Aviation Must Respond to Cybersecurity Threats

By Paul Alp

In the world of commercial air transportation, regulations and best practices that improve safety are written in blood. As the jet age dawned, an informal metric for measuring the effectiveness of an airline’s safety culture was whether it had experienced a fatal accident. As the number of fatal accidents from different causes rose, the industry adopted a collective change in mindset. Undertaking critical self-analysis and implementing proactive safety countermeasures, either on its own initiative or in concert with regulators, the industry developed robust measures to mitigate risk. The strong safety record of major commercial operators today demonstrates the success of this approach, which reflects an evolution from the simplistic view of “it hasn’t happened to us yet, so we’re safe” to “let’s think proactively and develop comprehensive mechanisms that will systematically mitigate risk.”

With respect to cybersecurity, the industry arguably has traveled back in time. Stakeholders often believe that because a major cybersecurity breach has not happened to them yet, they are taking appropriate measures. However, the industry must respond to the ever-evolving threat landscape and develop comprehensive strategies to safeguard against potential vulnerabilities.

The Local Future of the Low-Altitude Airspace

By William Goodwin and Tyler Finn

A police station in Chula Vista, California, receives a call about an assault in progress. Less than two minutes later, a buzz overhead signals the arrival of a drone, just in time to follow a suspect fleeing down the street. Across the country, in coastal North Carolina, state police route traffic around flooded freeways in the wake of a hurricane, informed by live video feeds from drones operating miles away. Approximately halfway in between, in the Choctaw Nation, a drone takes off from the police station, ready to assist in various public safety and crowd management activities. The future of low-altitude airspace is rapidly evolving, driven by advances in technology and the growing application of drones in law enforcement and emergency response.

continued on page 13

continued on page 19
As we close out another year and begin a new one, I reflect on 2018, which was a great year for the Forum on Air & Space Law. We had five in-person conferences, as well as numerous committee calls and webinars. We grew our membership even as the ABA lost members. More members of the Forum are getting involved, learning new things, meeting new people, and strengthening friendships. This is what being a member of the Forum is all about. And fun—we’re always about having fun.

While the Forum is going strong, the ABA itself is facing headwinds. As with many membership organizations, it is difficult to attract young people to become members and get involved, putting financial pressure on the organization. The ABA is working to address the issues on all fronts, but it is a challenging task. It has adopted the new membership model, with simpler, cheaper membership dues and more benefits for members. It is also working through a reorganization of the ABA itself. We are all hopeful that the efforts of ABA management and the leaders of the Sections, Divisions, and Forums will turn the tide, but there are challenges. Many of you will undoubtedly have noticed issues with the website this fall. The ABA launched a new website that was intended to modernize the way the ABA interacts with its members and the public. Unfortunately, there were issues and the website has not worked as intended. For any Forum members adversely affected, we apologize. Our Technology Committee is working with the ABA to set things right as soon as possible.

As members of the ABA and the Forum, I know we are all concerned about the health of the ABA and the knock-on effect to the Forum. We all have a part to play in this effort. It’s not up to “them,” it’s up to us. Encourage your friends and coworkers to join the ABA and/or the Forum. Lobby your company or law firm about the benefits of membership. Bring a colleague or two, especially a young lawyer, with you to the next conference or committee call you attend and introduce them to others. I suspect that each Forum member could introduce at least one new Forum and/or ABA member. That would have a significant impact. The Forum has grown in membership among more seasoned lawyers, thanks to our practice committees. If we add more committees, we’ll add more members as well.

This call to action is on every level—committee growth, articles for The Air & Space Lawyer, growing the membership of the Forum, and getting involved in whatever way you enjoy. We are only as good as our members and our members are great, but we can do more and do better.

Thanks for all you do!

Andrea J. Brantner
Chair, Forum on Air & Space Law
This issue’s two cover articles focus on the intersection between aviation and cutting-edge technology. First, Paul Alp of Jenner & Block analyzes cybersecurity threats to aviation and how the industry and regulators should respond. The author notes that aviation is a particular target for increasingly sophisticated cyber threats and that the FAA’s resources are strained as it seeks to keep pace. He cautions the aviation industry not to view cybersecurity only as a privacy risk, but rather as a safety threat. He urges industry to apply the same rigor and priority to combating cyber threats that it attributes to its safety mission. Failure to do so, he warns, could be painful and expensive, if not catastrophic.

Our second article, by William Goodwin and Tyler Finn of AirMap, focuses on the management of drone traffic in low-altitude airspace. The authors describe the innovative ways in which drones, with the benefit of unmanned traffic management (UTM) technology, are being deployed to support law enforcement, hurricane relief, and for commercial purposes. They describe the DOT’s Unmanned Aircraft System Integration Pilot Program, which enables states and municipalities to play a role in the management of drone operations in “local (low-altitude) airspace.” As a legal matter, this raises complex preemption issues. The authors argue that states and localities must be able to impose “time, place, and manner” regulations on the use of local airspace, particularly as we move toward a future in which unmanned aircraft, including package delivery drones, become commonplace.

Our next article, by Laura Montgomery, reviews the current, evolving state of commercial space regulation. The author notes that although the Trump administration included space transportation among its targets for regulatory streamlining, its proposals would actually increase some regulatory requirements while reducing others. Space transportation is subject to regulation by multiple federal agencies, including the FAA, NASA, the Federal Communications Commission, and the National Oceanic and Atmospheric Administration. The future of space regulation is further complicated by the conflicting visions of the administration and Congress.

Finally, Roy Goldberg of Stinson Leonard Street analyzes the scope of express federal preemption of airline “services” under the Airline Deregulation Act. He argues that, among other things, the provision of air transportation between airports, passenger reservations and the issuance of tickets and seat assignments (including the use of airline websites and mobile apps), the boarding of passengers, and the treatment of passengers during a tarmac delay are all preempted “services” under the Act. Thus, state and local law-based claims against an air carrier arising from the provision of (or failure to provide) such services would be preempted. He notes that the Ninth Circuit, following its decision in Charas v. Trans World Airlines, continues to adhere to a narrower interpretation of “service” preemption despite the U.S. Supreme Court’s decision in Rowe v. New Hampshire Motor Transport Ass’n.

In closing, I wish to thank the members of The Air & Space Lawyer’s editorial board for their excellent work on our publication over the past year. They are Brent Connor (Managing Editor), Ronce Almond, Terence Boga, Lisa Harig, Andrea Harrington, Graham Keithley, Jeff Klang, Naveen Rao, John Saba, Kathy Yodice, and our ABA editor, Melissa Vasich.

David Heffernan
Editor-in-Chief
Expanding and Streamlining: Space Regulation under President Trump

By Laura Montgomery

On March 23, 2018, President Trump announced a regulatory streamlining agenda directed at space with a new National Space Strategy. The strategy "prioritizes regulatory reforms that will unshackle American industry and ensure we remain the leading global provider of space services and technology." On May 24, 2018, the president signed Space Policy Directive-2 (SPD-2) to set a new direction for agencies that regulate commercial space activities, including the Secretaries of Transportation and Commerce. They oversee commercial space transportation and space remote sensing, respectively. SPD-2 does not provide guidance to the Federal Communications Commission (FCC), an independent agency, in its regulation of space satellites. The following month, the president signed Space Policy Directive-3 (SPD-3) regarding space traffic situational awareness and management.

This article reviews the president's regulatory streamlining proposals, agency steps to implement them, and some of the legislative responses. The president's space policy proposes more than mere streamlining. It also seeks to promote space traffic management. Although characterized as streamlining, the agency's implementation proposals would reduce some regulatory requirements and increase others.

Transportation to and from Orbit

Under authority delegated from the Secretary of Transportation, the Federal Aviation Administration (FAA) authorizes and regulates two legs of commercial space transportation, namely, launch and reentry. SPD-2 directs the Secretary of Transportation to review the FAA's regulations governing launch and reentry by February 1, 2019, for consistency with the president's goals. Those goals include that "regulations adopted and enforced by the executive branch promote economic growth; minimize uncertainty for taxpayers, investors, and private industry; protect national security, public-safety, and foreign policy interests; and encourage American leadership in space commerce."

The executive branch's Unified Agenda, a list of agencies' rulemaking plans, shows that the FAA intends to publish a notice of proposed rulemaking (NPRM) in February 2019 to carry out the president's directive. In addition, the president requires the Secretary of Transportation to consider replacing prescriptive with performance-based criteria in the FAA's launch and reentry licensing process, and requiring a single license for all types of commercial spaceflight launch and reentry operations.

Prescriptive and Performance-Based Regulations

A performance-based regulation requires an outcome. A prescriptive requirement tells a regulated entity how to achieve that outcome by prescribing the means of compliance. An FAA requirement for human spaceflight provides a good example of a performance-based requirement. In 14 C.F.R. section 460.5(b), the FAA requires that "[e]ach member of a flight crew [aboard a licensed or permitted launch or reentry] must demonstrate an ability to withstand the stresses of space flight, which may include high acceleration or deceleration, microgravity, and vibration, in sufficient condition to safely carry out his or her duties so that the vehicle will not harm the public." "In sufficient condition" to carry out one's duties shows that a commercial spaceflight crew member need not be a superhuman astronaut. That the flight "may" include high acceleration suggests that all flights might not include that particular stress of spaceflight. If a capsule gets near space via a balloon, the operator might not need to demonstrate to the FAA that the crew member can withstand high acceleration. The requirement, in other words, is tailored to the technology, and an applicant need only demonstrate that the crew can withstand the stresses of a particular vehicle.

