CSC 2.0

April 2025

Turbulence Ahead: Navigating the Challenges of Aviation Cybersecurity

Jiwon Ma

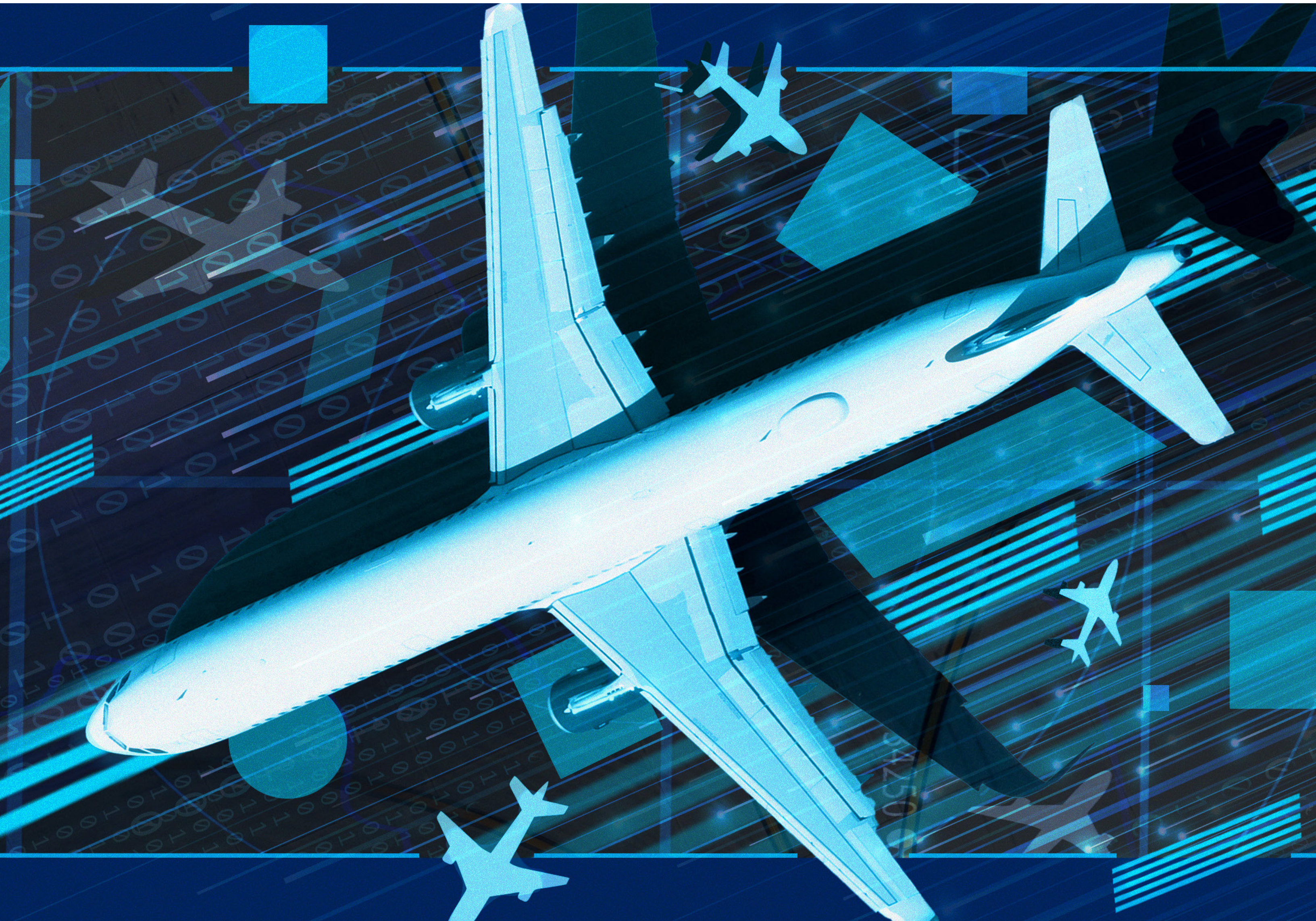
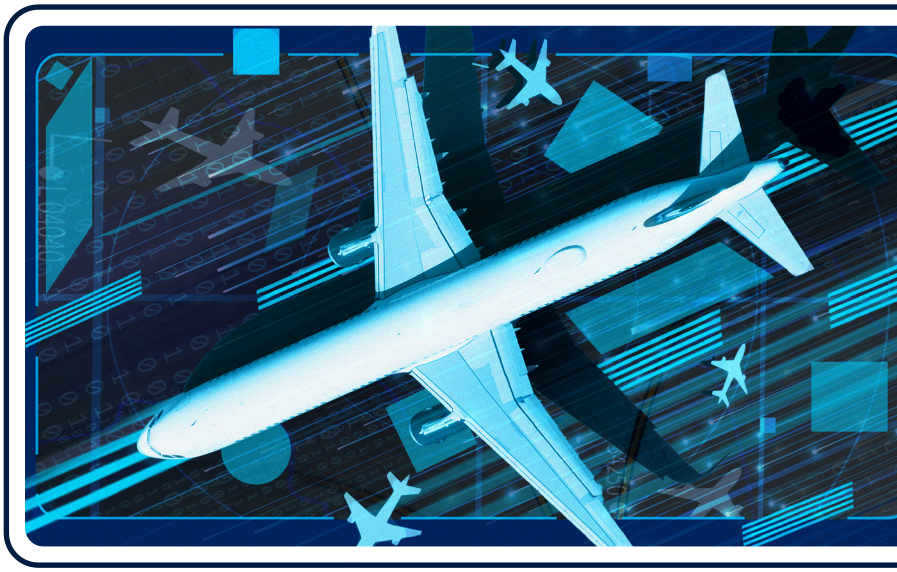


Table of Contents

Executive Summary



An FDD design collage by Lilia Gaufberg featuring an aerial view of a narrow-body aircraft departing airport runway (Thiago B Trevisan via Shutterstock)

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.

The Economic Importance of Air Transportation

The aviation subsector includes commercial airlines, air cargo carriers, airports, aircraft manufacturers, and supporting infrastructure and companies, such as maintenance and repair service providers. It accounts for roughly 5 percent of U.S. gross domestic product and plays a crucial role in ensuring timely delivery of people and goods. Each day, U.S. commercial airlines transport approximately 2.9 million passengers and 61,000 tons of cargo across the United States and around the world.[2]

The aviation industry has recovered rapidly from the COVID-19 pandemic, fueled by a sharp increase in passenger demand for air travel. In 2024, the Transportation Security Administration (TSA) reported a 6 percent increase in the daily average volume of passengers passing through security checkpoints compared with 2023.[3] This bump followed a 14 percent rise in passenger volume in 2022.[4] With over one billion travelers in 2023, airlines filled an average of 83 percent of available seats per flight.[5] This combination of increased demand and improved seat utilization boosted airlines' net profits from $1.63 billion in 2022 to $7.8 billion in 2023.[6]

In today's fast-paced global market, air cargo transportation offers a unique advantage over maritime, rail, and trucking, providing unmatched speed, reach, and reliability. While trucking and rail account for a dominant 70 percent share of domestic freight volume, they require longer transit times.[7] Air freight is costlier but reduces transit times down from weeks to days. This makes it essential for transporting high-value, time-sensitive goods, such as pharmaceuticals and other critical manufacturing parts, particularly when other transport modes face capacity constraints.[8]

During the pandemic, air freight proved essential amid severe disruptions in global maritime shipping. It delivered medical equipment, personal protective gear (PPE), and vaccines worldwide, preventing shortages and alleviating strain on healthcare systems.[9] For example, between January 2020 and March 2021, FedEx Express — the mail carrier's overnight air freight service — delivered more than 80 kilotons of PPE globally on behalf of the Department of Health and Human Services. Between March and November 2020, FedEx also flew 132 flights to transport more than 10 tons of PPE and vaccines to all 50 states and more than 25 countries.[10]

During the 2021 global semiconductor shortage, air freight played a crucial role in safeguarding supply chains. Aircraft swiftly transported temperature-sensitive components in climate-controlled environments, ensuring timely delivery of raw materials needed for semiconductor chip production. This prevented further slowdowns in critical sectors such as electronics and automotive manufacturing — delays that slower transport modes, such as maritime shipping, could not have mitigated.[11] These cases highlight air freight's vital role in maintaining global supply chain stability during one of the most volatile economic periods in recent history.[12]

Air freight also enables businesses to adapt quickly to market demand, enhancing supply chain elasticity, supporting efficient restocking, and lowering capital and overhead costs by reducing the need for high inventory levels. It also plays a key role in sustaining business continuity and driving the rapid growth of global e-commerce. In the fourth fiscal quarter of 2024, U.S. e-commerce sales surged to $308.9 billion, surpassing the previous quarter by 2.7 percent and marking the highest quarterly performance in history.[13] With growing demand for faster shipping, e-commerce now accounts for roughly 20 percent of global air freight volume,[14] underscoring the aviation industry's importance in facilitating global trade, maintaining efficient supply chains, and meeting consumer expectations.

> ***"Each day, U.S. commercial airlines transport approximately 2.9 million passengers and 61,000 tons of cargo across the United States and around the world."***

Military Mobility

Beyond its importance to economic prosperity, the commercial aviation industry plays an indispensable role in supporting the U.S. military. Though the military of course has its own transport aircraft and airfields, it relies in part on commercial airlines and civilian and joint-use airports for military logistics. Threats to the American commercial aviation industry therefore could imperil U.S. national security.

Civil Reserve Air Fleet

Commercial airlines play an important role in enabling efficient and timely delivery of personnel, supplies, and equipment to sustain Department of Defense (DoD) missions worldwide. While the military possesses its own aircraft, partnering with civilian commercial airlines expands the available air transportation and airlift capacity that can be activated quickly. For instance, in the nine months following Russia's 2022 invasion of Ukraine, contracted commercial airlines flew more than 820 national security-related missions to deliver essential weapons and equipment for Ukrainian forces.[15] The military's reliance on the commercial aviation industry, however, means that any disruption in that industry could directly impair the Pentagon's ability to maintain operational readiness across multiple theaters.

U.S. Transportation Command (USTRANSCOM) is the functional combatant command responsible for planning and conducting global mobility operations spanning air, land, and sea transportation modalities.[16] Alongside the Department of Transportation (DoT), USTRANSCOM collaborates with civilian commercial airlines through the Civil Reserve Air Fleet (CRAF) program. The CRAF program provides designated, mission-ready aircraft within 24 to 48 hours to meet surges in demand for emergency airlift operations. Twenty-five airlines currently participate in the program, together providing 450 aircraft, or 6 percent of the total cargo and passenger aircraft in service in the United States.[17]

During Operations Desert Shield and Desert Storm (1990-1991),[18] Operation Iraqi Freedom (2003),[19] and Operation Allies Refuge (2021), CRAF aircraft played an essential role in transporting troops and cargo and evacuating refugees.[20] CRAF extends USTRANSCOM's reach and enhances mission flexibility by reducing the time and DoD resources typically needed for large-scale mobilization of troops and materiel. [21] Moreover, CRAF allows USTRANSCOM to avoid fixed costs associated with maintaining a large military-only fleet. For instance, CRAF saved the Air Force an estimated $13 to $50 billion during Operation Desert Storm.[22]

Civilian and Joint-Use Airfields

Civilian and joint-use airfields are also a critical component of the U.S. military's ability to mobilize forces. Joint-use airfields refer to shared operational arrangements between military and civilian aviation. There are two categories of such airfields. The first constitutes military installations that allow civilian aircraft activity — such as Charleston Air Force Base — with 21 such installations in operations as of 2022.[23] The second constitutes civilian airports that allow military use for operations, totaling 69 civilian airports as of 2022.[24] The DoD Policy Board on Federal Aviation works with the FAA to coordinate and streamline military and civilian aviation operations, optimizing flight efficiency and reducing the need for separate military airfields.

