



421 Aviation Way
Frederick, Maryland 21701

T. 301-695-2000
F. 301-695-2375

www.aopa.org

April 1, 2011

Docket Management Facility
U.S. Department of Transportation
1200 New Jersey Avenue, SE.
West Building Ground Floor
Room W12-140
Washington, DC 20590

RE: Federal Aviation Administration Docket Number FAA-2011-0183

To Whom It May Concern:

The Aircraft Owners and Pilots Association (AOPA) on behalf of the more than 400,000 individual general aviation pilots and aircraft owners nationwide, is extremely concerned with limitations being proposed by the Federal Aviation Administration (FAA) in their notice of proposed modification to the FAA/Subscriber Memorandum of Agreement (MOA) on the Block Aircraft Registration Request (BARR) program.

AOPA has significant concerns with the implications on an individual's privacy, confidentiality, security and personal safety that could result from the proposed changes. Further, it appears the proposed FAA action is a solution in search of a problem that doesn't exist without due regard for the adverse impact it may have on private individual citizens because of the unnecessary release of personal information. AOPA has determined that the proposed changes are dangerous, invasive and unwarranted and the unintended negative implications are far reaching.

We note that, contrary to well established rulemaking principles, the Administrative Procedure Act, Executive Order 12866, and DOT order 2100.5, the Notice makes little to no attempt to articulate a public policy justification in making available to the general public and other non-governmental entities real time or near real-time tracking data on the location and identity of private aircraft. Although the proposed DOT Order appears to refer to a recent court decision, *National Business Aviation Association, Inc. v. FAA*, 686 F. Supp.2d 80 (D.D.C. 2010), as a justification, that ruling specifically does not extend to the release of real-time flight tracking data of private aircraft to the general public. We emphasize that access by the government and law enforcement to this data is legitimate and is not in dispute. However, we see no public policy purpose to be served in the indiscriminate disclosure of real time flight tracking data to the general public and unknown persons. We believe this will have profound personal privacy and security implications.

Further, and as discussed more fully below, we also believe the proposed order is at odds with a 2006 Department of Homeland Security Advisory regarding the intentions of terrorist groups in tracking and destroying private civilian aircraft. In light of this Homeland Security advisory and the actual example it contains, the requirement in the proposed order for operators to essentially prove and certify a “valid security concern” is too uncertain and demanding for establishing what the Department of Transportation will consider as a qualifying security threat.

The National Business Aircraft Association submitted independent comments to the docket and we concur with those comments as well.

Background

BARR was deployed by the FAA in the early 1990s as a valuable airspace management tool. It also facilitates the tracking by individuals of the minute-by-minute progress of their, or other, aircraft in real time. This is possible through Aircraft Situation Display to Industry (ASDI) data that the FAA now makes available to subscribers through several vendors.

Currently operators with privacy and/or security concerns for their operations resulting from the availability of ASDI data can request this data be blocked from public dissemination through the BARR program, which the National Business Aircraft Association (NBAA) administers on behalf of the FAA. Although AOPA currently chooses not to block the aircraft we operate, we fully understand the multitude of justifications that exist for those operators that choose to.

Privacy

The FAA's newly proposed limitation seemingly disregards the legitimate need and justification for the BARR Program, and it runs directly counter to long-established assumptions about government's role in the protection of privacy. The privacy protection that's been in place in the program for 20 years should remain in place for those among AOPA's membership and among the flying community who want to protect against disclosure to anyone who may desire to follow their aircraft. The impact of this change goes well beyond larger public owned companies, to individual private citizens whose information and movements will be shared publicly with anyone, whether they be a loved one following the safe arrival of an aircraft, a business associate watching for an arrival to assure attendance at a meeting, a curious observer, or a nefarious character interested in doing physical harm or in stealing business secrets. There is little to no public benefit in the release of the government's tracking data that an individual would otherwise seek to keep private, and it is questionable whether individuals even know that the government is giving out this information about them. The disclosure of aircraft tracking data does not shed light on a government function. It does not help to foster or improve aviation safety or security. Rather, for AOPA members, the disclosure of this information may only serve to needlessly intrude into individual and business concerns. If you own and operate a private aircraft and you wish to prevent the disclosure of where and when that aircraft is being flown, you should have the opportunity to do that.