However, what performance regulations often do not say is what a successful demonstration of compliance looks like. Does the flight crew have to undergo the anticipated stresses? How many times? To what level of reliability? Nine times out of 10, or 99 times out of 100? The answers to these questions may reveal hidden costs of the regulation. While each applicant gets to make a case for its vehicle, operators of similar vehicles should be treated similarly. One crew member should not be required to undergo hours of high acceleration while another is subjected to only minutes.

Consistency and fairness suggest that these unwritten demonstration "requirements" be made public. If the FAA finds one method of demonstrating compliance acceptable for certain circumstances, it could let everyone else...
know by publishing that method in an advisory circular. Then, other operators with a similar flight profile would know that they could follow that method without long negotiations with the agency. Alternatively, another operator might have something less costly in mind and could make its case to the FAA for using a different demonstration. That demonstration could also be shared. Publication, of course, carries concerns regarding proprietary information, but those can be resolved.

Single License for Launch and Reentry
Under current FAA regulations, an operator must obtain two different licenses for its launch and reentry activities. For example, SpaceX must obtain a launch license for the launch of its Falcon launch vehicles, and a reentry license for the reentries of its Dragon reentry vehicles. Requiring two licenses is a matter of administrative convenience, not legal necessity. The FAA could issue a single piece of paper rather than two as long as it was clear that the license applied just to launch and reentry, and not to activities on orbit.

Confusion could result from the grant of a single license for two different activities. If an operator has a single license for leaving the planet and for returning, that could lead some to think that the orbital transportation activity in the middle must also be covered. If it were not covered, there would be a “gap” in regulatory coverage, and nature is not the only one to abhor a vacuum. Regulators might want an expansive interpretation to increase their authority. Industry might want the expansion to extend the reach of the U.S. government’s potential payment of excess claims described in the Commercial Space Launch Act. However, activities on orbit are not eligible for such potential payment of excess claims by the U.S. government.

Such confusion seems unlikely now while things are clear, but the incentives for both regulators and industry to misunderstand the scope of a “single” license with this gap in the middle seems great. Past examples of such confusion include how the Office of Commercial Space Transportation issued licenses in the 1990s that governed prelaunch activity on the ground even before the passage of the legislative amendments that granted the Secretary such authority.

Accordingly, if the FAA’s 2019 NPRM allows for a single license, the regulations should clarify when launch and reentry begin and end. Current regulations provide that clarity, but the FAA should take care to maintain it, both in the license orders themselves and in its regulations.

Activities on Orbit
Remote Sensing
The Secretary of Commerce has commenced a process for regulatory streamlining of its remote sensing regulations. Anyone operating a remote sensing system in space must obtain a license to do so from the Secretary of Commerce, who delegated this task to the National Oceanic and Atmospheric Administration (NOAA). NOAA’s regulations define a remote sensing system as one that includes “any device, instrument, or combination thereof, the space-borne platform upon which it is carried, and any related facilities capable of actively or passively sensing the Earth’s surface, including bodies of water, from space by making use of the properties of the electromagnetic waves, emitted, reflected, or diffracted by the sensed objects.”

NOAA carries out its role under regulations codified at 15 C.F.R. part 960. NOAA last updated its regulations in 2006, but is now considering a rulemaking to change its regulations. In response to the president’s goals, NOAA wants to relieve industry of unnecessary regulatory burdens and sought input from stakeholders and the public about ambiguities in the current regulations through an advance notice of proposed rulemaking (ANPRM). The ANPRM invited discussion of streamlining, but also raised the question of whether NOAA should increase the scope of its regulation.

To advance the streamlining initiative, NOAA requested comments on whether it should reduce oversight of and requirements for remote sensing systems that pose less risk. NOAA contemplated that any systems it could identify as posing only a de minimis risk would be subject to an expedited review process, less restrictive license conditions, and less burdensome compliance requirements. It sought comments on factors relevant to identifying review categories, processes for different categories, and on license conditions and compliance requirements. NOAA also sought input on whether such a strategy was advisable, and if so, how to implement it. Commenters’ responses to these proposals have generally been positive.

NOAA also requested comments on proposals that could increase the regulatory burden on industry. For example, NOAA asked whether it should “consider a license condition requiring licensees to obtain some level of insurance to cover [an operator’s] potential liabilities.” Commenters who addressed this issue advised against such a requirement, noting both that operators already obtain insurance and that the FAA’s liability regime covers liability arising out of launch. In addition, a review of the statutory authority does not show that Congress gave NOAA authority to impose insurance requirements on its licensees.

NOAA currently only requires operators capable of sensing the surface of the Earth to obtain a license. In the ANPRM, the agency stated that it is also considering
licensing operators that sense different spectral bands. NOAA’s authority—or lack thereof—is unclear on this point. On the one hand, the statute defines “land remote sensing” to mean “the collection of data which can be processed into imagery of surface features of the Earth from an unclassified satellite or satellites, other than an operational United States Government weather satellite.”¹⁶ The spectral bands likely do not satisfy the congressional requirement that they be “surface features of the Earth.” On the other hand, the licensing provisions in sections 60121 and 60122 of the statute address something different than “land” remote sensing. They authorize the agency to license “private sector parties to operate private remote sensing space systems” and forbid any U.S. person from operating “any private remote sensing space system” without a license.¹⁷

The agency asked for comment on how to define a private remote sensing space system. Might NOAA consider the operation of a private remote sensing system as broader than the statutorily defined “land remote sensing”? NOAA’s notice says it wants to discuss changes to its regulations within the confines of its statutory authority. Is it considering broadening its interpretation of its statutory mandate so as to license remote sensing of more than surface features of the Earth? This does not appear to be consistent with the agency’s regulatory streamlining goal.

### Space Traffic

The Department of Defense currently provides commercial and governmental entities what is called “space situational awareness” (SSA). SPD-3 defines SSA to mean the knowledge and characterization of space objects and their operational environment. The directive defines a more burdensome “space traffic management” (STM) as the planning, coordination, and on-orbit synchronization of activities to enhance the safety, stability, and sustainability of operations in the space environment. The difference between the two is clear. With SSA, the government may provide a private operator notifications or warnings. With STM, the government would be able to synchronize, coordinate, and tell you to move over.

The directive contains some tensions. On the one hand, it wants debris regulations streamlined. On the other hand, it wants more government oversight. In order to facilitate commercial leadership in SSA and STM, section 4(c) mandates that the U.S. government reduce regulatory burdens that could inhibit commercial sector growth and innovation. At the same time, section 4(f) establishes a goal for regulatory agencies of adopting STM standards and best practices as domestic regulatory frameworks: “A critical first step in carrying out that goal is to develop U.S.-led minimum safety standards and best practices to coordinate space traffic. U.S. regulatory agencies should, as appropriate, adopt these standards and best practices in domestic regulatory frameworks and use them to inform and help shape international consensus practices and standards.”¹⁸

The FAA, the FCC, and NOAA all have orbital debris mitigation requirements in their regulations, namely, requirements to prevent the creation of debris. None of these agencies has authority for mandatory STM. The FAA has a new debris mitigation rulemaking listed on its agenda.¹⁹ That rulemaking, which has been on the agenda for a number of years, would update the FAA’s existing debris “mitigation regulations to more-closely align with the U.S. Government Orbital Debris Mitigation Standard Practices, and would update current launch collision avoidance regulations to match U.S. Air Force Space Command (AFSPC) practice.”²⁰ In short, the FAA proposes to impose preventive mitigation measures rather than active management of operations on orbit.

It will be interesting to see how the agencies reconcile these apparently conflicting goals. On the one hand, the president charges the agencies with reducing regulatory burdens that could inhibit growth and innovation. On the other hand, the agencies should adopt new requirements for STM. The latter will require legislative action to grant an agency that authority.

The House of Representatives’ Committee on Science, Space, and Technology approved a bill, the American Space Situational Awareness and Framework for Entity Management Act (American Space SAFE Management Act),²¹ directing the Secretary of Commerce to establish a civil SSA program to provide SSA data to, and obtain SSA data from, a state or its political subdivision, U.S. or foreign commercial entities, or a foreign government. The proposal would let the Secretary decide what constitutes a “basic” set of SSA services for which the Secretary would not charge a fee. More significantly, the bill proposes that the Secretary of Commerce develop a voluntary STM program, to include the development of voluntary guidelines and a voluntary pilot program. It would not, in other words, grant the Secretary of Commerce the kind of authority SPD-3 appears to anticipate.

The bill would also require the Secretary to report to the appropriate congressional committees on progress on legally binding requirements, even though the bill does not appear to provide the Secretary authority to develop legally binding requirements. Perhaps “legally binding” standards refers to those developed by foreign governments or those imposed on.

---

¹⁶ The Air & Space Lawyer, Volume 31, Number 4, 2018. © 2018 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.
government contractors through the procurement process. Thus, if NASA, for example, hired a private company to engage in work on orbit, NASA might by contract require the company to follow its debris guidelines. Those requirements would then be legally binding. And, of course, if a foreign regulator imposed STM requirements, those could be legally binding on anyone under its jurisdiction as well. The committee’s approval of the bill was the last activity on the bill. As of October 2018, the House had not yet voted on it.

**Article VI of the Outer Space Treaty**

With the advent of new space activities, the space law community frequently debates the question of a treaty requirement that signatories authorize and continuously supervise the acts of their nationals in outer space. The SPDs are noticeably silent on this issue, despite the uncertainty it has created within industry and government.