By leveraging civilian infrastructure, the Pentagon reduces the need for public investment in additional military airfields. These partnerships are crucial for cost savings, operational flexibility, and responsiveness.[25] Strategically located civilian airports provide ready access to international and domestic routes, facilitating the efficient transport of military assets and personnel. This integration also supports military training, testing, logistics, and disaster-response operations.

The benefits are not just one-sided. The DoD and FAA work together to ensure the capacity of the National Airspace System (NAS) to meet both military and civil aviation needs.[26] The Policy Board on Federal Aviation's coordination with the FAA plays a critical role in optimizing shared systems such as Global Positioning System (GPS) and communication networks, enhancing air traffic management and ensuring safety and performance within the NAS. This partnership helps improve navigational planning, reduce delays, identify direct routes, and facilitate smoother altitudes transitions, ultimately saving time and fuel.

Threats to U.S. Military Mobility

While the U.S. military's use of commercial airlines and civilian infrastructure offers numerous advantages, it also expands cybersecurity vulnerabilities.[27] One risk concerns potential compromises in the supply chains of commercial airlines. To mitigate this risk, the DoD's 2024 defense-industrial base strategy emphasizes strengthening the cybersecurity of its contractors, including key aviation suppliers such as Boeing. As part of this effort, the DoD's Defense Cyber Crime Center offers voluntary assessments through its Cyber Resilience Analysis service. These assessments identify vulnerabilities within the defense-industrial base, including the aviation supply chain, and share actionable intelligence with participating vendors.[28]

In addition, while civilian and military aviation maintain separate systems for handling passenger and cargo information and employ different communications systems,[29] both rely on the same Air Traffic Control (ATC) system for communication between aircraft and ground control. The ATC system ensures that both commercial and military aircraft can communicate with the ground and with each other in shared airspace. As a result, cyber threats targeting the ATC system jeopardize both civilian and military aviation.

A cyber incident targeting commercial airlines, commercial airport operating authorities, or even the ATC system itself could potentially disrupt DoD computer networks, causing schedules and dispatch logistics to go awry. Such incidents could diminish DoD's mission readiness and ability to coordinate resources for deployment. Additionally, adversaries may attempt to infiltrate shared communication systems used for both civilian and military purposes, potentially exfiltrating intelligence or disrupting military operations. Similarly, these cybersecurity incidents could lead to prolonged operational outages and substantial financial losses in the civilian aviation industry.

Operational Landscape

Despite its critical importance, the aviation industry is prone to disruptions. Delays caused by cyber incidents, supply chain disruptions, and other malicious attacks can cause significant financial losses. Likewise, delays due to weather, mechanical problems, accidents, and other incidents cost airlines, passengers, and industries dependent on air travel a total of $33 billion in 2019.[30] These losses include the financial impact of lost future business as well as disruptions in industries relying on just-in-time operations, where delayed deliveries can halt production lines on a global scale.[31] In the aviation industry, supply chain delays can hinder timely maintenance, fleet expansion, and essential technology and cybersecurity upgrades for operational efficiency. For instance, in December 2024, the International Air Transportation Association estimated that clearing the backlog of 17,000 delayed aircraft deliveries will take approximately 14.8 years.[32] Such prolonged delays leave the aviation industry relying on aging systems, amplifying the risk of emerging cyber threats.

Growing Cyber Threats

The aviation industry has become a prime target for increasingly sophisticated cyberattacks. These attacks exploit the subsector's intricate web of global operations and its critical role in global supply chains, where even a single disruption can ground flights, delay cargo, and send shockwaves through economies.

Ransomware, in particular, has emerged as a top threat confronting the industry. Overall, the number of cyberattacks affecting the aviation industry increased by 131 percent in 2023 compared with 2022.[33] The number of ransomware incidents, which are a subset of total attacks, surged even more dramatically — by 600 percent in 2023, according to a senior executive at Boeing.[34] Boeing itself suffered a ransomware attack in October 2023 but reportedly did not pay the exorbitant sum the hackers were demanding.[35]

Ransomware is particularly damaging because of the cascading impacts it can have on an industry heavily reliant on intricate communications systems. In November 2022, hackers caused flight delays when they launched a ransomware attack targeting Jeppesen, a Boeing subsidiary. Jeppesen supplies flight navigation and operation planning tools used by airlines and aviation authorities to plan safe and efficient routes. Jeppesen's tools also feed into the national Notice to Air Missions (NOTAM) system, which warns pilots and airlines of hazards on their planned routes.[36] The disruption affected flight planning across multiple carriers contributing to delays, illustrating how an attack on a single service provider can affect the broader aviation ecosystem.

More recently, in August 2024, Seattle-Tacoma International Airport suffered a ransomware attack that disrupted essential airport operations just ahead of a busy Labor Day travel rush. Airport staff quickly switched to manual processes, handling over 7,000 pieces of luggage and issuing paper boarding passes to keep operations running.[37] The attack strained airport logistics and passenger processing, demonstrating how ransomware can disrupt interconnected airport systems during peak demand. The Russian-affiliated Rhysida group demanded $6 million in ransom to decrypt the systems and avoid data leaks. However, rather than paying the ransom, airport authorities worked closely with the FBI and the Cybersecurity and Infrastructure Security Agency (CISA) to restore most operations within a week.[38] In subsequent Senate testimony, Lance Lyttle, the airport's aviation managing director, credited close coordination with the FBI, CISA, TSA, Customs, and airline partners with minimizing passenger disruption.[39]

The aviation industry is no stranger to data breaches. In 2018, British Airways and Hong Kong's Cathay Pacific suffered data breaches affecting nearly 10 million customers, resulting in fines exceeding $230 million.[40] In June 2020, hackers stole 1.5 terabytes of sensitive data from VT San Antonio Aerospace, an aviation maintenance firm.[41] By 2023, Air France-KLM, Scandinavian Airlines, and Sabre, a U.S.-based travel booking service provider, all reported data breaches compromising customer information.[42] That same year, Texas-based third-party recruiter Pilot Credentials also fell victim to a cyberattack in which hackers exfiltrated sensitive data of nearly 9,000 pilots and job applicants from American Airlines and Southwest Airlines.[43]

Geopolitical tensions have contributed to the cyber threats facing the aviation industry. In 2022, in retaliation for Western sanctions against Russia over its invasion of Ukraine, pro-Russia hacktivists overwhelmed the websites of airports in Atlanta, Los Angeles, Chicago, and other cities, temporarily knocking them offline. While these cyberattacks did not affect flight operations, they prevented travelers from accessing the websites for travel updates and airport services.[44] This was not the first time Russian-linked actors have targeted the aviation infrastructure. In March 2020, the Russian state-sponsored group Dragonfly breached San Francisco International Airport's websites, gaining access to sensitive data, including the credentials of employees and airport construction contractors.[45]

The aviation industry's globally distributed supply chain increases the subsector's vulnerability to cyber threats. An October 2020 report by the Government Accountability Office (GAO) identified several key areas of vulnerability within this supply chain: insufficient security among various suppliers, outdated systems on legacy aircraft, and the risk of malicious software being introduced during manufacturing or maintenance.[46] Malicious actors can exploit these weak points, potentially compromising the integrity of aircraft components or systems used by both commercial and military operators.[47] For instance, during production or software update phases, hackers could infiltrate a supplier's network to insert malware into key systems, such as flight management or navigation systems, allowing malware to propagate across the aviation networks.[48]

In addition, the heavy reliance by airports on other critical infrastructure introduces further risks. For instance, a disruption to fuel supplies can upend operations at affected airports, since options for alternative supplies are often limited. The high-profile ransomware attack on Colonial Pipeline in 2021 highlighted this vulnerability. The attack resulted in fuel shortages at East Coast airports, causing flights to be canceled or rerouted.[49]

Modernizing Legacy Systems

The aviation industry relies on a host of computer systems to support operations. For example, airlines use various platforms to manage bookings, fleet logistics, and transactions with third-party vendors. ATC systems are also critical to ensuring the safe and orderly movement of aircraft. In addition, airports rely on technology for handling baggage, screening passengers, operating security checkpoints, and managing terminals. Together, these systems form a complex ecosystem, where a cyber incident in one area could disrupt operations in others.

Unfortunately, many of these systems are outdated and lack the flexibility to adapt to emerging threats. While airline-specific failures often stem from poor investment decisions, such as neglecting to replace outdated inventory or scheduling systems, the broader concern lies in the systemic risks posed by aging foundational infrastructure such as ATC systems.

Airline Operational Resilience

Even the most advanced aviation operations can be brought to a standstill by a single point of failure. Recent incidents have demonstrated this stark reality.

In December 2022, Southwest Airlines experienced a major operational breakdown that resulted in nearly 17,000 canceled flights and left 2 million passengers stranded during the peak holiday travel season.[50] While the cancellations were triggered by inclement weather, the root cause was the failure of Southwest's inventory tracking system, which relied on software more than three decades old.[51] Overwhelmed by a surge in rebooking requests, the system forced crew members to manually update critical information on available seats, fleets, and crew assignments, severely limiting the airline's ability to reroute passengers.[52] This incident not only impacted customer satisfaction and the airline's reputation but also had significant financial repercussions. In that quarter alone, Southwest reported $410 million in operating revenue losses, highlighting the steep cost of relying on legacy systems.[53]

In July 2024, a faulty update issued by cybersecurity firm CrowdStrike crashed 8.5 million Windows devices, including devices used by airports around the world. Delta, which relied on CrowdStrike for its traffic and crew assignment management systems, was hit particularly hard.[54] Chaos ensued at Delta's largest hubs, leading to over 5,500 canceled flights — two-thirds of all flight cancellations globally.[55]

A July 2024 study by SecurityScorecard, a cybersecurity firm, underscored the risk of systemic disruptions. The study found that aviation-specific software and IT vendors scored the lowest in cybersecurity readiness across industries. While all sectors face significant cybersecurity risk from software and IT support supplied by third-party vendors, the aviation industry feels the impact of widespread disruptions more acutely due to its reliance on a small pool of key providers serving most airlines and airports.[56] This heavy concentration means that a disruption affecting one provider can impact operations globally, which is exactly what happened in the CrowdStrike incident.

Safeguarding the National Airspace System

Cybersecurity vulnerabilities in individual companies and organizations are only part of the risk. The broader NAS infrastructure lacks the technological resilience required for modern aviation operations.[57] The NAS encompasses all components of U.S. airspace, including air traffic control towers, navigational aids, and airports. ATC systems form the backbone of the NAS. They coordinate flight paths, maintain safe distances between aircraft, monitor weather conditions, conduct surveillance, and facilitate effective communication between pilots and air traffic controllers. However, these systems are alarmingly outdated.

