CSC 2.0

Turbulence Ahead: Navigating the Challenges of Aviation Cybersecurity

Jiwon Ma

Executive Summary

The aviation industry in the United States encompasses a vast network of nearly 20,000 airports and almost 7,000 aircraft.[1] Ensuring flight safety by protecting this critical subsector from cyberattacks is vital to safeguarding the nation's economic vitality and national security.

The aviation subsector is a complex ecosystem comprising not only airlines and their aircraft but also airport operating authorities and the air traffic control system. Each of these elements faces unique cybersecurity risks and challenges. This interconnected industry manages a wealth of sensitive data, including passenger information, financial records, and proprietary details of advanced technologies. This makes the industry an attractive target for cyberattacks.

In addition to compromising data integrity, confidentiality, and availability, cyberattacks and technology disruptions can impair flight navigation and communication channels crucial for both civil and military aviation operations. While policymakers and industry leaders increasingly recognize these vulnerabilities, relevant federal agencies and industry stakeholders face significant hurdles to addressing evolving threats. These challenges include fragmented oversight, insufficient investment in cybersecurity and modernization, and an under-resourced workforce.

The aviation subsector is a significant driver of economic productivity. Less understood but equally important is the industry's crucial role in U.S. military mobility. The military relies on aviation infrastructure to move forces, equipment, and supplies essential for deterring adversaries and winning wars. Given the industry's dual importance, the numerous shortcomings identified in this report — ranging from inefficient cybersecurity regulatory oversight to gaps in workforce training — demand swift and coordinated action from the executive branch, Congress, federal agencies, and industry stakeholders.

This report is divided into five sections. The first discusses the aviation industry's vital role in the U.S. economy. The second explores the importance of aviation critical infrastructure for military mobility. The third examines the subsector's multifaceted operational and cyber landscape. The fourth provides an overview of current federal government efforts, led by the Federal Aviation Administration and Transportation Security Administration, to address the cybersecurity challenges in the subsector. The report concludes with key insights and recommendations for policymakers, emphasizing the need to strengthen cybersecurity capabilities, advance workforce development, enhance stakeholder collaboration, modernize industry technologies, and improve interagency coordination to bolster the industry's resilience against emerging cyber threats.

[1] U.S. Department of Transportation, Bureau of Transportation Statistics. "Number of U.S. Aircraft, Vehicles, Vessels, and Other Conveyances," June 2, 2023. (https://www.bts.gov/content/number-us-aircraft-vehicles-vessels-and-other-conveyances)

The views of the authors do not necessarily reflect the views of CSC 2.0's distinguished advisors, senior advisors, or any affiliated organizations or individuals.

CSC 2.0 is preserving the legacy and continuing the work of the Cyberspace Solarium Commission For more information, visit **www.CyberSolarium.org**