The Outer Space Treaty went into effect in 1967 and has been signed by the United States, the former USSR, the United Kingdom, and a host of other spacefaring countries. The treaty provides a framework for international space law. It primarily addresses government activity, prohibiting weapons of mass destruction in space, barring claims of sovereignty, and stating that outer space shall be used for peaceful purposes. Article VI of the treaty, however, states that nongovernmental entities’ activities in space “shall require authorization and continuing supervision by the appropriate State Party to the Treaty.”

The commercial space sector is experiencing a renaissance of new activity. Asteroid mining companies such as Planetary Resources pursue ambitious plans. Entrants in the Lunar XPRIZE continue their efforts to create lunar rovers—even after the prize has officially ended. Bigelow Aerospace co-located one of its expandable habitats with the International Space Station. They all face many obstacles, including technical, legal, and financial. A misinterpretation of article VI is one such obstacle—but it is an unnecessary one.

Many in both government and industry believe that article VI prevents private U.S. companies from operating in outer space without explicit authorization or supervision. On this basis—and not on the basis of sound policy reasoning—some seek the creation of a new regulatory regime. The Obama administration interpreted article VI to require the government’s authorization of any and all nongovernmental activities in outer space. In 2016, the FAA indicated that it may deny a private entity access to space because of article VI. But these interpretations, which claim the government may deny private operators access to space just because they are unregulated, are flawed.

Article VI does not say that either all or any particular activity must be authorized. Instead, it leaves decisions regarding what activities require regulation to the member states. Most significantly, the FAA’s position ignores Supreme Court jurisprudence regarding non-self-executing treaties. Article VI is not “self-executing” under U.S. law. In other words, it does not create an obligation or a prohibition on the private sector unless and until Congress passes a law requiring the regulation of a particular space activity. This has been the law from the earliest days of the republic to the present. In 2008, the Supreme Court held in Medellin v. Texas that not even the president, with his constitutionally granted foreign policy authority, could execute a non-self-executing treaty provision, and thus the treaty in question did not “automatically constitute binding federal law.”

In short, regulatory agencies do not have the authority, without congressional legislation, to use article VI to deny a nongovernmental entity access to space. None of the policy directives has taken advantage of the opportunity to apply Medellin and thus put this question to bed. The president could announce that the administration recognizes that, under existing law, article VI of the Outer Space Treaty does not prohibit private space activities unless and until Congress enacts implementing legislation. Perhaps the next SPD will do so.

**Conclusion**

The president’s commercial space policy is playing out right now. February 2019 should reveal the extent of the FAA’s streamlining and whether the agency will initiate a rulemaking to add requirements. NOAA’s ANPRM, where it contemplated adding requirements, shows that space regulators may try to increase regulatory burdens in some areas while decreasing them in others. As of fall 2018, the state of play for space situational awareness and space traffic management remains murky. The White House and the House Science Committee bill appear to have conflicting visions, and the administration’s proposals appear to require new legislative authority. Finally, the administration has the opportunity to reduce regulatory uncertainty without increasing regulatory burdens with a clarifying executive order regarding article VI of the Outer Space Treaty. We may have to wait and see if it takes advantage of the opportunity to do so.

**Endnotes**

Passenger and cargo airlines confronting class actions, state and local government investigations, or other forms of judicial or administrative proceedings enjoy qualified federal statutory immunity granted by the preemption clause in the Airline Deregulation Act of 1978 (ADA), currently codified at 49 U.S.C. section 41713(b), with regard to claims directly or indirectly related to the “price, route, or service of an air carrier.” However, the lack of a definition of “service of an air carrier” in the ADA has created uncertainty regarding whether or not particular claims are preempted. Fortunately, both long-standing and recent court decisions offer meaningful instruction for determining whether an airline act is a covered “service,” including the following four guideposts:

1. Air transportation between two airports is a “service,” and therefore state and local law claims arising from the failure of an airline to operate a flight should be preempted as long as the carrier provides an alternative flight or refund, pursuant to its contract of carriage.
2. “Service” includes the process of taking passenger reservations and issuance of tickets and seat assignments, including the use of websites and mobile apps, and the consumer privacy issues that are an inherent part of these activities, according to most courts.
3. The process of “boarding” passengers is a “service,” according to most courts.
4. The treatment of passengers during a tarmac delay is a “service.”

The ADA Preemption Clause
Section 41713(b) states that, unless otherwise provided, “a State, political subdivision of a State, or political authority of at least 2 States may not enact or enforce a law, regulation, or other provision having the force and effect of law related to a price, route, or service of an air carrier.”

In Morales v. Trans World Airlines, Inc., the U.S. Supreme Court held that the ADA preempted Travel Industry Enforcement Guidelines of the National Association of Attorneys General, which regulated the content and format of airline fare advertising. The Court emphasized that the phrase “relating to” as used in the ADA is “a broad one—to stand in some relation; to have bearing or concern; to pertain; refer; to bring into association with or connection with,” Black’s Law Dictionary 1158 (5th ed. 1979)—and the words thus express a broad pre-emptive purpose. A state law could “relate to” airline prices, routes, or services even if the state law did not directly affect those activities. The Court similarly concluded that ADA preemption could apply to “laws of general applicability.”

The Morales Court acknowledged that “[s]ome state actions may affect [airline services] in too tenuous, remote, or peripheral a manner” to be preempted. For example, the relationship of “state laws against gambling and prostitution” to airline prices, routes, and services would be too tenuous, remote, or peripheral. This implies that a broad range of state and local laws of general applicability exist that are sufficiently connected to airline prices, routes, or services (unlike laws against gambling and prostitution) to fall under the preemption umbrella. Nevertheless, for some courts, personal injury tort claims are not preempted because the connection of such claims to airline prices, routes, or services is too tenuous, remote, or peripheral.

Congressional Intent behind the Preemption Clause
Congress’s purpose in enacting the ADA preemption clause was to ensure “maximum reliance on competitive market forces,” thereby stimulating “efficiency, innovation, and low prices” as well as “variety” and “quality.” Congress sought to “ensure that the States would not undo federal deregulation with regulation of their own.”

In American Airlines, Inc. v. Wolens, the U.S. Supreme Court held that claims under the Illinois Consumer Fraud and Deceptive Business Practices Act relating to American’s frequent flyer program were preempted because they “relate[d] to ‘rates,’ i.e., American’s charges in the form of mileage credits for free tickets and upgrades, and to ‘services,’ i.e., access to flights and class-of-service upgrades unlimited by retrospectively applied capacity controls and blackout dates.” The Court stated that preemption was required in “light of the full text of the preemption clause, and . . . the ADA’s purpose to leave largely to the airlines themselves, and not at all to States, the selection and design of marketing mechanisms appropriate to the furnishing of air transportation services.” The Court added that “Congress could hardly have intended to allow the...
States to hobble [competition for airline passengers] through the application of restrictive state laws.”

Four Judicial Beacons for Interpreting Air Carrier “Service”

Air Transportation

If a state or local law claim against an airline relates to the transportation of passengers or cargo, it likely falls under the “service” language in the ADA. In the most recent U.S. Supreme Court decision concerning ADA preemption, Northwest, Inc. v. Ginsberg, the Court ruled that an airline frequent flyer program related to “services,” because it involved “access to flights and to higher service categories.” Prior to Ginsberg, the Fifth Circuit, in its en banc decision in Hodges v. Delta Airlines, Inc., defined “service” to include “items such as ticketing, boarding procedures, provision of food and drink, and baggage handling, in addition to the transportation itself.” More recently, the Fifth Circuit, in 2017, affirmed a district court decision that the ADA preempted a tort claim relating to an airline’s refusal to transport big game wildlife. The district court had emphasized that the “Fifth Circuit’s definition of service includes not only ‘baggage handling,’ but also, ‘the transportation’ of passengers and cargo, and the ban on big game trophies ‘is a refusal to provide transportation.’”

Even if a state or local law claim relates to airline transportation (or another airline “service”) it still may not be preempted by the ADA if the claim merely seeks to enforce an airline’s “self-imposed” contractual obligation. In Wolens, the Supreme Court established a narrow exception to preemption by declining to “read the ADA’s preemption clause . . . to shelter airlines from suits alleging no violation of state-imposed obligations, but seeking recovery solely for the airline’s alleged breach of its own, self-imposed undertakings.” Importantly, however, only alleged contract breaches that fall within the Wolens exception survive express ADA preemption. For example, in Sanchez v. Aerovias De Mexico, S.A. De C.V., the Ninth Circuit considered a breach of contract claim where the plaintiff did not cite any provision in the contract creating the defendant’s obligation. The court held that the claim could not proceed under the Wolens exception because, “[t]here being no contractual obligation to advise passengers about Mexico’s tourism tax, or to not to collect it from those who are exempt, or to refund it to exempt passengers from whom it was nevertheless collected, [the plaintiff’s] claims against [the defendant] may not proceed.” If a breach of contract claim seeks to “use state law to avoid the part of the contract that limits the carrier’s liability,” that claim is preempted. Similarly, in Howell v. Alaska Airlines, Inc., the court held that the ADA preempted claims for refunds by airline customers unable to use tickets that were explicitly nonrefundable. The plaintiffs were “attempting to enlarge or enhance their agreements with Alaska based on the laws or policies of this state.”

