.

We are sending copies of this report to the appropriate congressional committees, the Chaiman of the Federal Communications Commission, the Secretary of Commerce, the Secretary of Defense, the Secretary of Homeland Security, Secretary of Transportation, the respective Offices of Inspector General for these departments, aviation stakeholders, 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 III.

//SIGNED//

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

List of Addresses

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

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

The Honorable Tom Cotton
Chairman
The Honorable Mark Warner
Vice Chairman
Select Committee on Intelligence
United States Senate

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

The Honorable Rick Crawford
Chairman
The Honorable Jim Himes
Ranking Member
Permanent Select Committee on Intelligence
House of Representatives

The Honorable Sam Graves
Chairman
The Honorable Rick Larsen
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 Federal Aviation Administration (FAA) has identified and mitigated spectrum-related cybersecurity threats to the National Airspace System (NAS) and international flight routes; (2) the extent to which FAA has collaborated with federal partners to strengthen defenses against cybersecurity threats; (3) what specific cybersecurity vulnerabilities exist in key communication applications, including the Aircraft Communications Addressing and Reporting System (ACARS) and the Controller Pilot Data Link Communications (CPDLC), and to what extent FAA has addressed them; and (4) what cybersecurity measures FAA requires for new aircraft technologies to reduce potential vulnerabilities.

To address our first objective, we analyzed threat and vulnerability assessments of FAA communication datalinks and conducted interviews with cognizant officials to identify spectrum related threats to the NAS and to see how they were mitigating such threats. We selected eight spectrum dependent systems that are critical to the NAS for review.[1] These systems rely on radio frequency (RF) signals for essential functions such as communication, navigation, surveillance, and air traffic management functions. These eight systems also enable aircraft and air traffic controllers to exchange information and maintain situational awareness throughout air traffic operations.

We assessed the eight NAS system's authorization-to-operate packages against selected controls from the National Institute of Standards and Technology (NIST) to identify gaps in security controls. In addition, we assessed the eight systems' authorization-to-operate packages against the FAA Security Authorization Handbook to identify instances of misalignment with FAA policy. Specifically, we reviewed FAA security assessment reports which convey assessment results, including vulnerability scans, independent testing, and control effectiveness evaluations along with finding and corrective action recommendations for identified control weaknesses. In addition, we reviewed FAA vulnerability assessments and a general risk assessment that addressed threats, likelihood, and impact.

To address our second objective, we reviewed aviation cybersecurity responsibilities shared across FAA, Department of Defense (DOD), Department of Homeland Security (DHS), Federal Communications Commission (FCC), and other stakeholders. Accordingly, we used GAO's

[1]We did not include the names of the eight systems due to sensitivity concerns.

leading practices for interagency collaboration as criteria for evaluating FAA's collaborative efforts.[2] We compared documentation of key FAA collaboration mechanisms, including interagency groups, against GAO's eight leading practices for interagency collaboration. We assessed the collaboration mechanism against these leading practices including:

- defining common outcomes;
- ensuring accountability;
- bridging organizational cultures;
- identifying and sustaining leadership;
- clarifying roles and responsibilities;
- including relevant participants;
- leveraging resources and information, and
- developing and updating written guidance and agreements.

Specific documentation that we compared against these leading practices included the Aviation Cyber Initiative charter and Communications Plan; meeting minutes and presentations from information sharing meetings involving FAA and other agencies and organizations; Interdepartmental Radio Advisory Committee documentation; and CRUCIBLE process documentation. We compared this documentation to the leading practices for interagency collaboration to determine the extent to which FAA's collaborative efforts addressed them. We assessed FAA against the eight key practices and rated each practice as fully, partially, or not met. For each practice, we evaluated the supporting evidence and determined the extent to which FAA implemented the activities associated with that practice:

- fully met—FAA provided evidence which showed that it fully or largely addressed the elements of the leading practice.
- partially met—FAA provided evidence that showed it had addressed at least part of the leading practice.
- not met—FAA did not provide evidence that it had addressed any part of the leading practice.

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

To address the third objective, we assessed outage and incident reports along with other FAA documentation to identify cybersecurity risks and vulnerabilities of ACARS and CPDLC. We also reviewed academic publications that described vulnerabilities associated with ACARS and CPDLC. We reviewed documents to see whether mitigation existed for these vulnerabilities.