Any disruption in the NAS has the potential to cripple the movement of aircraft. For example, in January 2023, a major outage in the FAA's NOTAM system shut down the NAS, which grounded commercial flights across the country for two hours and caused hundreds of delays and cancellations.[58] The incident was not caused by a cyberattack but by a contractor accidentally deleting files while synchronizing a live database related to a key pilot safety system and its backup. Still, the damage was severe.[59] An FAA official described the incident as "an honest mistake that cost the country millions."[60]

Following that incident, a GAO audit revealed that 105 out of the FAA's 138 ATC systems are outdated and vulnerable to critical failures.[61] The audit found 51 of those systems to be "unsustainable," meaning they are no longer cost-effective to maintain. Another 54 systems were deemed "potentially unsustainable," indicating the risk of further deterioration in the near future.[62] Some of the systems found to be incapable of meeting "mission needs" are responsible for critical safety functions, such as collision avoidance and pilot safety notifications.

The 105 outdated systems vary in age. Seventy-three were deployed 20 to 30 years ago and some more than 60 years ago. However, even some systems less than a decade old were classified as "unsustainable."[63] Many of the outdated systems face maintenance challenges because they use parts that are not manufactured anymore, forcing technicians to salvage components from older equipment. Additionally, the FAA has reported a growing shortage of skilled workers to maintain these systems, as many trained technicians have already retired or are nearing retirement.[64]

The FAA is working on modernizing 90 of the outdated systems, particularly those with the highest operational and safety risks. But some of these upgrades will not be completed until 2030, while others are expected to take until 2038. Several of the outdated systems currently remain without a modernization plan or funding for modernization.[65] For now, much of the NAS remains vulnerable.

Flight Safety at Risk: The Growing Threat of GPS Spoofing and Jamming

The GPS — made up of orbiting satellites, ground control stations, and user receivers — provides precise positioning, navigation, and timing services on which critical infrastructure sectors depend. In aviation, from flight planning to en route navigation and real-time communications with ground control, GPS enhances the efficiency and safety of every flight. But with some GPS satellites still operating after more than 25 years in service,[66] the aging system is increasingly vulnerable to spoofing and jamming. These electronic warfare attacks can disrupt aviation operations and endanger lives.

Spoofing occurs when malicious actors send fake GPS signals intended to mislead a GPS receiver about its location, while jamming blocks GPS signals entirely. Though GPS spoofing and jamming do not affect other critical systems such as engine controls or communication, they cause a loss of situational awareness, increasing the risk of mid-air collisions or flight path errors. These risks become even more acute during in-flight emergencies, where any disruptions to navigation systems can impair a pilot's ability to respond.[67]

Spoofing and jamming attacks directly compromise the accuracy and reliability of navigation during critical phases of flight, including takeoff, cruising, and landing. For instance, in August 2024, a United Airlines flight from New Delhi to Newark experienced a spoofing attack near the Black Sea. The attack caused the aircraft's GPS coordinates to deviate from its original flight path,[68] though the aircraft's backup systems enabled a safe landing.

Another notable incident occurred in January 2022. A 33.5-hour GPS disruption affected GPS reception for aircraft within an 8,000-square-mile area around Denver, including high-traffic airspace near the Denver International Airport, the sixth-busiest in the world. [69] The disruption forced pilots to abort landings due to unreliable navigation displays and collision-avoidance systems, demonstrating the risks GPS jamming poses, particularly in congested airspace.[70]

The reliability of GPS technology is contingent on the health of the satellite network. The U.S. Space Force maintains a minimum of 24 operational satellites 95 percent of the time, though a fully operational GPS constellation consists of 31.[71] While DoD initiated a much-needed upgrade program nearly two decades ago, it has launched only 17 new, more capable GPS satellites. As a result, the United States has had to continue using some older ones despite having newer satellites ready for launch. Additionally, delivery of the operating system for these new satellites is five years behind schedule, so the ones already launched still have not reached full capability.[72]

Recent data shows a sharp rise in GPS disruptions affecting U.S. commercial flights, up from just a few dozen in the first months of 2024 to over 1,100 by August.[73] While newer data is not yet available, the pace of growth is concerning, and remedial action is urgent.

> ***"Spoofing and jamming attacks directly compromise the accuracy and reliability of navigation during critical phases of flight, including takeoff, cruising, and landing."***

Roles and Responsibilities of the Federal Aviation Administration and Transportation Security Administration

The FAA and TSA share responsibility for cybersecurity regulations for aviation critical infrastructure. The FAA's primary focus is to ensure the safety and efficiency of civil aviation infrastructure, as well as overall regulation and standards for the industry. Meanwhile, the TSA's mandate emphasizes the protection of passengers, personnel, and the physical aspects of TSA-regulated airports, as well as security equipment and systems.[74] Both agencies collaborate with other government agencies, such as CISA, to coordinate cybersecurity efforts, exchange threat intelligence, and promote cybersecurity best practices.[75]

While the FAA and TSA have taken important steps on cybersecurity in recent years, each has significant room for improvement, as detailed below. Moreover, the complementarity of the FAA's and TSA's roles often results in an unclear delineation of responsibilities, leading to fragmented oversight and inconsistent or duplicative regulation. In addition, gaps in interagency communication and differing priorities continue to undermine effective cybersecurity governance across the industry.

The Federal Aviation Administration

A decade ago, the FAA established the Cybersecurity Steering Committee to help meet evolving cyber challenges. This committee developed the FAA's 2015 Cybersecurity Strategy, outlining an agency-wide approach to protecting FAA networks, including ATC systems.[76] Internationally, the FAA actively engages in forums and working groups within the International Civil Aviation Organization to develop international cybersecurity frameworks that promote information sharing among member states to address cyber threats.[77] The FAA also engages with the international, industry-led Aviation Information Sharing and Analysis Center to exchange insights into emerging cyber threats and vulnerabilities affecting the aviation supply chain.[78]

Domestically, legislative mandates have shaped the FAA's cybersecurity efforts. Through the FAA Extension, Safety, and Security Act of 2016, Congress directed the FAA to create a comprehensive framework to clarify the roles and responsibilities of FAA offices.[79] Congress further refined this framework through follow-up legislation passed in 2018,[80] stressing the importance of interagency collaboration with the TSA and other federal agencies.

More recently, the FAA Reauthorization Act of 2024 solidified the FAA's central role as the regulator of aviation cybersecurity. By granting the agency exclusive authority to issue cybersecurity regulations for "civil aircraft, aircraft engines, propellers, and appliances,"[81] Congress affirmed cybersecurity as a core component of boosting airworthiness standards. With this new authority, Congress once again directed the FAA to update its cybersecurity strategy, which it had not done since 2020.[82]

In response, in August 2024, the FAA issued a notice of proposed rulemaking to establish standardized cybersecurity requirements as part of the agency's airworthiness standards for avionics that cover systems critical to flight safety.[83] The FAA closed the public comment period in October 2024, and the rules are pending finalization.[84]

Resource constraints have also hamstrung the FAA's cybersecurity efforts. In 2016, the FAA, DoD, and DHS launched a tri-agency forum called the Aviation Cyber Initiative (ACI) to enhance public-private partnerships and information sharing. The forum aims to leverage the strengths and expertise of each participating agency. By 2020, however, the ACI still lacked dedicated budget and personnel aside from its three co-chairs from participating agencies, according to a report by the DoT's Office of Inspector General (OIG).[85] The ACI has also failed to implement tracking mechanisms to document and evaluate progress in mitigating cybersecurity risks, improving resilience, and enhancing information sharing.[86]

In 2019, an OIG report raised concerns about the FAA's own cyber hygiene, revealing that many certification engineers responsible for ensuring the safety of avionics had not received adequate cybersecurity training.[87] The following year, the GAO found that the FAA still had not addressed the cybersecurity training gaps highlighted in the 2019 OIG report. This reflected the FAA's under-resourcing of both its internal cybersecurity priorities and its external partnerships, further undermining its efforts to enhance aviation cybersecurity.[88]

Furthermore, the FAA has faced a multitude of problems with its Next Generation Air Transportation System (NextGen) program, intended to modernize air traffic control networks by integrating advanced technologies. In a 2023 report, the GAO noted challenges similar to those facing the FAA's other programs, including a failure to implement tracking mechanisms. In addition, the NextGen program has experienced significant delays and cost overruns due to problems integrating new technology with legacy systems, resistance from various stakeholders arguing over proposed procedural changes, and complex logistical hurdles in implementing new systems across numerous airports.[89] Despite the FAA spending over $14 billion on the program in fiscal year 2022, these compounding factors have exacerbated delays and led to substantial increases in cost.[90]

While the FAA's latest progress report on NextGen presents a positive outlook, internal assessments tell a different story.[91] A 2024 OIG report concluded that NextGen "will be less transformational than originally promised," citing the FAA's lack of transparency in program expenditures and consistent failure to meet delivery timeline.[92] Persistent problems such as flight delays, air traffic congestion,[93] and frequent aircraft near-misses[94] show little to no improvement over the years, underscoring the gap between the program's objectives and its outcomes.[95] In the past, FAA officials have acknowledged that insufficient funding and challenges in coordinating cybersecurity efforts across its offices have hindered progress on the NextGen program, though efforts to address these issues have seen limited success.[96]

Nevertheless, the news is not all bad. The aviation industry welcomed the FAA's recent steps to strengthen cybersecurity, particularly the August 2024 notice of proposed rulemaking as well as the new requirements under the FAA Reauthorization Act of 2024. Industry supported the FAA's assertion that these updated standards will streamline airworthiness certification processes, reducing costs and timelines while maintaining consistent safety benchmarks.[97]

The Transportation Security Administration

Unlike the FAA, whose regulatory authority focuses on the aircraft and its certified systems, the TSA is concerned with the cyber and physical security of the regulated entities and their organizations. These regulated entities include airports and airlines within the aviation subsector, along with pipeline operators, passenger and freight rail systems, public transportation systems, and maritime facilities and operators.[98] Following the 2021 ransomware attack against Colonial Pipeline, the TSA intensified its cybersecurity efforts.[99] As part of its efforts to implement the 2023 National Cybersecurity Strategy,[100] the TSA has continued to issue updated security directives across the transportation sector.

However, the TSA has faced criticism for its poor handling of cybersecurity and broader operational security efforts, particularly for issuing reactive rather than proactive measures. The agency has also struggled to collaborate with industry stakeholders. Following the 2021 Colonial Pipeline attack, the TSA issued its first iteration of security directives for pipeline operators.[101]Industry stakeholders lamented that the agency either did not consult them or dismissed their feedback.[102] Industry experts viewed the TSA directives as rigid and poorly tailored to the sector, with industry experts pointing to requirements such as a 24-hour timeline to report a cyber incident as unrealistic and disconnected from sector-specific operational realities.[103]

In March 2023, the TSA issued emergency cybersecurity directives for TSA-regulated airports and aircraft operators. These directives require the development and implementation of plans for continuous cyber threat monitoring and detection, timely patching of systems, network segmentation, and cyber incident response. Additionally, the TSA mandated that significant cybersecurity incidents be reported to CISA.[104] Industry experts criticized these requirements for being nearly identical to those issued for passenger and freight railroad carriers in October 2022,[105] indicating a lack of customization to address the unique needs of different transportation sectors.