Passenger Reservations and Issuance of Tickets and Seat Assignments, including Use of Websites and Mobile Apps

Airline activity in enabling and facilitating air travel reservations and ticket issuance and modifications, as well as airline acts (and omissions) relating to consumer privacy, are also a preempted “service” as most courts construe that term. In 2005, a federal district court held that the ADA preempted claims that JetBlue violated the state and common laws by transferring personal information of passengers to a data mining company working with the Transportation Security Administration (TSA). The court applied a three-part test for deciding that a state law claim relates to an airline service: First, is the activity an airline service; second, does the claim affect the airline service directly or remotely; and, third, is the allegedly tortious conduct reasonably necessary to provide the airline service? In finding that the test was satisfied, the court concluded that (1) “the relevant activity . . . is the provision of reservations and the sale of tickets to travel with JetBlue,” which is an airline service; (2) “an attempt to regulate the representations and commitments that JetBlue makes in connection with reservations and ticket sales directly affects the airline’s provision of those services”; and (3) “the communication of company policy concerning data collection and disclosure is reasonably necessary to the facilitation of reservations and ticket sales.”

In Privacy Rights Clearinghouse v. JetBlue Airways Corp., a California appellate court similarly found that the ADA preempted a challenge to JetBlue’s conduct in releasing passengers’ personal information because it related to an airline “service.” The court found that the claims “clearly” intruded upon or affected the Department of Transportation’s (DOT’s) regulation (or the airline’s self-regulation) of air fares and other rates, routes, or services. Specifically, DOT “regulations expressly govern an airline’s collection of passenger information (intended to be used after an aviation disaster) and the circumstances in which an airline must divulge that data to a government agency.”

In People ex rel. Harris v. Delta Air Lines, Inc., the California appellate court held that the ADA preempted a claim by the state that the lack of a privacy policy posted on Delta’s mobile app violated the California Online Privacy Protection Act (OPPA). The OPPA required that operators of a commercial website or online service post
a privacy policy that informed California-based consumers of the website’s or online service’s information practices with regard to consumers’ personally identifiable information, and to abide by its policy.

The privacy policy, among other things, had to: (1) identify the categories of personally identifiable information that the operator collects through the website or online service about individual consumers who use or visit its commercial website or online service, and the categories of third-party persons or entities with whom the operator may share that personally identifiable information; and (2) disclose whether other parties may collect personally identifiable information about an individual consumer’s online activities over time and across different websites when a consumer uses the operator's website or online service.

To facilitate access to its services by actual and potential passengers, Delta maintained a commercial website (Delta.com) and a mobile app (Fly Delta) that passengers used to check-in online for flights, view reservations for air travel, rebook canceled or missed flights, pay for checked baggage, track checked baggage, access a frequent flyer account, take photos, or save a user’s geolocation. Whereas the app allowed customers to send and receive information over the Internet and collected certain personally identifiable information about individual customers residing in California, Delta had not posted a readily accessible privacy policy concerning the personally identifiable information collected from users of the Fly Delta app, either via the app itself, the platform stores from which the app could be downloaded, or on the Delta.com website.

California sued Delta in state court seeking injunctive and monetary damages for the airline’s failure to have a conspicuously posted privacy policy reasonably accessible to consumers within the carrier’s mobile app. California specifically alleged that Delta’s failure to have the privacy policy constituted “unlawful, unfair, or fraudulent business acts and practices” in violation of the OPPA and California’s unfair competition law. In affirming dismissal of the complaint, the appellate court held that enforcement of the OPPA “relat[ed] to Delta’s services.” Specifically, the “Fly Delta mobile application, selected and designed to facilitate access to the airline’s services, is a marketing mechanism ‘appropriate to the furnishing of air transportation services.’” The app could “be used to check-in for an airplane flight, view reservations for air travel, rebook cancelled or missed flights, pay for checked baggage, track checked baggage, [and] access a user’s frequent flyer account.”

The court also found that the OPPA obligations “would have a significant impact upon the airline[s] ability to market [its] product [through its Fly Delta mobile application], and hence a significant impact upon the fares they charge.” In addition, if “each State were to require Delta to comply with its own version of the OPPA, it would force Delta to design different mobile applications to meet the requirements of each State.” Indeed, “enforcement of the OPPA’s privacy policy requirements might well make it impossible for an airline to use a mobile application as a marketing mechanism at all.”

**State and local efforts to regulate what occurs during a tarmac delay should be preempted as relating to an air carrier “service.”**

**The Process of “Boarding” Passengers**

Airl ine acts and omissions relating to boarding of passengers also should be encompassed within the term "service." In Smith v. Comair, Inc., the Fourth Circuit held that tort claims “based in part upon [an airline’s] refusal of permission to board” the aircraft are preempted because “boarding procedures are a service rendered by an airline.” The plaintiff was allowed to board the first leg of his journey in Roanoke, Virginia, without producing his photo ID because the airline agent failed to ask for it. When the plaintiff attempted to board the second leg in Cincinnati on his way to Minneapolis, he was denied boarding because he did not have his ID. The plaintiff claimed that the airline was at fault because had he been asked for his ID in Roanoke he would have fetched it from his car in the airport parking lot. The court held that the claim was preempted because it related to the “service” of boarding, and the airline was entitled to deny boarding given FAA regulations which, for safety reasons, require that a passenger have a photo ID to board an aircraft. The court stated that “airlines must be accorded broad discretion in making boarding decisions related to safety. Allowing [the plaintiff’s] claim to proceed would frustrate this important federal objective. Airlines might hesitate to refuse passage in cases of potential danger for fear of state law contract actions claiming refusal to transport.”

**Treatment of Passengers during a Tarmac Delay**

The DOT strictly regulates tarmac delays from a federal perspective. However, efforts by state and local governments to regulate what occurs during a tarmac delay should be preempted as relating to an air carrier “service.” In Air Transport Ass’n of America, Inc. v. Cuomo, the Second Circuit held that the ADA preempted a New York law which required airlines to provide water and other items during lengthy tarmac delays because it “substitut[ed] New York’s commands for competitive market forces, requiring airlines to provide the services that New York specifies during lengthy ground delays.”
Caution: The Ninth Circuit’s Narrow Definition of “Service”

As a general rule, airlines seeking to use ADA preemption as a defense fare better in federal court rather than state court. However, an exception still exists for states within the Ninth Circuit, including Alaska, Arizona, California, Hawaii, Idaho, Montana, Nevada, Oregon, and Washington. The Ninth Circuit has adopted a very narrow view of what constitutes a “service.” In Charas v. Trans World Airlines, Inc., the Ninth Circuit stated that “service” refers “to such things as the frequency and scheduling of transportation, and to the selection of markets to or from which transportation is provided” (as in, “This airline provides service from Tucson to New York twice a day.”). The court added that to “interpret ‘service’ more broadly is to ignore the context of its use; and, it effectively would result in the preemption of virtually everything an airline does. It seems clear to us that that is not what Congress intended.”

The court further stated that there was no legislative history to support the position that “service” included “the dispensing of food and drinks, flight attendant assistance, or the like.” Although courts and commentators predicted that the Ninth Circuit would broaden its definition of “service” following the U.S. Supreme Court’s 2008 decision in Rowe v. New Hampshire Motor Transport Ass’n, this has not yet happened. Rather, in the 2016 decision in National Federation of the Blind v. United Airlines Inc., a three-judge Ninth Circuit panel held that an airline’s automated airport terminal ticketing kiosks were not a “service” within the meaning of the ADA. The court reasoned that kiosks were not prices, schedules, origins, or destinations of point-to-point transportation of passengers. To the extent that California’s antidiscrimination laws regulated kiosks, they regulated an amenity and not the provision of air transportation. Although kiosks are convenient for passengers, they are not services in the public utility sense. The panel noted that other circuits had interpreted “service” more broadly, but claimed that the Charas definition was better, and that nothing in Rowe was so “clearly irreconcilable” with Charas “as to allow a three-judge panel to overrule” the en banc decision in Charas. Accordingly, if an airline wants a broader definition of “service” in a case filed in one of the Ninth Circuit states, it may want to try to have the matter heard in state court if possible. State courts within the Ninth Circuit are not bound by Ninth Circuit precedent.

Endnotes

3. Id. at 383.
4. Id. at 384.
5. Id. at 386.
6. Id. at 390.
7. Id.
8. See Montalvo v. Spirit Airlines, 508 F.3d 464, 475 (9th Cir. 2007) (“Congress’ intent in deregulating the aviation industry was to ‘encourage the forces of competition,’ not to obviate all tort claims under state law that might in some peripheral way impact the airlines.”) (emphasis added).
10. Id.
12. Id. at 228.
13. Id. (alteration in original).
15. 44 F.3d 334, 336 (5th Cir. 1995) (en banc) (emphasis added).
17. Id.
18. 513 U.S. at 228 (emphasis added).
19. See, e.g., Smith v. Comair, Inc., 134 F.3d 254, 257 (4th Cir. 1998) (concluding that the Wolens exception applies only to “actions confined to the terms of the parties’ bargain”); Delta Air Lines, Inc. v. Black, 116 S.W.3d 745, 755 & n.6 (Tex. 2003) (holding that the plaintiff’s breach of contract claim related to airline “services” and was preempted under the ADA).
20. 590 F.3d 1027 (9th Cir. 2010) (reviewing the plaintiff’s claim that the airline breached the contract by improperly collecting a Mexican tourism tax after having failed to disclosed that the tax was not due from exempt passengers).
21. Id. at 1030–31.
22. Treiber & Straub, Inc. v. UPS, Inc., 474 F.3d 379, 386–87 (7th Cir. 2007).
24. Id.
26. Id. at 315–16.
28. Id. at *5.
29. Id.
31. CAL. BUS. & PROF. CODE §§ 17200 et seq.
32. Harris, 202 Cal. Rptr. 3d at 408.
33. Id. (quoting Am. Airlines, Inc. v. Wolens, 513 U.S. 219, 228 (1995)).
34. Id.
35. Id. at 410 (alterations in original).
36. Id.
Space Regulation under President Trump

continued from page 7

2.  Id.
4.  In 1995, the Secretary of Transportation delegated his authority over commercial launch and reentry under the Commercial Space Launch Act to the FAA. As part of the Department of Transportation (DOT), the FAA answers to the DOT for its oversight of the industry. Accordingly, any directions in the president’s policy directive to the Secretary also constitute directions to the FAA.
5.  Space Policy Directive-3: National Space Traffic Management Policy, 83 Fed. Reg. 28,969 (June 21, 2018) [hereinafter SPD-3] (“[To foster] continued growth and innovation in the U.S. commercial space sector, . . . the U.S. Government should streamline processes and reduce regulatory burdens that could inhibit commercial sector growth and innovation, enabling the U.S. commercial sector to continue to lead the world in [space traffic management]-related technologies, goods, data, and services on the international market.”).
7.  SPD-2, supra note 3, § 1.
12.  15 C.F.R. § 960.3.