To address the fourth objective, we reviewed FAA documents describing the process of establishing cybersecurity measures for new aviation technologies. The policies and documentation we reviewed included the certification process, aircraft-specific regulatory requirements called special conditions, Aircraft Network Security Programs, and other policy documents and guidance from FAA, Radio Technical Commission for Aeronautics (RTCA), and the International Civil Aviation Organization.

For all four objectives, we either met with or received written responses from FAA officials in the offices of Aviation Security, Data Communications, Spectrum Engineering, Voice and Enterprise Data Control, National Security Programs and Incident Response, Aviation Security, and Safety and Hazardous Materials. We also interviewed officials from DOD's Space Force; the Department of Commerce's National Telecommunications and Information Administration; DHS's Cybersecurity and Infrastructure Security Agency; and FCC. These officials provided insight into the radio frequency threats posed to the NAS, collaboration efforts, ACARS and CPDLC vulnerabilities and mitigations, and information on how cybersecurity requirements are identified, defined, and implemented for new aviation technologies. Finally, we conducted site visits to the Air Route Traffic Control Center in Leesburg, Virginia and the Air Traffic Control System Command Center in Warrenton, Virginia to interview staff and tour the facility to understand the operations of these systems and how threats are mitigated.

We also selected a non-generalizable sample of 21 aviation stakeholder groups and either conducted semi-structured interviews or received questionnaire responses from them. Of those 21 stakeholders, 13 responded to our meeting request. The remaining 8 either did not respond or stated that they were unable to assist us. To save time, we leveraged a prior GAO team's sampling methodology for the aviation stakeholder groups based on their knowledge on the transition from ground-based radar systems to a system based on satellite navigation methodology. We used the same set of questions for each aviation stakeholder and tailored a few group's questions based on their expertise and involvement in the NAS. We conducted a high-level content analysis

based on the responses we received and identify key themes which we incorporated in the report as appropriate. While we received several comments from aviation stakeholders, we only incorporated those that were within the scope of our review and supported by sufficient evidence. We did not incorporate comments that could not be independently verified or that were not raised or substantiated by FAA officials.

We conducted this performance audit from April 2025 to September 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.

Appendix II: Comments from the Department of Transportation

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

Assistant Secretary for Administration

1200 New Jersey Avenue, SE
Washington, DC 20590

July 30, 2026

Jennifer Franks
Director, Physical Infrastructure
U.S. Government Accountability Office (GAO)
441 G Street N.W.
Washington, D.C. 20548

Dear Ms. Franks:

The Federal Aviation Administration (FAA) remains committed to safeguarding the National Airspace System (NAS) while supporting the integration of next-generation aviation technologies. As aircraft and flight operations become more interconnected, cyber and electromagnetic vulnerabilities pose increasing risks to critical systems, including air traffic control, data communications, and avionics. To address these threats, FAA is strengthening its risk assessment process to ensure that it reflects the current threat landscape and leverages relevant guidance. The agency analyzes avionics systems, investigates interference, develops and procures monitoring tools, and provides technical analysis to inform spectrum policy and criteria. In addition, the interagency Aviation Cyber Initiative will enhance outreach efforts to ensure broad representation across the ecosystem. FAA will continue collaborating with industry and government partners to identify and mitigate emerging risks to the NAS, including denial-of-service attacks and spectrum interference.

Upon review of GAO's draft report, we concur with the nine recommendations issued to strengthen FAA's management of spectrum-related cybersecurity risks, enhance collaboration, and improve the security of aviation communication applications. We 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,

Keith Washington
Deputy Assistant Secretary for Administration

On behalf of
Dr. Anne Byrd
Assistant Secretary for Administration

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contacts

Jennifer R. Franks, FranksJ@gao.gov

Staff Acknowledgments

In addition to the contact named above, the following staff made key contributions to this report: Saar Dagani (Assistant Director), Tammi Kalugdan (Assistant Director), AJ Yohn (Analyst-in-Charge), Luis Alicea, Joseph Andrews, Tasha Beyzavi, Chris Businsky, Ryan Fetrow, Jonnie Genova, Elizabeth Harris, Anh-Thi Le, Jacob Leehy, Julia Munroe, Koushik Nalluru, Zsaroq Powe, Kirpal Sukumar, and Walter Vance.