Recognizing these shortcomings, the TSA has striven to improve its partnerships with private industry. In September 2022, the White House provided classified threat briefings to aviation executives.[106] Building on this progress, the TSA demonstrated signs of improvement in 2023 with more flexible security program mandates for the aviation subsector. These new mandates allow regulated entities to meet cybersecurity standards through various performance-based measures. The mandates also provide clarification in three areas: implementing network segmentation, advancing a more nuanced approach to protecting operational technology systems, and establishing structured guidance for preventing unauthorized access.[107]

Regarding physical security, the TSA has faced challenges in keeping up with growing demand for air travel. Between March 2023 and March 2024, there were approximately 300 incidents of unruly travelers attempting to bypass security in areas such as document checkpoints, unmanned scanners, and no reentry areas — a figure that quadrupled since 2019, according to a TSA official.[108] The TSA's Transportation Security Officers (TSOs) serve as the first line of defense during physical security incidents. In 2024, TSOs intercepted nearly 7,000 firearms at airport checkpoints, 94 percent of which were loaded, similar to 2023 figures.[109] This surge in security incidents mirrors the significant increase in air travel, with the TSA screening over 858 million passengers in 2023, averaging about 2.4 million passengers per day.[110] In 2024, the TSA screened an average of 3 million people per day.[111] While these incidents highlight TSA's critical role in maintaining physical security, they also raise concerns about the adequacy of current security measures at airports, particularly given persistent staffing shortages.

TSOs also play a crucial role in ensuring the smooth operation of airport checkpoints by managing passenger flow. However, the surge in passenger volume has placed mounting pressure on the TSA's airport operations. Even minor staffing gaps have caused bottlenecks at critical airport checkpoints. A GAO report found that in 2023, only 96 percent of TSO positions were filled — a four-point improvement since 2022 but still below levels required for optimal operations.[112]

To compensate for these shortages, the TSA has increasingly relied on TSOs working overtime, compounding employee dissatisfaction with pay levels and limited career advancement opportunities.[113] Despite these challenges, the TSA achieved an 88 percent retention rate of its security workforce in 2023, an improvement from 83 percent in 2022.[114] However, frustration with the TSA's lack of responsiveness to employee input and engagement continues to hinder its efforts to improve workplace satisfaction and retention.[115]

On the positive side, the TSA has shown commitment to improving its own cybersecurity capabilities. For instance, the TSA included funding for 41 additional cybersecurity experts in its fiscal year 2025 budget request.[116]

In another welcome move, the TSA in November 2024 announced a Notice of Proposed Rulemaking related to cybersecurity risk management requirements for surface transportation owners and operators, including airport operations and physical security systems. The proposal represents a shift from prescriptive to performance-based regulatory models. This approach provides operators with greater flexibility in meeting the TSA's defined security goals while addressing industry concerns that previous directives were overly rigid.[117] Based on aviation industry feedback, the TSA now conducts on-site inspections in which companies discuss and provide sensitive security information directly rather than submitting it electronically. While more time-intensive, this alternative better addresses concerns about securely handling data.

During testimony before Congress in November 2024, TSA officials reaffirmed the agency's commitment to refining its approach based on industry feedback.[118] Public comments for TSA's proposed rules were due in early February 2025. With the feedback it received from stakeholders, the TSA plans to address sector-specific vulnerabilities by harmonizing regulations to avoid duplication.

Overlap Between FAA and TSA Roles

Despite the recent progress, federal regulatory overlap remains a critical challenge for the industry. According to a 2023 report on harmonization published by the Office of the National Cyber Director (ONCD), conflicting requirements from the FAA's airworthiness standards, the TSA's security directives, and DoD's contractor guidelines have caused compliance inefficiencies. These conflicts have overburdened industry, the report found, with representatives from Airlines for America and the Association of American Railroads both emphasizing the need to harmonize regulation.[119]

A lack of consistent industry engagement has left stakeholders frustrated as they navigate unclear expectations. The 2023 report cited an industry respondent who criticized federal agencies for having "varying interests and expectations" regarding cybersecurity requirements.[120] Another industry association highlighted discrepancies between TSA requirements and FAA's airworthiness requirements, stating that agencies often conduct cybersecurity assessments using different frameworks and definitions.[121]

Adding to the complexity, aviation operators must also prepare to comply with the forthcoming reporting requirements under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), which are currently under development by CISA.[122] Although CIRCIA aims to improve and standardize national cybersecurity incident reporting processes, the law's potential overlap with existing FAA, TSA, and DoD requirements could further burden the industry and increase administrative demands, ultimately detracting from the intended proactive cyber threat response efforts.

The evolving regulatory environment underscores the high risks facing the industry. While the FAA and TSA's combined efforts have made meaningful progress, their success will depend on clearly defining roles and responsibilities, harmonizing regulatory frameworks, and active industry participation in implementing new requirements.

Recommendations

1. The FAA should implement comprehensive technology modernization and cybersecurity enhancement for air traffic control systems.

Despite the ongoing efforts to modernize aviation technologies, the FAA's cybersecurity framework still contains gaps, particularly in risk management and incident response capabilities.[123] The FAA is currently implementing the NextGen program to modernize its ATC systems. However, the program does not introduce necessary cyber-physical security measures, crucial for protecting both the digital operations and the physical components of the increasingly interconnected and digitized aviation infrastructure.[124] Moreover, NextGen's delayed implementation timeline and substantial cost have called the program's effectiveness into question.[125]

To address these issues, the FAA should develop and implement a comprehensive cybersecurity-focused technology modernization and enhancement program designed specifically to strengthen ATC systems. While the FAA's ongoing NextGen program aims to improve the overall performance of air traffic management through technology upgrades, it has not sufficiently prioritized cybersecurity-specific enhancements. This new cybersecurity enhancement program would complement NextGen by embedding cybersecurity measures into modernization efforts, ensuring that technological upgrades do not outpace the FAA's ability to defend them.

This program should reference existing National Institute of Standards and Technology (NIST) guidelines, such as NIST publication SP 800-53, titled "Security and Privacy Controls for Information Systems and Organizations,"[126] to ensure implementation of robust and standardized measures. In conjunction with this program, the FAA should provide specialized training to its security operations center personnel to enable them to effectively monitor and respond to cyber threats targeting air traffic control systems. These trained professionals would continuously monitor data flow, enabling a swift response to cyber incidents, following the guidelines set by the NIST publication SP 800-61, titled "Information Security Continuous Monitoring for Federal Information Systems and Organizations."[127]

Implementing these measures will require Congress to appropriate additional resources. However, this investment is crucial for ensuring resilience against evolving cyber threats. To ensure the effectiveness of these measures, the FAA should conduct regular audits and assessments of its cybersecurity framework. These assessments should evaluate compliance with industry standards and best practices, identify areas for improvement, and guide the allocation of resources to address any identified vulnerabilities. By prioritizing these efforts, the FAA can strengthen its cybersecurity posture and maintain the integrity of the nation's ATC systems in the face of increasingly sophisticated cyber threats.

2. The FAA should establish a Cybersecurity Infrastructure Grant Program for Strategic Airport Defense.

In collaboration with DoD, the FAA should establish a cybersecurity grant program for airport control authorities. This program should provide financial assistance to strategic airports, which are critical to national defense due to their role in supporting military operations, emergency response efforts, and other national security functions. Currently, there are 69 airports that are designated as strategic across the United States.[128] To help decide which airports to prioritize, the FAA should establish criteria that consider factors such as the airports' criticality to national defense, passenger and cargo volume, and geographic location.

Once identified, potential grant recipients should be obligated to conduct a comprehensive assessment to pinpoint specific cybersecurity vulnerabilities and requirements that need to be addressed. This assessment would require the involvement of cybersecurity experts and other relevant industry stakeholders. The allocation of funds should be tailored to address these needs while prioritizing areas that would have the greatest impact.

In addition, the FAA and DoD should provide technical guidance to help grant recipients effectively utilize the funds and implement cybersecurity measures. Moreover, the FAA should establish clear performance metrics and reporting requirements, which will ensure accountability and ongoing evaluation of grant effectiveness. Information from continuous monitoring and evaluation can be shared among grant recipients, industry partners, and government agencies to promote knowledge exchange and help identify emerging threats.

3. The TSA should collaborate with the FAA and CISA to conduct comprehensive cybersecurity vulnerability and risk assessments on select high-impact airports.

By fostering a close partnership with the FAA and CISA, the TSA can leverage their combined resources and expertise to conduct comprehensive cybersecurity vulnerability and risk assessments of select airports, particularly focusing on airports that serve as hubs for both commercial and military operations. These agencies should work with industry partners to identify and prioritize airports that act as central nodes in hub-and-spoke networks, as disruptions in these hubs can cascade throughout the airline network, affecting not only commercial services but also military mobility. In tandem, these assessments can address unique challenges posed by point-to-point models, ensuring that proper redundancies are in place to mitigate disruptions to IT infrastructure at airports with frequent delays and limited airline operations.

Given that disruptions to hub-and-spoke networks can undermine military mobility, these risk assessments should focus on identifying both system redundancies and critical modernization areas that support DoD operations. Incidents discussed in this report highlight the need for the FAA to strengthen its oversight to ensure robust cybersecurity standards for aviation critical infrastructure. In parallel, the TSA, in partnership with the FAA, can revise existing policies to require independent testing procedures for airport security — for example, engaging CISA for unbiased testing of airport infrastructure to uncover vulnerabilities that might otherwise go unnoticed.

Additionally, insights from these assessments should be used to enhance civil-military collaboration, allowing the TSA, CISA, FAA, and DoD to share threat intelligence and cybersecurity best practices with TSA-regulated airports, operators, and federal law enforcement partners. The Aviation Cyber Initiative could be a key member of this discussion. Strengthening these partnerships would ensure that critical integration points where civilian airlines support military operations are secured against potential cyberattacks.

Furthermore, in support of this effort, the FAA and TSA must address staffing and training gaps for its inspectors specializing in avionics and airport operational cybersecurity and physical security. While the FAA says it has allocated oversight resources related to staffing and training,[129] instituting continual training on emerging cybersecurity and technological threats would ensure the FAA's inspectors and engineers are well equipped to handle these challenges. TSA should also identify incentives to attract, retain, and train both its cybersecurity and physical security workforce.

By implementing flexible and adaptable cybersecurity requirements informed by industry, TSA can improve security outcomes while minimizing burdensome compliance requirements. Similarly, by improving career advancement opportunities based on feedback from its workforce, the TSA can increase employee retention rates and reduce turnover-related costs. Ultimately, this would support more consistent operations and deliver improvements in public safety overall.

4. The FAA and TSA should harmonize cybersecurity regulatory requirements for the aviation subsector.

Aviation industry stakeholders have continued to raise concerns about conflicting requirements between the TSA's security directives and the FAA's airworthiness standards.[130] As one industry stakeholder noted in a response to a request for information by the ONCD,[131] overlapping regulatory demands "increase compliance costs and hinder sound cyber risk management."[132] These discrepancies can create operational challenges.

Regulatory harmonization is needed to ensure consistency and effectiveness. As they are working to align their directives and regulations, the TSA and FAA should also cross-reference existing cybersecurity guidance, such as NIST's Cybersecurity Framework[133] and publication SP 800-161, titled "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations," for supply chain risk management.[134] The harmonized regulations should also include specific guidelines for security of the supply chain, from vendor selection to product delivery. These guidelines should be tailored to the unique cybersecurity needs of aviation operations, including critical programs such as the Civil Reserve Air Fleet. Industry input will also be crucial in this process, as it provides practical insights into regulatory burden and reasonable expectations around the feasibility of cybersecurity requirements. Associations such as the Aviation Information Sharing and Analysis Center can play a vital role in disseminating new guidance and engaging industry stakeholders in education and training sessions, further enhancing cybersecurity awareness within the aviation industry.