44.  552 U.S. 364 (2008). In
45.  813 F.3d 718 (9th Cir. 2016) (rejecting United’s ADA express preemption argument, but dismissing the case on the basis of implied preemption under the Air Carrier Access Act).
46.  Nat’l Fed’n of the Blind, 813 F.3d at 727–28. The court also stated that the definition of “service” in Charas was not inconsistent with the Supreme Court’s 2014 ruling in North- west, Inc. v. Ginsberg.
47.  Airlines also may be better served in state court in the states that are part of the Third Circuit, such as New Jersey and Pennsylvania. See Taj Mahal Travel, Inc. v. Delta Airlines Inc., 164 F.3d 186, 194 (3d Cir. 1998) (adopting the Charas definition of “service”).
Aviation Must Respond to Cybersecurity Threats

continued from page 1

steps to mitigate the risk. This way of thinking is flawed and dangerous. A single cyberattack can cause catastrophic loss. Industries that have experienced transformational changes from the digital revolution, such as the financial sector, have been proactive in developing robust, forward-thinking cybersecurity countermeasures and mitigations. It is time for the aviation industry to do the same.

Cybersecurity is fundamental to enterprise risk management and safety. The introduction of e-enabled aircraft and NextGen technology to manage the national airspace system (NAS) is creating a complex, rapidly evolving cybersecurity environment. In recent years, reports have multiplied of cybersecurity breaches in aviation-related networks and systems, including breaches of in-flight broadband, claims that aircraft systems were hacked, and malicious intrusions into back-office airline systems containing sensitive passenger data. These risks implicate a wide range of domains with different risk profiles. This article discusses the state of cybersecurity risk in commercial aviation and how the Federal Aviation Administration (FAA) is responding.

The Nature of Cybersecurity Risk

The cybersecurity risks associated with aviation are real and complex. Cyberattacks on the aviation sector are commonly estimated to be taking place at a rate of over 1,000 per month. In 2015, a consultant made headlines by claiming he hacked into computer systems while traveling on aircraft. He claimed that he physically connected to in-flight entertainment (IFE) systems approximately 15 to 20 times, accessed other airplane networks, and was able to overwrite the code of a thrust management computer during flight and issue a climb command. The manufacturer of the aircraft involved denied that the aircraft’s control systems were breached, or that such breaches were even possible due to multiple redundant intrusion protection measures built into onboard flight-critical systems.

Also in 2015, hackers attacked flight planning computers at Warsaw Chopin Airport, causing 10 flight cancellations and 15 other flight delays. In the United States, a Department of Homeland Security (DHS) official asserted that in 2016 he wirelessly accomplished a remote penetration of the systems of a Boeing 757 that was parked on the ground. Details of this event are not publicly available, but its feasibility has drawn pointed questions from many quarters. In 2017, Russian hackers reportedly penetrated the U.S. aviation sector in conjunction with wide-ranging attacks on the nation’s infrastructure, although information about what they may have accomplished is not publicly known.

What Is Cybersecurity?

The term “cybersecurity” is not synonymous with information security and privacy. Cybersecurity is not limited to protection of data, but includes the security of systems and networks. The Transportation Research Board of the National Academy of Sciences defines “cybersecurity” as “[m]eans and methods that protect data and systems from unauthorized access, inappropriate modification, or unintentional loss.” In thinking about cybersecurity, legal practitioners often focus on data protection, in part because many pertinent laws and regulations trace their roots to privacy law. Although data protection is important, cybersecurity in aviation encompasses threats to critical safety and operational technologies. In this regard, the following definition of “cyberattack” is instructive: “A deliberate attempt to violate the security of a digital system. A successful attack is one that achieves its goal, typically causing harm to information, systems, or infrastructure or disrupting operations that rely on these resources.” The FAA’s preferred term for cybersecurity as it relates to aircraft systems and networks is “aircraft systems information security protection” (ASISP). In recent years, increasing reports of ASISP breaches in aviation-related networks and systems have exposed risks that implicate a wide range of domains with different hazard profiles.

Critical Aviation Technologies

Interconnectivity between and among networks brings a variety of attendant risks. Critical systems in aviation subject to threat include aircraft flight, navigation, and engine control computers; aircraft networks; personal electronic devices linked to such systems; datalink communications; air traffic control (ATC) networks, satellites, and ground stations; and a variety of other technologies surveyed briefly below.

Aircraft systems. Experts believe that the greatest cybersecurity threat to aircraft is from hackers breaching aircraft systems from public networks. The development of aircraft with networked systems has given rise to a new term, the “e-enabled” aircraft. These aircraft have a high

Paul Alp (pulp@jenner.com) is a special counsel based in the Washington, D.C., office of Jenner & Block LLP and a member of the firm’s Aviation and Aerospace practice group. He is a certified flight instructor.
degree of connectivity among systems, boasting wired and wireless networks, fileservers, and multiple data links to networks outside the aircraft. In addition to providing robust IFE and Internet services for passengers, e-enabled aircraft support operational improvements such as remote updating of software and charts, continuous monitoring of health information from aircraft systems, and support for dispatching and redispachaing. Flight crews use electronic flight bags wirelessly connected to aircraft networks in flight, and to ground networks at the gate, to manage charts and checklists, receive weather and safety advisories, and manage other functions.

The three primary domains of an e-enabled aircraft are (see fig. 1):

- Aircraft control;
- Airline information services, including systems like ACARS (aircraft communications addressing and reporting system) and real-time maintenance monitoring; and
- Passenger information entertainment services, including videos, e-mail, and Internet for passengers.

Fundamental to the security of this networked infrastructure is the principle that any potential intrusion into passenger systems must be isolated and contained. No single-point failures should be available for exploit, and faults must not propagate across domains. For these reasons, e-enabled aircraft employ various firewalls and other cybersecurity controls. Sometimes, however, linkages across domains may be found, such as where IFE networks are on the same network as aircraft control systems, separated only by a firewall.

The challenges to secure such systems are both obvious and subtle. Passengers need not be malicious actors to pose a threat. For instance, malware embedded in a website visited by a passenger could compromise aircraft systems. Moreover, the rapid deployment of new technologies has given rise to diverse threats such as the transmission of threatening or hostile messages from outside the aircraft to passengers’ personal devices or even to devices in luggage connected to explosives; erroneous maintenance messages; the capture of passenger credit card data from in-flight purchases; and the reprogramming of flight or engine-control software with altered code. In addition, given the use of electronic flight bags and mobile devices by flight and cabin crew members, securing and separating flight-critical data from personal data remains an ongoing concern because trusted insiders with approved devices could compromise aircraft systems, by design or accident, when their devices communicate with the aircraft.

**Datalink communications.** Datalink systems are replacing voice transmissions with electronic ones, for purposes ranging from transmitting weather information to allowing text communications with ATC instead of time-consuming voice communications that are prone to misunderstandings. Because information transmitted through data links includes flight plans, ATC clearances, weather, advisories, and performance data, the risks posed by potential malicious interference are substantial. As the U.S. Department of Transportation (DOT) observed, “it is critical that FAA incorporate sufficient controls to prevent potential security threats from compromising flight data and communications.” A malicious actor could, for example, upload a false flight plan or clearance to an aircraft, or send false weather information to a flight crew to prompt a course change.

**ATC.** As of 2015, about one-third of ATC systems in the United States used technologies that relied on Internet protocol (IP) to communicate. Interconnectivity will increase substantially as the FAA rolls out NextGen, its ATC modernization effort. NextGen involves a transition...
to IP-based communications and reliance on interconnected systems to increase the capacity and efficiency of the ATC system. The FAA is phasing out the use of radar in favor of automatic dependent surveillance-broadcast service (ADS-B), which will use GPS to precisely locate aircraft and stream that information to other aircraft and ground stations. Another initiative, En Route Automation Modernization (ERAM), will improve air traffic flow through the use of satellite-based air traffic management. The technologies that comprise NextGen raise security concerns due to the inherent interconnectivity needed to make NextGen work: if one system connected to a network is compromised, impacts can spread to other systems. The use of satellite-based navigation and aircraft tracking, although revolutionary in operational terms, raises substantial risks relating to the integrity of communications to and from satellites.

