

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

GAO-26-108439

September 2026

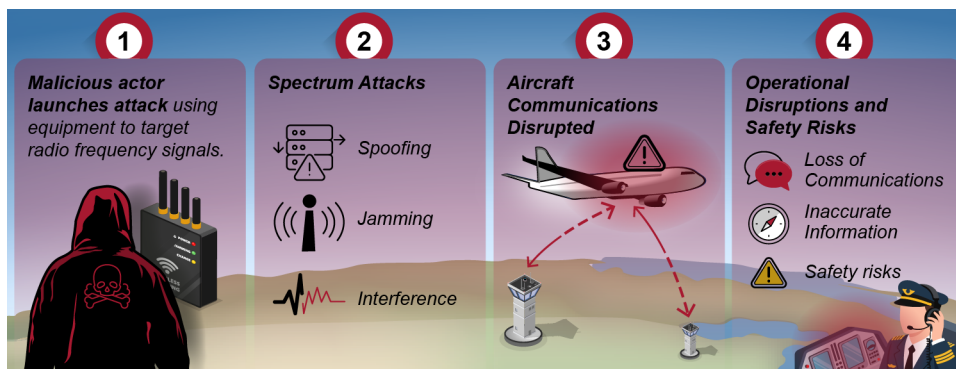
A report to congressional committees

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.