5. The FAA should address and implement the recommendations outlined in the GAO's October 2020 report to enhance both the ACI and to improve cybersecurity across the aviation industry.

The FAA should prioritize enhancing the ACI's tracking mechanisms to bolster its effectiveness in improving cybersecurity across the aviation industry.[135] Strengthening these tracking mechanisms can enable the ACI to better capture and utilize valuable insights derived from its collaborative coordination efforts, thus informing strategic cybersecurity enhancements industry-wide. Additionally, increasing funding for the ACI's joint research and development program could improve coordination mechanisms that foster innovation and advancement of cybersecurity capabilities and preparedness within the aviation subsector.

Effective documentation and dissemination of insights gained from ACI's efforts are essential for informed decision-making and continuous improvement in cybersecurity coordination. The FAA should establish clear guidelines and protocols for documenting and sharing best practices, lessons learned, and emerging trends in aviation cybersecurity. This information should be made readily accessible to all relevant stakeholders through secure, user-friendly digital platforms. Furthermore, the FAA should maintain transparency by sharing with the GAO challenges encountered in implementing recommendations. This transparency will foster open dialogue for tailored solutions to help address underlying issues. Regular progress reports and updates to the GAO will ensure accountability and track the effectiveness of implemented recommendations.

Conclusion

Enhancing cybersecurity resilience in the aviation industry is crucial for maintaining public trust, economic stability, and national security. Failure to address cybersecurity challenges could have far-reaching consequences, impacting not only the nation's economic well-being but also U.S. military power projection and flight safety. While civilian and military joint use of critical infrastructure provides many benefits, cyberattacks targeting these intertwined networks could severely disrupt military logistics, compromising mission readiness and military mobility.

Addressing these cybersecurity challenges requires a concerted effort by federal agencies, Congress, and industry stakeholders. This collaborative approach should involve investment in capabilities to detect, prevent, and respond to evolving cyber threats and development of a skilled workforce through tailored training programs. It also necessitates strong public-private partnerships and effective interagency coordination among the FAA, TSA, and CISA.

Many of the issues identified in this paper are lingering problems that have been known to industry and policymakers for years. This lack of attention and failure to take timely action puts America's national security, economic productivity, and public safety at risk.

Endnotes

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)

2. Airlines for America, “Economic Impact of Commercial Aviation,” accessed March 26, 2025. (https://www.airlines.org/impact)

3. Airlines for America, “The State of U.S. Commercial Aviation,” accessed March 26, 2025. (https://www.airlines.org/dataset/state-of-us-aviation)

4. Ibid.

5. U.S. Department of Transportation, Federal Aviation Administration, “Air Traffic by the Numbers,” May 2024, page 7. (https://www.faa.gov/air_traffic/by_the_numbers/media/Air_Traffic_by_the_Numbers_2024.pdf)

6. Airlines for America, “Annual Results: U.S. Passenger Airlines,” August 21, 2024. (https://www.airlines.org/dataset/annual-results-u-s-passenger-airlines)

7. U.S. Department of Transportation, Federal Railroad Administration, “Freight Rail Overview,” February 24, 2025. (https://railroads.dot.gov/rail-network-development/freight-rail-overview)

8. Ibid.

9. U.S. International Trade Commission, “Shifts in U.S. Merchandise Trade, 2020, Investigation No. 332-345,” Publication 5239, November 2021. (https://www.usitc.gov/research_and_analysis/tradeshifts/2020/special_topic.html)

10. FedEx Corporation, “FedEx 2021 ESG Report,” May 18, 2021, pages 8-9. (https://www.fedex.com/content/dam/fedex/us-united-states/sustainability/gcrs/FedEx_2021_ESG_Report.pdf)

11. Bindiya Vakil and Tom Linton, “Why We’re in the Midst of a Global Semiconductor Shortage,” *Harvard Business Review*, February 26, 2021. (https://hbr.org/2021/02/why-were-in-the-midst-of-a-global-semiconductor-shortage); Tomasz Sniedziewski, “Semiconductor Industry: Linchpin of Taiwan’s Cargo Sector,” *Orient Aviation*, October 1, 2023. (http://www.orientaviation.com/articles/10740/semiconductor-industry-linchpin-of-taiwan’s-cargo-sector)

12. U.S. International Trade Commission, “Shifts in U.S. Merchandise Trade, 2020, Investigation No. 332-345,” Publication 5239, November 2021. (https://www.usitc.gov/research_and_analysis/tradeshifts/2020/special_topic.html)

13. U.S. Census Bureau, “Quarterly Retail E-Commerce Sales: 4th Quarter 2024,” February 19, 2025, page 1. (https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf)

14. Greg Knowler, . “Air cargo shrugs off seasonality to ride wave of e-commerce demand,” *S&P Global Market Intelligence*, August 19, 2024. (https://www.spglobal.com/marketintelligence/en/mi/research-analysis/air-cargo-shrugs-off-seasonality-to-ride-wave-of-ecommerce-dem.html)

15. Marcus Weisgerber, “Commercial Planes, Ships Would Play Large Role in Pacific War, TRANSCOM Head Says,” *Defense One*, October 17, 2022. (https://www.defenseone.com/business/2022/10/commercial-planes-ships-would-play-large-role-pacific-war-transcom-head-says/378524)

16. United States Transportation Command, “About USTRANSCOM,” accessed March 26, 2025. (https://www.ustranscom.mil/cmd/aboutustc.cfm)

17. There were 6,852 aircraft in service in the United States as of 2022. As of September 2022, the number of CRAF aircraft included 268 long-range and 145 short-range aircraft supporting international segments and 37 aircraft supporting national segments. The number of CRAF aircraft varies each month. See: 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)

18. U.S. Transportation Command, Press Release, “Civil Reserve Air Fleet is critical to national security,” August 22, 2022. (https://www.ustranscom.mil/cmd/panewsreader.cfm?id=C40F192D-0E8E-F824-109458213BB174B5)

19. U.S. Department of Defense, Office of Inspector General, “Management Advisory: The DOD’s Use of the Civil Reserve Air Fleet in Support of Afghanistan Noncombatant Evacuation Operations,” June 28, 2022, page 1. (https://media.defense.gov/2022/Jun/30/2003027866/-1/-1/1/DODIG-2022-109.PDF); U.S. Air Force, “Operation Iraqi Freedom,” April 30, 2003. (https://www.afhistory.af.mil/FAQs/Fact-Sheets/Article/458942/2003-operation-iraqi-freedom)

20. U.S. Transportation Command, Press Release, “Afghanistan Evacuation Support,” accessed March 26, 2025. (https://www.ustranscom.mil/cmd/neo.cfm)

21. U.S. Government Accountability Office, “KC-46 Tanker: Air Force Needs to Mature Critical Technologies in New Aerial Refueling System Design,” January 27, 2022, page 27. (https://www.gao.gov/products/gao-22-104530)

22. Christopher Bolkcom, “Civil Reserve Air Fleet (CRAF),” *Congressional Research Services*, October 18, 2006, page 4. (https://sgp.fas.org/crs/weapons/RL33692.pdf)

23. U.S. Department of Transportation, Federal Aviation Administration, “Joint Civilian/Military (Joint-Use) Airports,” August 2, 2022. (https://www.faa.gov/airports/planning_capacity/joint_use_airports)

24. U.S. Department of Transportation, Federal Aviation Administration, “National Plan of Integrated Airport Systems (NPIAS) 2023-2027,” September 30, 2022, page 13. (https://www.faa.gov/sites/faa.gov/files/npias-2023-2027-narrative.pdf)

25. Alexander Mitchell, “Joint-Use Airports: Everything You Need To Know,” *Simple Flying*, August 6, 2023. (https://simpleflying.com/joint-use-airports-complete-guide)

26. U.S. Department of Defense, “DoD Directive 5030.19, DoD Responsibilities on Federal Aviation,” March 6, 2023, pages 3-4. (https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/503019p.pdf?ver=kXwPF30cLr5h9yJFNUNwHg%3D%3D)

27. Heidi M. Peters, “Defense Acquisitions: DOD’s Cybersecurity Maturity Model Certification Framework,” *Congressional Research Services*, December 18, 2020, page 2. (https://sgp.fas.org/crs/natsec/R46643.pdf)

28. U.S. Department of Defense, “Defense Industrial Base Cybersecurity Strategy 2024,” March 21, 2024, page 17. (https://media.defense.gov/2024/Mar/28/2003424523/-1/-1/1/DOD_DOB_CS_STRATEGY_DSD_SIGNED_20240325.PDF); U.S. Department of Defense, Cyber Crime Center (DC3), “Defense Industrial Base Collaborative Information Sharing Environment Overview,” accessed March 26, 2025. (https://www.dc3.mil/Missions/DIB-Cybersecurity/DIB-Cybersecurity-DCISE)

29. U.S. Department of Transportation, Federal Aviation Administration, “ATC Facilities and Engineering Services,” November 21, 2024. (https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/atc_facilities); U.S. Department of Defense, Defense Logistics Agency, “Defense Automatic Addressing System (DAAS),” accessed March 26, 2025. (https://www.dla.mil/Working-With-DLA/Applications/DAAS); U.S. Department of Defense, “Summary of the Joint All-Domain Command & Control (JADC2) Strategy,” March 2022, page 3. (https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF)

30. U.S. Department of Transportation, Federal Aviation Administration, “Air Traffic by the Numbers,” May 2024, page 17. (https://www.faa.gov/air_traffic/by_the_numbers/media/Air_Traffic_by_the_Numbers_2023.pdf)

31. Ibid.

32. International Air Transportation Association, Press Release, “Supply Chain Issues Continue to Negatively Impact Airline Performance into 2025,” December 10, 2024. (https://www.iata.org/en/pressroom/2024-releases/2024-12-10-02)

33. Rosehana Amin, Tom van der Wijngaart, Aron Dindol, and Danielle Rodgers, “Cyber threats in the aviation industry,” *Clyde & Co*, December 11, 2024. (https://www.clydeco.com/en/insights/2024/11/cyber-threats-in-the-aviation-industry)

34. “Panel Warns of Increased Cybersecurity Threats to Aviation,” *American Institute of Aeronautics and Astronautics*, April 21, 2023. (https://www.aiaa.org/news/news/2023/04/21/panel-warns-of-increased-cybersecurity-threats-to-aviation)

35. AJ Vicens, “Boeing confirms attempted $200 million ransomware extortion attempt,” *CyberScoop*, May 8, 2024. (https://cyberscoop.com/boeing-confirms-attempted-200-million-ransomware-extortion-attempt)

36. Carly Page, “Boeing confirms ‘cyber incident’ after ransomware gang claims data theft,” *Tech Crunch*, November 2, 2023. (https://techcrunch.com/2023/11/02/boeing-cyber-incident-ransomware-gang-claims-data-theft) See also: Rear Adm. (Ret.) Mark Montgomery and Jiwon Ma, “No Room for Half-Measures in Aviation Cybersecurity,” *Foundation for Defense of Democracies*, November 22, 2022. (https://www.fdd.org/analysis/2022/11/22/no-half-measures-aviation-cybersecurity)

37. U.S. Senate Committee on Commerce, Science, and Transportation, “Aviation Cybersecurity Threats,” September 18, 2024, page 3. (https://commerce.senate.gov/services/files/A254A80D-EB70-4F21-BAD4-5ACF13CA6088)