On the ground, ATC networks and computers, as well as airline reservation and ticketing systems, are exposed to a variety of vulnerabilities. In 2015, a computer glitch at an ATC center in Virginia caused a so-called "flypocalypse" in which more than 1,000 flights were delayed or canceled along the East Coast. This event apparently was caused by a software issue in a NextGen route automation system. Although not a cyberattack, the impact of a one-time computer glitch demonstrates the vulnerability of the ATC system to new technologies.

Other systems. Security of aircraft software maintained on laptop computers is also a concern. Typically, updates to critical software are handled through physical connection of a laptop to the aircraft. Security is enhanced through a wireless system in which the integrity of the code is validated against data on an external server before upload to the aircraft system. If the laptop or the internal hard drive containing the software is stolen, malicious actors could modify the software.

Finally, unmanned aircraft systems present unique potential vulnerabilities to cyber threats arising from the use of command and control links between ground stations and the remote vehicle, as well as among ground stations and ATC.

**FAA Response Activities**

The global aviation industry, lawmakers, and regulators are engaged in a difficult and wide-ranging assessment of cybersecurity risks and mitigations. The FAA has drawn criticism over the pace of its work on securing its own infrastructure and the NAS. In 2014, the FAA formed a cybersecurity steering committee to integrate strategy and planning across the agency. The FAA’s wide variety of challenges include mitigating enterprise IT risks, securing data communications, managing security in the technologies associated with the NextGen transition, coordinating with other U.S. agencies and international bodies, and assessing risks and mitigations associated with manned and unmanned aircraft operations.

The FAA’s Approach to E-Enabled Aircraft Cybersecurity

With respect to securing e-enabled aircraft in commercial operations, the FAA has not yet issued regulations specifically directed to cybersecurity risks and requirements, although it has begun the process of doing so. In 2015, it formed a working group of the Aviation Rulemaking Advisory Committee (ARAC) to advise on ASISP-related rulemaking, policy, and guidance. The working group issued a report to the FAA in August 2016 with 30 recommendations. Also in 2016, the FAA commissioned research by outside experts on ASISP vulnerabilities, threats, and safety risks to support the development of policies and regulations to secure aircraft from cyberattacks.

Currently, the FAA’s approach to cybersecurity on e-enabled aircraft centers on two tools: (1) special conditions issued as part of the airworthiness certification process, and (2) approved aircraft network security programs (ANSPs) implemented by commercial operators. As the FAA has explained, existing regulations do not anticipate the types of system architecture or electronic access to critical aircraft systems found in e-enabled aircraft. Of particular concern are connections between aircraft and “nontrusted services,” such as the Internet and other public networks. Through policy and guidance documents the FAA has established a framework for addressing these concerns where regulations are silent.

**Special conditions.** Special conditions are standards that the FAA deems necessary to ensure safety beyond those contained in airworthiness regulations. They are treated as additional certification requirements that apply to particular type designs. The FAA issues special conditions when it finds “that the airworthiness regulations for an aircraft . . . do not contain adequate or appropriate safety standards, because of a novel or unusual design feature.”

Where aircraft connect to nontrusted services, the FAA attaches special conditions to type certificates or supplemental type certificates. As used with respect to e-enabled aircraft, special conditions may impose requirements on the type certificate holder to:

- Establish system security protection from unauthorized external access;
- Identify and assess security risks and implement appropriate protection strategies; and
- Establish procedures to allow an operator to ensure continued airworthiness and maintenance of electronic system safeguards.
As is the case with other airworthiness standards, the type certificate holder bears the burden to show “how to accomplish tests and write documentation that proves that the special conditions can be met.”27 The FAA’s involvement largely focuses on validation of the certificate holder’s testing to ensure compliance.28

**Aircraft network security programs.** In order to comply with special conditions, design approval holders typically issue guidance on network security to operators of specific aircraft. The FAA requires part 121 operators of such aircraft to develop processes that establish how to follow this guidance and maintain security. These processes are formally documented and approved by the FAA as an air carrier’s ANSP. Each operator is required to develop and maintain an ANSP that is tailored to specific threats and technology pertinent to its operations. The FAA requires that each such program:

1. Ensure that data security protection is sufficient to prevent access by unauthorized devices or personnel external to the aircraft;
2. Ensure that security threats specific to the certificate holder’s operations are identified and assessed, and that risk mitigation strategies are implemented to ensure the continued airworthiness of the aircraft;
3. Prevent inadvertent or malicious changes to the aircraft network, including those possibly caused by maintenance activity; and
4. Prevent unauthorized access from sources aboard the aircraft.29

An airline’s ANSP is described in a lengthy manual protected as sensitive security information that addresses the security of aircraft networks and systems, as well as back office administrative infrastructure and personnel issues, including matters such as:

- Control of access to networks;
- Software controls;
- Roles and training of personnel;
- Use and management of specific equipment;
- Control of maintenance laptop access and use; and
- Methods for identifying security intrusions and responding to them.30

The operator must establish means for oversight of the program, with a data security manager responsible for administering the ANSP,31 and must continuously monitor its program to verify compliance and identify, analyze, and develop responses to pertinent threats.32

**Critical Studies of the FAA’s Approaches to Cybersecurity**

In 2015, the Government Accountability Office (GAO) released a study of the FAA’s cybersecurity efforts in connection with the transition to NextGen.33 It found that the FAA faces cybersecurity challenges in (1) protecting ATC information systems, (2) protecting avionics, and (3) clarifying cybersecurity roles and responsibilities within the agency. The GAO concluded that although the FAA was taking steps to address these challenges, the FAA could do more.34 Another GAO report addressing the FAA’s information security programs discussed cybersecurity challenges faced by the agency in securing the interconnected systems that manage the NAS.35 Among other things, the report found that although “[t]he excessive interconnectivity between NAS and non-NAS environments increased the risk that FAA’s mission-critical air traffic control systems could be compromised[,] the FAA did not consistently control access to NAS systems.36

The DOT Office of Inspector General (DOT OIG) audited the security controls of the FAA’s DataComm pilot-controller datalink system and issued a report in July 2018. The DOT OIG concluded that the FAA was “identifying—but [] not mitigating—security risks in a timely manner.”37 The FAA attributed delays in addressing vulnerabilities to a lack of available funds.38

**Other U.S. Government Activities**

While some believe that the FAA is not acting with sufficient speed to identify and respond to cyber threats, other parts of the executive branch have increased their activities in this area while Congress considers new cybersecurity legislation.

Aviation cybersecurity is playing a larger part of the DHS’s broader cybersecurity portfolio. In 2013, Executive Order 13,636 directed various administrative agencies to collaborate and coordinate with respect to the gathering and sharing of information and the development of a framework to reduce cyber risk to critical infrastructure.39 Among other things, this order provided guidance for the DHS to work with the FAA on sharing information about threats and countermeasures.40

The Transportation Security Administration (TSA) is collaborating with industry on information sharing with support from the U.S. intelligence apparatus.41 For example, in partnership with the FBI and industry representatives, the TSA has established entities such as the Air Domain Intelligence Integration and Analysis Center (ADIAC) and Aviation Information Sharing and Analysis Center (A-ISAC) to share information and analyze threats to civil aviation.42 These initiatives focus on emerging vulnerabilities and forward-looking efforts to proactively identify future threats and countermeasures. In addition, Congress has directed the TSA to periodically review threats to civil aviation by cyberattack.43

Congress has shown sporadic but increasing interest in aviation cybersecurity legislation. Section 2111 of the FAA Extension, Safety, and Security Act of 2016 directed the

---

Published in The Air & Space Lawyer, Volume 31, Number 4, 2018. © 2018 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.
agency to develop a “comprehensive and strategic” aviation cybersecurity framework that would address risks associated with the modernization of the NAS, aircraft, and equipment. A bill entitled the “Cyber Air Act” has twice been introduced in Congress, but did not pass. The recently passed FAA Reauthorization Act of 2018 contains a handful of provisions relating to aviation cybersecurity. It directs the FAA to consider revising airworthiness regulations to address cybersecurity in avionics systems and review its comprehensive framework of principles and policies developed under the 2016 legislation.

Finally, of interest to aviation companies that do business with the U.S. government is the requirement that they safeguard controlled unclassified information (CUI), which encompasses information a private entity possesses for or on behalf of the government. Certain government agencies, notably the Department of Defense and NASA, require any entity that works with CUI to implement specific data security measures in accordance with standards published by the National Institute of Standards and Technology. Meeting these standards may present substantial challenges arising from the need to restructure existing IT systems. The FAA is currently enmeshed in the complex process of establishing its own internal controls for CUI, but has not imposed general requirements on certificated entities to safeguard CUI.

Conclusion
Commercial aviation presents a multifaceted technological environment with a seemingly unlimited universe of emerging cyber threats. Many of the initiatives in place or under development that address cybersecurity are products of voluntary industry initiatives and industry-developed standards and best practices. While the government considers various new initiatives, reports of attempted cyberattacks continue to proliferate. Concerned stakeholders should not wait for the government to issue mandates before taking action to identify, assess, and mitigate cyber risk. Cybersecurity is not just about information privacy—it is a safety issue. The industry is uniquely positioned to apply proactive, systematic approaches to cyber risk like those it has established for safety risk. Engaging fully in this effort with sufficient resources will help to avert a painful, expensive, or tragic teaching moment.

Endnotes
7. TRANSP. RESEARCH BD., AIRPORT COOP. RESEARCH PROGRAM (ACRP) REPORT 140, GUIDEBOOK ON BEST PRACTICES FOR AIRPORT CYBERSECURITY 73 (2015).
8. Id.
9. E-enablement has been defined as “[t]he integration of aircraft IT networks with ground systems . . . and IT-infrastructure to enable new airline business processes and/or safety controls.” What Exactly Is Aircraft eEnablement?, GET CONNECTED (June 1, 2017), https://www.getconnected.aero/2017/06/feature-exactly-aircraft-eenablement/.
14. The FAA’s datalink program for ATC aircraft messages, known as “DataComm,” is part of the NextGen initiative. It encompasses the use of text messaging for pilot-controller transmissions of flight plans, clearances, instructions, advisories, and other messages. It is gradually being rolled out at major U.S. airport control towers. The second phase will add en route services that support rerouting of aircraft in flight. See U.S. DEP’T OF TRANSP., REPORT NO. F12018059, OPPORTUNITIES EXIST TO FURTHER STRENGTHEN THE SECURITY CONTROLS OF FAA’S DATA COMMUNICATIONS PROGRAM (2018) [hereinafter DOT DATACOMM REPORT], Fact Sheet, FAA, Data Communications (Data Comm) (Oct. 17, 2018), https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=21994.
15. DOT DATACOMM REPORT, supra note 14, at 1.


18. Id. at 7.

19. Beyond the scope of this article is a discussion of voluntary efforts to establish cybersecurity standards and best practices, such as the cybersecurity framework created by the National Institute of Standards and Technology in 2014 and the ISO 27001 standard created by the International Organization for Standardization in 2007. The International Civil Aviation Organization (ICAO) has also been active, establishing a cybersecurity task force in 2012 and adding a recommended practice to annex 17 in 2013 that encourages states to adopt cybersecurity measures.


24. Id. Special conditions are intended to “contain such safety standards for the aircraft . . . as the FAA finds necessary to establish a level of safety equivalent to that established in the regulations.” Id. § 21.16.


28. See id. The FAA does not issue special conditions to address all potential cyber threats on aircraft. For instance, various other policies and guidance, in particular guidelines issued by entities such as Aeronautical Radio, Inc. (ARINC), apply to the airworthiness and operational approval of field-loadable software, aeronautical databases, and ACARS. See FAA Policy No. PS-AIR-21.16-02 Rev. 2, supra note 25, at 2.

29. FAA, ADVISORY CIRCULAR AC 119-1, AIRWORTHINESS AND OPERATIONAL AUTHORIZATION OF AIRCRAFT NETWORK SECURITY PROGRAM (ANSP) 3 (Sept. 30, 2015).

30. Id. at 4.

31. Id. at 3.

32. Id. at 5.


34. Id. at 11.

35. GAO-15-221, supra note 17, at 5.

36. Id. at 13–14.


38. Id. at 5. In a 2017 report on the FAA’s management of the transition to NextGen, the DOT OIG concluded that the FAA “lacks a comprehensive process for effectively identifying or assessing risks” to the transition, and that it was “not proactively mitigating risks to keep the [transition] on track.” U.S. Dept. of Transp., Report No. AV2018001, FAA Has Made Progress Implementing NextGen Priorities, But Additional Actions Are Needed to Improve Risk Management 4–5 (2017).


40. On May 11, 2017, President Trump issued Executive Order 13,800, which built upon Executive Order 13,636 by directing agencies to improve their support of entities in the private sector in their efforts to address critical infrastructure cybersecurity.

41. Unfortunately, the TSA has also been widely criticized for how it manages its own enterprise and operational cybersecurity. See Violet Blue, The TSA Is Failing Spectacularly at Cybersecurity, Engadget (May 20, 2016), https://www.engadget.com/2016/05/20/the-tsa-is-failing-spectacularly-at-cybersecurity/.


44. The Act also directed the FAA to reduce cyber risk to ATC, improve implementation of information security standards, and provide more support for voluntary efforts by the industry and standards setting organizations. Pub. L. No. 114-190, § 2111, 130 Stat. 615, 625 (July 15, 2016).


47. H.R. 302, § 506.

48. Id. § 509.

49. Exec. Order No. 13,556, 75 Fed. Reg. 68,675 (Nov. 9, 2010), directed agencies to handle unclassified information that requires controls in a systematic, unified way. See also 32 C.F.R. pt. 2002 (implementing regulation for handling CUI overseen by the National Archives and Records Administration).

The Local Future of the Low-Altitude Airspace

continued from page 1

the brush, after rebaiting a feral hog trap in an ongoing war on the oversize agricultural pests.

These scenes are not part of a futuristic advertisement for the drone industry. Rather, they are actual missions that have occurred dozens and even hundreds of times in recent months, in airspace managed, in part, by the states and localities where they took place.

These operations are part of the U.S. Department of Transportation’s (DOT’s) Unmanned Aircraft System (UAS) Integration Pilot Program (IPP). Designed by the White House to accelerate the growth of commercial drone operations, the IPP is tackling the thorny legal and regulatory questions that have constrained the growth of this burgeoning industry. The IPP in particular enables states and localities to take the lead in pushing for complex operations not currently allowed, and managing those operations, through a time, manner, and place framework that recognizes the nuances of local airspace. The IPP points toward a future in which drones will be able to operate at scale, where there is collaboration across the levels of government, and where management of the low-altitude airspace is local in a way thought to be simply not feasible just a few years ago.

This article discusses three significant recent developments regarding low-altitude airspace management, including the IPP. These developments demonstrate the need for a new paradigm to usher in a future of low-altitude airspace management. This paradigm recognizes the complementary roles of both local and federal governments and the unique capacity for unmanned traffic management (UTM) technology to mediate the roles each participant plays.

FAA Reauthorization and Preemption

Nearly four years ago, the Federal Aviation Administration (FAA) posted an article on its website attempting to debunk what it described as “myths” about the FAA and UAS. Exhibit 1 was the “myth” that “[t]he FAA doesn’t control airspace below 400 feet.” In fact, the agency claimed, “[t]he FAA is responsible for the safety of U.S. airspace from the ground up.” Agency officials repeated in various public fora that the FAA managed the airspace from the top of the blades of grass to the heavens. The assumption of federal airspace sovereignty was so strong, aviation lawyers would assert that “in the context of aviation, federal preemption long has been understood to sweep with a wide broom.”

Four years later, those sweeping assumptions seem far less certain. An analysis by the National Conference of State Legislatures (NCSL) in 2017 found that at least 38 states had considered laws or regulations to govern local UAS operations, with dozens having actually passed them. The FAA’s roadmap for the national airspace system (NAS) states that it will not provide air traffic control (ATC) services below 400 feet, where the overwhelming majority of today’s drone operations occur. FAA Acting Administrator Dan Elwell recently described the future of drone regulation as one that “will require local level coordination” with rules of “broad applicability that can be tailored by the local community.” Even if a national framework is necessary, delegation of authority is central to a successful drone integration plan: state and local governments will play a significant role in the future.

This sea change in the distribution of authority and responsibility is captured by omission in the FAA Reauthorization Act. In October 2018, Congress passed the first long-term FAA reauthorization legislation in six years. This compromise bill includes long-overdue provisions remedying issues that have held back the drone industry. But perhaps the most intriguing aspect of this legislation is what it does not contain, namely express federal preemption of all state and local regulation of UAS operations.

By contrast, an amendment that would have expressly preempted state and local authority was the topic of heated discussion during the congressional debate over the 2016 FAA reauthorization bill, which ultimately did not pass. Throughout 2017, however, a coalition recognizing the state and local role in accelerating drone operations began to emerge at the federal level, with the bipartisan Drone Federalism and Drone Innovation Acts introduced in the Senate and House of Representatives, respectively.

Also in 2017, operational UTM systems emerged. UTM systems are how airspace will be managed to ensure the safety of the NAS when multiple drone operations occur simultaneously. UTM coordinates, manages, and deconflicts UAS operations in low-altitude airspace, in real time. UTM is also necessary to enable advanced drone operations, such as those beyond the operator’s visual line of sight (BVLOS). UTM systems anticipate an airspace that is vastly more complex than the skies above 400 feet, and one that requires a fundamentally different relationship

William Goodwin (bill@airmap.com) is the general counsel of AirMap, an airspace management startup based in Santa Monica, California. Tyler Finn (tyler@airmap.com) is a law and public policy manager at AirMap.
with stakeholders on the ground. The FAA itself laid the cornerstone of its UTM system (and ecosystem) with the launch of the Low Altitude Authorization and Notification Capability (LAANC), which supports ATC authorization requirements for UAS operations conducted under the FAA’s small UAS rule (14 C.F.R. part 107).

By the time Congress considered the 2018 FAA reauthorization bill, the landscape had shifted even further from the previous two years. LAANC had achieved nationwide deployment, allowing automated access to airspace at more than 500 airports (and showing the capacity of technology to reduce complexity for the operator and enable safer operations in controlled airspace. The first flights under the IPP demonstrated the potential of an accelerated timeline for complex operations, facilitated by UTM. The 2018 FAA Reauthorization Act codified the IPP, enacting into law the ability of states and localities in the program to establish time, manner, and place restrictions on drone operations. Finally, the Act directed the FAA to align multiple programs supporting the development and deployment of UTM technology, an effort that will facilitate precisely this type of collaboration between levels of government.

**Evolution of the FAA’s Perspective**

Recent developments, particularly the creation and codification of the IPP, are significant shifts in the debate over state and local authority and a recognition of the new collaboration that will be required across all levels of government to manage low-altitude airspace.