38. “Hackers demand $6 million for files stolen from Seattle airport operator in cyberattack,” *Associated Press*, September 18, 2024. (https://apnews.com/article/seattle-airport-cyberattack-ransomware-rhysida-95cd980a9f45112f0fdce488233eec9c); Ionut Arghire, “Data Stolen in Ransomware Attack That Hit Seattle Airport,” *SecurityWeek*, September 16, 2024. (https://www.securityweek.com/data-stolen-in-ransomware-attack-that-hit-seattle-airport)

39. U.S. Senate Committee on Commerce, Science, and Transportation, “Aviation Cybersecurity Threats,” September 18, 2024, pages 3-4. (https://commerce.senate.gov/services/files/A254A80D-EB70-4F21-BAD4-5ACF13CA6088)

40. “Theft of Customer Data at British Airways,” *International Airlines Group*, July 8, 2019. (https://www.investegate.co.uk/announcement/rns/international-consolidated-airlines-group-sa-cdi---iag/theft-of-customer-data-at-british-airways-update/81851); Ingrid Lunden, “UK’s ICO fines British Airways a record £183M over GDPR breach that leaked data from 500,000 users,” *TechCrunch*, July 8, 2019. (https://techcrunch.com/2019/07/08/uks-ico-fines-british-airways-a-record-183m-over-gdpr-breach-that-leaked-data-from-500000-users); Cathay Pacific, “Cathay Pacific announces data security event affecting passenger data,” October 24, 2018. (https://news.cathaypacific.com/cathay-pacific-announces-data-security-event-affecting-passenger-data-250618); Will Horton, “Cathay Pacific Faulted For Data Breach, But Hackers’ Objective Unclear,” *Forbes*, June 6, 2019. (https://www.forbes.com/sites/willhorton1/2019/06/06/cathay-pacific-faulted-for-data-breach-but-hackers-objective-unclear); Kevin Townsend, “Cathay Pacific Airways Fined Over Long-Running Breach,” *Security Week*, March 5, 2020. (https://www.securityweek.com/cathay-pacific-airways-fined-over-long-running-breach)

41. Stephenson Harwood, “Aviation is facing a rising wave of cyber-attacks in the wake of COVID,” *SH Legal*, August 8, 2022. (https://www.shlegal.com/insights/aviation-is-facing-a-rising-wave-of-cyber-attacks-in-the-wake-of-covid)

42. Sergiu Gatlan, “Air France and KLM notify customers of account hacks.” *BleepingComputer*, January 6, 2023. (https://www.bleepingcomputer.com/news/security/air-france-and-klm-notify-customers-of-account-hacks); Bill Toulas, “Scandinavian Airlines says cyberattack caused passenger data leak,” *Beeping Computer*, February 16, 2023. (https://www.bleepingcomputer.com/news/security/scandinavian-airlines-says-cyberattack-caused-passenger-data-leak); Zack Whittaker, “Ransomware gang claims credit for Sabre data breach,” *Tech Crunch*, September 6, 2023. (https://techcrunch.com/2023/09/06/ransomware-gang-claims-credit-for-sabre-data-breach)

43. “Data Breach Exposes Pilot Personal Information at American Airlines and Southwest Airlines,” *Galaxkey*, July 4, 2023. (https://www.galaxkey.com/blog/data-breach-exposes-pilot-personal-information-at-american-airlines-and-southwest-airlines); Ionut Arghire, “American Airlines, Southwest Airlines Impacted by Data Breach at Third-Party Provider,” *SecurityWeek Network*, June 26, 2023. (https://www.securityweek.com/american-airlines-southwest-airlines-impacted-by-data-breach-at-third-party-provider)

44. The Russian group KillNet targeted Atlanta’s Hartsfield-Jackson International Airport (ATL), Los Angeles International Airport (LAX), Chicago O’Hare International Airport (ORD), Orlando International Airport (MCO), Denver International Airport (DIA), Phoenix Sky Harbor International Airport (PHX), and others in Kentucky, Mississippi, and Hawaii. See: Bill Toulas, “US airports’ sites taken down in DDoS attacks by pro-Russian hackers,” *Bleeping Computer*, October 10, 2022. (https://www.bleepingcomputer.com/news/security/us-airports-sites-taken-down-in-ddos-attacks-by-pro-russian-hackers); Silviu Stahie, “Pro-Russian KillNet Group Hits US Airline Websites with DDoS Attack,” *Bitdefender*, October 11, 2022. (https://www.bitdefender.com/blog/hotforsecurity/pro-russian-killnet-group-hits-us-airline-websites-with-ddos-attack)

45. Catalin Cimpanu, “Russian state hackers behind San Francisco airport hack,” *ZDNET*, April 14, 2020. (https://www.zdnet.com/article/russian-state-hackers-behind-san-francisco-airport-hack); Phil Muncaster, “San Francisco Airport Attack Linked to Russian State Hackers,” *Infosecurity Magazine*, April 15, 2020. (https://www.infosecurity-magazine.com/news/san-francisco-airport-attack)

46. U.S. Government Accountability Office, “Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks,” October 9, 2020. (https://www.gao.gov/products/gao-21-86)

47. U.S. Government Accountability Office, “Commercial Aviation Manufacturing: Supply Chain Challenges and Actions to Address Them,” March 6, 2024. (https://www.gao.gov/products/gao-24-106493)

48. U.S. Government Accountability Office, “Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks,” October 2020, pages 5 and 22. (https://www.gao.gov/assets/gao-21-86.pdf)

49. Stephenson Harwood, “Aviation is facing a rising wave of cyber-attacks in the wake of COVID,” *SH Legal*, August 8, 2022. (https://www.shlegal.com/insights/aviation-is-facing-a-rising-wave-of-cyber-attacks-in-the-wake-of-covid)

50. David Shepardson, “Southwest Airlines agrees to $140 million penalty over 2022 holiday meltdown,” *Reuters*, December 18, 2023. (https://www.reuters.com/business/aerospace-defense/southwest-airlines-agrees-140-million-penalty-over-2022-holiday-meltdown-2023-12-18)

51. John Grant, “CrowdStrike Travel Chaos: Airlines Struggling Back to Normal Operations,” *OAG*, July 22, 2024. (https://www.oag.com/blog/crowdstrike-travel-chaos-airlines-struggling-back-to-normal-operations)

52. Linda Rutherford, “December Disruption: A Message from Southwest’s Chief Administration & Communications Officer,” *Southwest Airlines*, February 9, 2023. (https://community.southwest.com/t5/Blog/December-Disruption-A-Message-from-Southwest-s-Chief/ba-p/155323)

53. Southwest Airlines, Press Release, “Southwest Airlines Reports Fourth Quarter and Full Year 2022 Results,” January 26, 2023. (https://www.southwestairlinesinvestorrelations.com/news-and-events/news-releases/2023/01-26-2023-114537893)

54. CNN Staff, “Which airports and airlines have been affected by the outages?” *CNN*, July 19, 2024. (https://www.cnn.com/2024/07/19/travel/the-airlines-impacted-by-the-global-tech-outage/index.html); “Tech outage eases after widespread disruption,” *Reuters*, July 19, 2024. (https://www.reuters.com/technology/global-cyber-outage-grounds-flights-hits-media-financial-telecoms-2024-07-19); Jordan Robertson and Shona Ghosh, “Global IT Failure Puts Cyber Firm CrowdStrike in Spotlight,” *Bloomberg*, July 19, 2024. (https://www.bloomberg.com/news/articles/2024-07-19/global-it-collapse-puts-cyber-firm-crowdstrike-in-spotlight)

55. The Delta Virtual, “Our Hubs: Minneapolis–Saint Paul International Airport,” *Delta Airlines*, accessed March 26, 2025. (https://thedeltavirtual.com/hubs); Derek James, “Delta fliers at MSP Airport still frustrated, despite matters improving,” *CBS News*, July 24, 2024. (https://www.cbsnews.com/minnesota/news/delta-air-lines-fliers-msp-airport-delays-cancellations); CNN Staff, “Which airports and airlines have been affected by the outages?” *CNN*, July 19, 2024. (https://www.cnn.com/2024/07/19/travel/the-airlines-impacted-by-the-global-tech-outage/index.html); Reuters, “Tech outage eases after widespread disruption,” *Reuters*, July 19, 2024. (https://www.reuters.com/technology/global-cyber-outage-grounds-flights-hits-media-financial-telecoms-2024-07-19)

56. SecurityScorecard, “The Cyber Risk Landscape of the Global Aviation Industry,” July 2024, page 7. (https://securityscorecard.com/wp-content/uploads/2024/07/Aviation_Cyber-Risk-Landscape-Report.pdf)

57. U.S. Department of Transportation, Federal Aviation Administration, “Budget Estimates, Fiscal Year 2023,” April 2022, page 2. (https://www.transportation.gov/sites/dot.gov/files/2022-04/FAA_Budget_Estimates_FY2023.pdf)

58. Emily Olson, Rachel Treisman, and Jaclyn Diaz, “A damaged file may have caused the outage in an FAA system, leading to travel chaos,” *National Public Radio*, January 11, 2023. (https://www.npr.org/2023/01/11/1148340708/faa-notam-ground-stop-flight-delay)

59. Adam Janofsky, “Cyber incident at Boeing subsidiary causes flight planning disruptions,” *The Record*, November 2, 2022. (https://therecord.media/cyber-incident-at-boeing-subsidiary-causes-flight-planning-disruptions); David Shepardson, Rajesh Kumar Singh, and Abhijith Ganapavaram, “Airlines hope for return to normal Thursday after FAA outage snarls U.S. travel,” *Reuters*, January 11, 2023. (https://www.reuters.com/business/aerospace-defense/us-faa-says-flight-personnel-alert-system-not-processing-updates-after-outage-2023-01-11); Brian Rokus, “FAA says unintentionally deleted files are to blame for nationwide ground stop,” *CNN*, January 19, 2023. (https://www.cnn.com/2023/01/19/business/faa-notam-outage/index.html)

60. Sam Sweeney, Jon Haworth, Kevin Shlvey, Meredith Deliso, and Josh Margolin, “Software maintenance mistake at center of major FAA computer meltdown: Official,” *ABC News*, January 11, 2023. (https://abcnews.go.com/US/computer-failure-faa-impact-flights-nationwide/story?id=96358202)

61. U.S. Government Accountability Office, “Air Traffic Control: FAA Actions Are Urgently Needed to Modernize Aging Systems,” September 23, 2024. (https://www.gao.gov/products/gao-24-107001)

62. Ibid., page 15.

63. Ibid., pages 17 and 20.

64. Ibid., page 18.

65. Ibid., pages 18-20.

66. Joseph Gedeon, “Can’t teach an old GPS new tricks,” *Politico*, May 28, 2024. (https://www.politico.com/newsletters/weekly-cybersecurity/2024/05/28/cant-teach-an-old-gps-new-tricks-00160066)

67. Sandra Erwin, “GPS startup bets on advanced signal to counter jamming threats,” *SpaceNews*, July 17, 2024. (https://spacenews.com/gps-startup-bets-on-advanced-signal-to-counter-jamming-threats); U.S. Government Accountability Office, “Delays Continue in Delivering More Secure Capability for the Warfighter,” September 2024, pages 4 and 12. (https://www.gao.gov/assets/gao-24-106841.pdf); Andrew Tangel and Drew Fitzgerald, “Electronic Warfare Spooks Airlines, Pilots and Air-Safety Officials,” *The Wall Street Journal*, September 23, 2024. (https://www.wsj.com/business/airlines/electronic-warfare-spooks-airlines-pilots-and-air-safety-officials-60959bbd)