Announced in October 2017, the IPP was created to expand cutting-edge drone operations into the NAS by partnering state, local, and tribal governments with industry members. The program is intended to help the DOT and FAA design rules to allow more complex low-altitude operations by: (1) identifying ways to balance local and national interests related to UAS integration; (2) improving communications with local, state, and tribal jurisdictions; (3) addressing security and privacy risks; and (4) accelerating the approval of operations that currently require special authorizations.

In announcing the first 10 program awardees, Secretary of Transportation Elaine Chao said, “Instead of a dictate from Washington, this program takes another approach. It allows interested communities to test drones in ways they are comfortable with.”

Chao’s comments represented a historic shift in the willingness of federal authorities to work with states and localities to integrate new operations in the NAS. Since the Airline Deregulation Act of 1978, the FAA has exercised its authority almost unilaterally. In 1990, the federal consolidation of authority extended to include perhaps the most local of issues: noise. Prior to 1987, a former chief counsel of the FAA could credibly comment: “it might really surprise the millions of Americans who, on a daily basis, enjoy the benefits of our strong national air transportation system to know just how little control over that system resides with the national government and how much control actually resides at the local level.” With the passage of the Airport Noise and Capacity Act (ANCA) of 1990, however, it was clear that Congress had accepted the FAA’s belief that “a national aviation noise policy was not only necessary but vital to the fitness of the country’s air transportation system.”

The emergence of ubiquitous drone use in airspace adjacent to homes, businesses, and people, and the classification of drones as aircraft, has forced the FAA to revisit its capacity to address the issue of noise on its own. Earl Lawrence, head of the FAA’s UAS Integration Office, has publicly affirmed the need to involve local communities in this conversation. In September 2018, Lawrence said, “You have to deal with the societal issues. How are you going to take off and land in cities? How are you going to deal with the noise issues? So, right now, we’re testing this and getting input.”

In fact, the IPP is an attempt not just to solve challenges, such as noise concerns and safe operation over people, but also to enable new economic opportunity, through collaboration with states and localities. Industry and regulators alike believe the IPP represents the first clear regulatory path to high-volume commercial operations for complex operations, such as BVLOS operations, in the world.

The IPP has also made UTM technology central to this collaboration and to complex operations. UTM providers were included in all but one of the 10 IPP awards. Since the program’s launch, UTM technology has been a component of the safety mitigation cases submitted to the FAA and the means by which state, local, and tribal governments manage the operations occurring in their jurisdictions.

In parallel, the FAA has expanded its LAANC program from beta testing (at three airports) to a nationwide program, available at more than 500 airports. Originally launched in September 2017, LAANC allows part 107 commercial operators to digitally file airspace authorization requests through third-party providers. LAANC replaced a paperwork system in which it could take as long as 90 days for operators to receive airspace approval in controlled airspace, vastly increasing the amount of airspace accessible to commercial drone operations in the United States.

Conceptually, LAANC represents a set of conditions that, once met, open the airspace to an operation.
This approach raises the question, what additional conditions, such as a qualitative risk analysis, could demonstrate compliance and safe operations, such that automatic approval could be granted? The program also points toward the future importance of automation in ensuring compliant, but timely, access to airspace. Community preferences, such as noise restrictions or limits on operations after midnight, could be just another automatic check for flight approval, instantly visible to operators and as easy to address or route around as Waze directs a driver around a road closure, or as Uber directs travelers to a specific street corner for pick up.

The FAA’s vision for the future of UTM appears to recognize the potential, even the necessity, of incorporating all levels of government in this framework. The FAA’s UTM Concept of Operations version 1.0, released in May 2018, documents what the FAA has learned to date through the use of case development, insights on rulemaking, and the evolution of UTM technology.”14 The document recognizes the role state, local, and tribal governments have felt compelled to perform: “Many states have passed laws that regulate or prohibit the flight, weaponization, and surveillance use of UAS in select airspace to preserve the rights of its citizens.”15

In the FAA’s framework, private companies act as UAS service suppliers (USS), to work “with states, municipalities, and other entities as required ensuring local airspace access restrictions, or preemptions, are incorporated into, and maintained in, the USS Network and Operation Volumes are de-conflicted from these areas during the intent sharing processes.”16 Dynamic restrictions by local authorities are a necessary vehicle for preserving the safety of operations in low-altitude airspace. The easiest way to communicate these dynamic restrictions to drone operators is through a UTM system. How LAANC and the FAA more generally embrace the possibilities of automated access to airspace will also be informed by another program: the UTM Pilot Program (UPP). Established in April 2017, the UPP’s primary goal is to develop, demonstrate, and provide enterprise services that will support implementation of initial UTM operations. Although a full rollout of the UPP has been delayed until 2019, it will be a useful mechanism to identify how UTM technology will enable BVLOS operations in the future. It will include testing technology required to implement dynamic restrictions of operations around events of local significance (such as for first responder activity, parades, and large public gatherings) in both controlled and uncontrolled airspace, and the means by which states and localities influence the low-altitude airspace above them.

What Does the Future Hold?
The future of low-altitude airspace management is hard to predict, given the difference in scale of operations that drones will bring, but it will be necessarily local in nature. The FAA’s approach to drones as well as how aircraft operate in the low-altitude airspace today provide clues in this regard. Crop dusters, for instance, are uniquely exposed to dangers close to the ground and share the same airspace that will increasingly be populated by drones. Today, crop dusters operate pursuant to local rules, which reflects that when aircraft operate at low altitudes, local concerns are important for safe operations.17

Similarly, FAA Acting Administrator Dan Elwell recently drew comparisons between the FAA’s shift toward working with communities to its historical approach to emergency operations:

Ultimately, what we want is some sort of standard or overarching rule(s) with broad applicability that can be tailored by the local community. To illustrate this further, let’s look at other aviation contexts. Medivac helicopters operate under certain rules and regulations set forth by the FAA. However, the local jurisdictional authority provides additional guidance on where they can take off or land for routine operations. We envision the same dynamic for drone operations.18

While medivac helicopters and crop dusters may be the closest analogy, the future of low-altitude airspace is unlike anything the world of aviation has witnessed to date. Just as scooters and bicycles crisscross our cities on short trips, the low-altitude airspace will see inspection drones circling buildings at or near sidewalk height. UPS or FedEx vans will have their airborne counterparts, with package delivery drones buzzing to and from commercial hubs and delivery trucks. Electric vertical takeoff and landing (eVTOL) aircraft will pass through to deliver people and cargo, not unlike the Ubers or buses temporarily occupying curb space. The skies below 400 feet will look far more like the ground just beneath them than the relatively uncrowded skies above.

Like the ground below, the management of that traffic flow will require complementary roles for different authorities. A city’s ability to erect a stop sign in the sky will be no more of an inconvenience than it is for a driver whose navigation app will automatically route a drone around a fire, hostage standoff, or other emergency. The orchestration of traffic will be as simple for commercial operators as it is for you to be directed around the corner by Uber or Lyft, when you’re hailing a ride in a no-stopping zone. This will
be one of the most exciting opportunities for the cities of the future. Armed with the technologies available to private companies today, the cities of tomorrow will be able to welcome a host of new vehicles in the sky.

Commercial aviation has long believed that national coordination of the airspace was a prerequisite for safety and the consistent growth of the industry. Drones have forced the FAA to rethink those assumptions, both the collaboration required to ensure safety and the degree to which local concerns must be addressed to enable the drone economy. The FAA, to its credit, is rising to the challenge. The responsibility now lies with the next generation of aviation and urban leaders to embrace the opportunity.

Endnotes

2. Id.
15. Id. at 19.
16. Id.
Drones Across America
Unmanned Aircraft Systems (UAS)
Regulation and State Laws
By Dr. Sarah Nilsson

The popularity of drones (unmanned aircraft systems, or UAS) and drone technology in the United States has excited entrepreneurs and corporations, while sending lawmakers scrambling to keep pace with the industry’s growth. This comprehensive book lays out a framework for demystifying the sometimes unwieldy and ever-changing area of federal and state drone laws. This book allows readers to develop a detailed understanding of the organization of federal and state regulations of drone law. It also provides a detailed exploration of policies and best practices for the operation of commercial, government, and recreational drones in different airspaces. Also included is a comprehensive matrix of state laws related to UAS. This book is a necessary and important resource for anyone working with unmanned aircraft systems.

ISBN: 9781634257138
Product Code: 5540026
Paperback 7x11
2017, 349 pages
List Price $119.95
Forum on Air & Space Law Member Price $95.96

Aviation Regulation in the United States
Edited by David Heffernan and Brent Connor

This truly unique publication is your practical and comprehensive guide to aviation regulation in the United States. It is an essential resource for veterans and newcomers alike.

This book introduces the various institutions that govern aviation in the United States and covers the international framework—legal and institutional, multilateral and bilateral—within which U.S. regulation takes place. Written by a distinguished panel of experts, requirements applicable to every aspect of the aviation industry are clearly explained with citations.

Experienced and new practitioners, journalists, or business professionals will find this bountiful reference makes a hugely important body of law far more accessible than ever before.

ISBN: 9781627226059
Product Code: 5540025
Paperback 7x10
2014, 657 pages
List Price $169.95
Forum on Air & Space Law Member Price $144.95

shop.americanbar.org
IN THIS ISSUE...

Aviation Must Respond to Cybersecurity Threats ...................... 1
The Local Future of the Low-Altitude Airspace .......................... 1
Chair’s Message ............................................ 2
Editor’s Column ........................................... 3
Expanding and Streamlining: Space Regulation under President Trump ........................................... 4
Judicial Beacons Light the Way for Interpreting Airline “Service” under the ADA ........................ 8