68. U.S. Government Accountability Office, “Delays Continue in Delivering More Secure Capability for the Warfighter,” September 2024, pages 4 and 12. (https://www.gao.gov/assets/gao-24-106841.pdf)

69. Andrew Tangel and Drew Fitzgerald, “Electronic Warfare Spooks Airlines, Pilots and Air-Safety Officials,” *The Wall Street Journal*, September 23, 2024. (https://www.wsj.com/business/airlines/electronic-warfare-spooks-airlines-pilots-and-air-safety-officials-60959bbd); U.S. Government Accountability Office, “Delays Continue in Delivering More Secure Capability for the Warfighter,” September 2024, pages 4 and 12. (https://www.gao.gov/assets/gao-24-106841.pdf)

70. Andrew Tangel and Drew Fitzgerald, “Electronic Warfare Spooks Airlines, Pilots and Air-Safety Officials,” *The Wall Street Journal*, September 23, 2024. (https://www.wsj.com/business/airlines/electronic-warfare-spooks-airlines-pilots-and-air-safety-officials-60959bbd); U.S. Department of Homeland Security, Cybersecurity and Infrastructure Agency, “Global Positioning System (GPS) Interference,” December 2022. (https://www.cisa.gov/sites/default/files/publications/CISA-Insights_GPS-Interference_508.pdf)

71. U.S. Space Force, the National Coordination Office for Space-Based Positioning, Navigation, and Timing, “Space Segment,” June 28, 2022. (https://www.gps.gov/systems/gps/space)

72. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, “Global Positioning System (GPS) Interference,” December 2022. (https://www.cisa.gov/sites/default/files/publications/CISA-Insights_GPS-Interference_508.pdf); Sandra Erwin, “GPS startup bets on advanced signal to counter jamming threats,” *SpaceNews*, July 17, 2024. (https://spacenews.com/gps-startup-bets-on-advanced-signal-to-counter-jamming-threats); U.S. Government Accountability Office, “Delays Continue in Delivering More Secure Capability for the Warfighter,” September 2024, pages 4 and 12. (https://www.gao.gov/assets/gao-24-106841.pdf)

73. Andrew Tangel and Drew Fitzgerald, “Electronic Warfare Spooks Airlines, Pilots and Air-Safety Officials,” *The Wall Street Journal*, September 23, 2024. (https://www.wsj.com/business/airlines/electronic-warfare-spooks-airlines-pilots-and-air-safety-officials-60959bbd). For live data on GPS spoofing and jamming incidents affecting aviation, see: Zurich University of Applied Sciences, SkAI Data Services, “Live GPS Spoofing and Jamming Tracker Map,” accessed March 26, 2025. (https://spoofing.skai-data-services.com)

74. “Cybersecurity,” *U.S. Department of Homeland Security*, accessed March 26, 2025. (https://www.dhs.gov/topics/cybersecurity); “Timeline,” *U.S. Department of Homeland Security, Transportation Security Administration*, accessed March 26, 2025. (https://www.tsa.gov/timeline); U.S. Department of Homeland Security, Transportation Security Administration, “Biennial National Strategy for Transportation Security,” April 18, 2023, pages 1-2. (https://www.dhs.gov/sites/default/files/2023-06/TSA_Biennial_NSTS_20230418_Signed_508C.pdf)

75. U.S. Department of Homeland Security, Transportation Security Administration, “2023 Biennial National Strategy for Transportation Security Appendices,” June 2, 2023, pages 22-33. (https://www.dhs.gov/sites/default/files/2023-06/NSTS_Appendices_Final_4_18_23_508C.pdf)

76. U.S. Department of Transportation, Office of Inspector General, “FAA Has Made Progress but Additional Actions Remain To Implement Congressionally Mandated Cyber Initiatives,” March 20, 2019, page 4. (https://www.oig.dot.gov/sites/default/files/FAA%20Cybersecurity%20Program%20Final%20Report%5E03.20.19.pdf)

77. International Civil Aviation Organization, “Aviation Cybersecurity,” accessed March 26, 2025. (https://www.icao.int/aviationcybersecurity/Pages/default.aspx); U.S. Department of Transportation, Federal Aviation Administration, “Office of International Affairs,” accessed March 26, 2025. (https://www.faa.gov/international_affairs); U.S. Department of Transportation, Federal Aviation Administration, “ICAO and International Training,” accessed March 26, 2025. (https://www.faa.gov/about/office_org/headquarters_offices/apl/international_affairs/global_issues)

78. Aviation Information Sharing Analysis Center, accessed March 26, 2025. (https://www.a-isac.com)

79. FAA Extension, Safety, and Security Act, 2016, Pub. L. 114-190, 130 Stat. 625. (https://www.congress.gov/114/statute/STATUTE-130/STATUTE-130-Pg615.pdf); Larry Grossman, “The Evolving Cybersecurity Landscape: Federal Perspectives on Securing the Nation’s Infrastructure,” December 2, 2021. (https://www.transportation.gov/evolving-cybersecurity-landscape-federal-perspectives-securing-nations-infrastructure)

80. This is the Comprehensive Strategic Framework that Congress directed the FAA to establish in the FAA Extension, Safety, and Security Act of 2016. See: FAA Extension, Safety, and Security Act, 2016, Pub. L. 114-190, 130 Stat. 625. (https://www.congress.gov/114/statute/STATUTE-130/STATUTE-130-Pg615.pdf)

81. FAA Reauthorization Act, 2024, Pub. L. 118-63, 138 Stat. 1144. (https://www.congress.gov/118/plaws/publ63/PLAW-118publ63.pdf)

82. FAA Reauthorization Act, 2024, Pub. L. 118-63, 138 Stat. 1144. (https://www.congress.gov/118/plaws/publ63/PLAW-118publ63.pdf); U.S. Senate Committee on Commerce, Science, and Transportation, Press Release, "Senate Commerce Committee Passes 5-Year Bipartisan Senate FAA Reauthorization Focused on Improving Safety, Advancing Technology," February 8, 2024. (https://www.commerce.senate.gov/2024/2/senate-commerce-committee-passes-5-year-bipartisan-senate-faa-reauthorization-focused-on-improving-safety-advancing-technology); FAA Reauthorization Act, 2024, Pub. L. 118-63, 138 Stat. 1144. (https://www.congress.gov/118/plaws/publ63/PLAW-118publ63.pdf); U.S. Department of Transportation, Office of Inspector General, "FAA Has Made Progress but Additional Actions Remain To Implement Congressionally Mandated Cyber Initiatives," March 20, 2019. (https://www.oig.dot.gov/sites/default/files/FAA Cybersecurity Program Final Report%5E03.20.19.pdf)

83. Equipment, Systems, and Network Information Security Protection, Federal Aviation Administration, 14 Federal Register 67564, "Equipment, Systems, and Network Information Security Protection," August 21, 2024. (https://www.federalregister.gov/documents/2024/08/21/2024-17916/equipment-systems-and-network-information-security-protection) Specifically, the standards cover "propulsion output, propulsion controls, monitoring functions that track the health of the engine's systems, communication functions such as data buses and networks, and auxiliary equipment such as fuel, lube, or pneumatic subsystems with embedded electronics."

84. Equipment, Systems, and Network Information Security Protection, Federal Aviation Administration, 14 Federal Register 67564, August 21, 2024. (https://www.federalregister.gov/documents/2024/08/21/2024-17916/equipment-systems-and-network-information-security-protection)

85. U.S. Department of Transportation, Office of Inspector General, "FAA and Its Partner Agencies Have Begun Work on the Aviation Cyber Initiative and Are Implementing Priorities," September 2, 2020, pages 6-9. (https://www.oig.dot.gov/sites/default/files/FAA Aviation Cyber Initiative Final Report%5E09-02-20.pdf)

86. Ibid., pages 3 and 6-

87. U.S. Department of Transportation, Office of Inspector General, "FAA Has Made Progress but Additional Actions Remain To Implement Congressionally Mandated Cyber Initiatives," March 20, 2019, page 16. (https://www.oig.dot.gov/sites/default/files/FAA Cybersecurity Program Final Report%5E03.20.19.pdf)

88. U.S. Government Accountability Office, "Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks," October 9, 2020, page 29. (https://www.gao.gov/products/gao-21-86)

89. U.S. Government Accountability Office, "Air Traffic Control Modernization: Program Management Improvements Could Help FAA Address NextGen Delays and Challenges," November 2023, page 2. (https://www.gao.gov/assets/gao-24-105254.pdf)

90. U.S. Government Accountability Office, "Air Traffic Control Modernization: Program Management Improvements Could Help FAA Address NextGen Delays and Challenges," November 9, 2023. (https://www.gao.gov/products/gao-24-105254)

91. U.S. Department of Transportation, Federal Aviation Administration, "NextGen Annual Report Fiscal Year 2023," September 12, 2024, pages 4-6. (https://www.faa.gov/nextgen/NextGen-Annual-Report-2023.pdf)

92. U.S. Department of Transportation, Office of Inspector General, "FAA's Report on Air Traffic Modernization Presents an Incomplete and Out-of-Date Assessment of NextGen," April 30, 2024. (https://www.oig.dot.gov/sites/default/files/library-items/FAA%20NextGen%20Status%20Report_4.30.24.pdf)

93. Andrew Tangel, "Why Fixing New York Air Traffic Has Been a Bumpy Ride," *The Wall Street Journal*, October 24, 2024. (https://www.wsj.com/business/airlines/faa-air-traffic-congestion-new-york-4b3effb9)

94. Sydney Ember and Emily Steel, "Airline Close Calls Happen Far More Often Than Previously Known," *The New York Times*, August 21, 2023. (https://www.nytimes.com/interactive/2023/08/21/business/airline-safety-close-calls.html)

95. U.S. Department of Transportation, Bureau of Transportation Statistics, "On-Time Performance – Reporting Operating Carrier Flight Delays at a Glance," accessed March 26, 2025. (https://www.transtats.bts.gov/HomeDrillChart.asp); Data from each month in 2024 showed a consistent increase of U.S. airline traffic compared to the same months in 2023. See: U.S. Department of Transportation, Bureau of Transportation Statistics, "News and Statistical Releases," accessed March 26, 2025. (https://www.bts.gov/statistical-releases?field_effective_date_value=2024-01-01&field_effective_date_value_1=2025-02-13&combine&field_editorial_type_target_id=371&page=0)

96. U.S. Government Accountability Office, "Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks," October 9, 2020. (https://www.gao.gov/products/gao-21-86); Larry Grossman, "The Evolving Cybersecurity Landscape: Federal Perspectives on Securing the Nation's Infrastructure," December 2, 2021. (https://www.transportation.gov/evolving-cybersecurity-landscape-federal-perspectives-securing-nations-infrastructure)

97. Edward Graham, "FAA proposes new cyber rules for airplanes and aviation equipment," *NextGov*, August 21, 2024. (https://www.nextgov.com/cybersecurity/2024/08/faa-proposes-new-cyber-rules-airplanes-and-aviation-equipment/398964)

98. U.S. Department of Homeland Security, Transportation Security Administration, "Annual Report on Transportation Security: Fiscal Year 2022 Report to Congress," October 10, 2024, pages 2, 8, and 12. (https://www.tsa.gov/sites/default/files/tsa_annual-report-on-transportation-security-fy-2022_final_signed.pdf)

99. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years," May 7, 2023. (https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years)

100. Jiwon Ma, "TSA's Cybersecurity Requirements Prepare for Takeoff," *Foundation for Defense of Democracies*, March 13, 2023. (https://www.fdd.org/analysis/2023/03/13/tsa-cybersecurity-requirements-prepare-for-takeoff)

101. U.S. Department of Homeland Security, Transportation Security Administration, Information Circular, "Enhancing Surface Transportation Cybersecurity," December 31, 2021. (https://www.tsa.gov/sites/default/files/20211201_surface-ic-2021-01.pdf); Jonathan Greig, "TSA to change cybersecurity rules for pipelines following industry criticism," *The Record*, June 28, 2022. (https://therecord.media/tsa-to-change-cybersecurity-rules-for-pipelines-following-industry-criticism)

102. Jonathan Greig, "TSA to change cybersecurity rules for pipelines following industry criticism," *The Record*, June 28, 2022. (https://therecord.media/tsa-to-change-cybersecurity-rules-for-pipelines-following-industry-criticism)

103. Ibid.

104. U.S. Department of Homeland Security, Transportation Security Administration, Press Release, "TSA issues new cybersecurity requirements for airport and aircraft operators," March 7, 2023. (https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft)

105. U.S. Department of Homeland Security, Transportation Security Administration, Press Release, "TSA issues new cybersecurity requirements for passenger and freight railroad carriers," October 18, 2022. (https://www.tsa.gov/news/press/releases/2022/10/18/tsa-issues-new-cybersecurity-requirements-passenger-and-freight)

106. Suzanne Smalley, "White House to give aviation executives classified cyberthreat briefing, latest in series of industry meetings," *CyberScoop*, August 30, 2022. (https://cyberscoop.com/white-house-classified-threat-briefings-critical-infrastructure)

107. U.S. Department of Homeland Security, Transportation Security Administration, Press Release, "TSA issues new cybersecurity requirements for airport and aircraft operators," March 7, 2023. (https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-for-airport-and-aircraft)

108. Natalie B. Compton, "Hundreds of people bypassed parts of airport security in last year," *The Washington Post*, April 4, 2024. (https://www.washingtonpost.com/travel/2024/04/04/airport-security-tsa-stowaway)

109. U.S. Department of Homeland Security, Transportation Security Administration, Press Release, "TSA intercepts 6,678 firearms at airport security checkpoints in 2024," January 15, 2025. (https://www.tsa.gov/news/press/releases/2025/01/15/tsa-intercepts-6678-firearms-airport-security-checkpoints-2024)

110. U.S. Department of Homeland Security, Transportation Security Administration, Press Release, "2023 Year in Review: TSA highlights a year of innovation and improvements to security effectiveness, efficiency and the passenger experience," January 12, 2024. (https://www.tsa.gov/news/press/releases/2024/01/12/2023-year-review-tsa-highlights-year-innovation-and-improvements)

111. U.S. Department of Homeland Security, Science and Technology Directorate, "Feature Article: Reimagining Imaging at the Airport," January 7, 2025. (https://www.dhs.gov/science-and-technology/news/2025/01/07/feature-article-reimagining-imaging-airport)

112. U.S. Government Accountability Office, "Aviation Security Transportation Security Administration Could Further Improve Officer Engagement," February 2024, page 25. (https://www.gao.gov/assets/gao-24-106052.pdf)

113. Ibid., page 16.

114. U.S. Government Accountability Office, "Aviation Security Transportation Security Administration Could Further Improve Officer Engagement," February 2024, pages 24-25 (https://www.gao.gov/assets/gao-24-106052.pdf); U.S. Department of Homeland Security, Transportation Security Administration, Press Release, "2023 Year in Review: TSA highlights a year of innovation and improvements to security effectiveness, efficiency and the passenger experience," January 12, 2024. (https://www.tsa.gov/news/press/releases/2024/01/12/2023-year-review-tsa-highlights-year-innovation-and-improvements)

115. U.S. Government Accountability Office, "Aviation Security Transportation Security Administration Could Further Improve Officer Engagement," February 2024, pages 12 and 16. (https://www.gao.gov/assets/gao-24-106052.pdf)

116. U.S. Department of Homeland Security, "Transportation Security Administration Fiscal Year 2025 Congressional Justification," April 2024, page 134. (https://www.dhs.gov/sites/default/files/2024-04/2024_0318_transportation_security_administration.pdf)

117. Enhancing Surface Cyber Risk Management, 49 Federal Register 88488, November 7, 2024. (https://www.federalregister.gov/documents/2024/11/07/2024-24704/enhancing-surface-cyber-risk-management)

118. Chad Gorman and Steve Lorincz, "Impacts of Emergency Authority Cybersecurity Regulations on the Transportation Sector," *Testimony Before the United States House of Representatives Committee on Homeland Security Subcommittee on Transportation and Maritime Security*, November 19, 2024. (https://homeland.house.gov/wp-content/uploads/2024/11/2024-11-19-TMS-HRG-Testimony.pdf)

119. The White House, Office of the National Cyber Director, "Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information," June 2024, page 29. (https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/06/Cybersecurity-Regulatory-Harmonization-RFI-Summary-ONCD.pdf)

120. Ibid., page 12

121. Jiwon Ma, "Boeing's Cyber Incident Highlights Need for Greater Information Sharing," *Foundation for Defense of Democracies*, November 7, 2023. (https://www.fdd.org/analysis/2023/11/07/boeings-cyber-incident-highlights-need-for-greater-information-sharing); The White House, Office of the National Cyber Director, "Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information," June 2024, page 12. (https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/06/Cybersecurity-Regulatory-Harmonization-RFI-Summary-ONCD.pdf)

122. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)," accessed March 26, 2025. (https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia)

123. U.S. Government Accountability Office, "Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks," October 9, 2020. (https://www.gao.gov/products/gao-21-86)

124. U.S. Government Accountability Office, "Air Traffic Control Modernization: Program Management Improvements Could Help FAA Address NextGen Delays and Challenges," November 9, 2023. (https://www.gao.gov/products/gao-24-105254)

125. U.S. Government Accountability Office, "Air Traffic Control Modernization: Program Management Improvements Could Help FAA Address NextGen Delays and Challenges," November 9, 2023. (https://www.gao.gov/products/gao-24-105254)

126. National Institute of Standards and Technology, "Security and Privacy Controls for Information Systems and Organizations," September 23, 2020. (https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final); National Institute of Standards and Technology, "Security and Privacy Controls for Information Systems and Organizations, 5.1.1," November 7, 2023. (https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home)

127. National Institute of Standards and Technology, "Cybersecurity Framework," April 24, 2024. (https://www.nist.gov/cyberframework)

128. U.S. Department of Transportation, Federal Aviation Administration, "National Plan of Integrated Airport Systems (NPIAS) 2023-2027," September 30, 2022, page 13. (https://www.faa.gov/sites/faa.gov/files/npias-2023-2027-narrative.pdf)

129. U.S. Government Accountability Office, "Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks," October 9, 2020. (https://www.gao.gov/products/gao-21-86)

130. Jiwon Ma, "Boeing's Cyber Incident Highlights Need for Greater Information Sharing," *Foundation for Defense of Democracies*, November 7, 2023. (https://www.fdd.org/analysis/2023/11/07/boeings-cyber-incident-highlights-need-for-greater-information-sharing); Jonathan Grieg, "Experts push back on TSA's 24-hour cybersecurity incident reporting rule for aviation industry," *The Record*, August 28, 2022. (https://therecord.media/experts-push-back-on-tsas-24-hour-cybersecurity-incident-reporting-rule-for-aviation-industry)

131. The White House, Office of the National Cyber Director, "Request for Information on Cyber Regulatory Harmonization," July 19, 2023. (https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/06/Cybersecurity-Regulatory-Harmonization-RFI-Summary-ONCD.pdf)

132. The White House, Office of the National Cyber Director, "Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information," June 4, 2023, page 34. (https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/06/Cybersecurity-Regulatory-Harmonization-RFI-Summary-ONCD.pdf)

133. National Institute of Standards and Technology, "Cybersecurity Framework," accessed March 26, 2025. (https://www.nist.gov/cyberframework)

134. National Institute of Standards and Technology, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations," November 1, 2024. (https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final)

135. U.S. Government Accountability Office, "Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks," October 9, 2020. (https://www.gao.gov/products/gao-21-86)

About the Author

Jiwon Ma is a senior policy analyst at FDD's Center on Cyber and Technology Innovation, where she contributes to the CSC 2.0 project. Jiwon received a Master of International Affairs degree from Columbia University's School of International and Public Affairs and a B.A. in global studies from Lesley University.

ACKNOWLEDGMENTS

The author extends sincere thanks to the many experts across industry and government who generously shared their time, perspectives, and feedback throughout the research and drafting of this report, including FAA, TSA, and DoD experts, as well as Alan Burke, Igor Dubinsky, Esq., Lt. Col. James "Pharaoh" Hesson, David H. Hopfe, Ph.D, retired Col. USAF Craig Miller, Philip Niedermair, Dr. Georgianna Shea, Sam Singer, and Scott Tousley.

Special recognition goes to retired Rear Adm. Mark Montgomery and Annie Fixler for their guidance and encouragement throughout the preparation of this report. Their consistent support, clear thinking, and thoughtful engagement shaped the report at every stage.

While many experts helped refine the report, any errors in fact or judgment are the author's alone. Finally, the author would like to thank David Adesnik, John Hardie, and Tzvi Kahn for their rigorous edits; Katy Wickberg and Allie Shisgal for their coordination efforts; and Daniel Ackerman and Erin Blumenthal for the design and production of this report.

Cover illustration by Lilia Gaufberg/FDD

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

About CSC 2.0

CSC 2.0 is preserving the legacy and continuing the work of the Cyberspace Solarium Commission (CSC). Congress created the CSC in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences." The commission operated successfully for two and a half years, publishing its flagship report in March 2020 along with subsequent white papers. The CSC issued more than 80 recommendations to reform U.S. government structures and organization, strengthen norms and non-military tools, promote national resilience, reshape the cyber ecosystem, operationalize public-private collaboration, and preserve and employ military instruments of national power.

At the CSC's planned sunset, the commissioners launched the CSC 2.0 project to support continued efforts to implement outstanding CSC recommendations, provide annual assessments of the implementation of CSC recommendations, and conduct research and analysis on several outstanding cybersecurity issues identified during the commission's tenure.

For more information, visit **www.CyberSolarium.org**.

Co-Chairmen

Angus S. King Jr., U.S. Senator for Maine

Mike J. Gallagher, Former U.S. Representative for Wisconsin's 8th District

Distinguished Advisors

Frank J. Cilluffo, Director of Auburn University's Charles D. McCrary Institute for Cyber and Critical Infrastructure Security

Tom Fanning, Former Chairman, President, and CEO of Southern Company

Chris Inglis, Former National Cyber Director

Jim Langevin, Former U.S. Representative for Rhode Island's 2nd District

Patrick J. Murphy, Former Acting Secretary and Under Secretary of the U.S. Army & Former U.S. Representative for Pennsylvania's 8th District

Samantha F. Ravich, Chair of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

Ben Sasse, Former U.S. Senator for Nebraska

Suzanne Spaulding, Senior Adviser for Homeland Security at the Center for Strategic and International Studies

Partners

FDD

CSC 2.0

Preserving and Continuing the Cyberspace Solarium Commission