There is a sense that citizens who own their own aircraft and fly the plane must justify their right to privacy. Again, this seems an unusual standard when at the same time, an automobile owner and operator is not required to share where and when he operates with the general public. Will we need to justify why we might prefer not to have EZ Pass information released about where our private automobiles travel? At a minimum, the same privacy provision available to automobile owners should apply to private aircraft owners.

Society in general is working very hard to protect personal privacy with many lifeguards and safeguards being put into effect to protect individuals. At the same time, the FAA is telling the public they have no problem with sharing all information on your operation. And yet, the same agency that wants to deny all individual private aircraft owner their right to privacy has chosen to block all of its own aircraft movements and those of other government agencies. This is a classic example of a Government that is out of sync with those that it regulates.

Security and Personal Safety Concerns

The restrictions being proposed for the BARR program are in direct contradiction to guidance provided by the Department of Homeland Security. In a security advisory to aircraft owners and operators the Transportation Security Administration issued a warning to high end aircraft operators of a threat posted on a jihadist forum that urged followers to:

“Destroy private American aircraft...We call upon all Muslims to follow and identify private civilian American aircrafts in all airports of the world...It is the duty of Muslims to destroy all types of private American aircrafts that are of the types Gulf Stream and Lear Jet and all small jet aircraft usually used by distinguished (people) and businessmen.”

The message also advised readers how to identify American aircraft and provided the tail number of a private aircraft allegedly used by the CIA. One valuable tool in averting this threat has been through the use of the BARR program. The proposed changes have the significant potential of becoming a matter of personal safety and deteriorating security. But more important, the proposal by DOT is inconsistent with the DHS Advisory and seems to pit one agency against the other. In light of this advisory DOT should be looking to expand the program and change it to “Opt In” versus “Opt Out”. It seems counterproductive that at a time when individuals are taking prudent steps to prevent a known risk, the government appears unconcerned. Unfortunately, this threat alone will most likely not reach the FAA’s threshold to continue having the aircraft information blocked otherwise they would not have proposed modifying the current BARR program.

Perhaps even more troubling than the unprecedented intrusion into the privacy of citizens is the potential impact on National Security and the security of those that utilize general aviation aircraft. Since the tragic events of September 11, there has been a continuous drive to obtain the most up-to-date information on aircraft and pilots operating in the National Airspace System (NAS). Every minute of every day all aircraft operating over the U.S. are monitored by agencies whose primary responsibility is the protection and defense of the Nation. While the proposed changes to the BARR program will not impact their ability to see the movement of these aircraft, it will greatly complicate, if not completely eliminate their ability to accurately piece together the information that is needed for them to accomplish their jobs. If the BARR program is eliminated, in order to protect their privacy many aircraft owners will bury the true identity of the operator under layers of Limited Liability Corporations, shadow leasing firms and other techniques that will be devised to serve the same purpose that the BARR program serves today. This will make it impossible for those working to protect our Nation from ascertaining the true identity and intentions of the aircraft and those operating it. In sidebar conversations with key individuals within the Homeland Security and Defense sectors these fears have been expressed multiple times.

Finally, the modifications proposed to the BARR program unnecessarily place the occupants of the aircraft and the general public at risk. A case in point surrounds the travel of a very popular musical group that was utilizing general aviation aircraft for their multi-city tour. Unbeknownst to the airport manager a group of several hundred fans descended on the airport in advance of the band's arrival. They had been tracking the aircraft via FAA released data and were aware of the arrival airport and the time and utilized social media tools to spread that information to other fans with a like interest. The resulting crowd quickly overwhelmed the limited police on hand and needlessly endangered the personal well being of the band and the multitude of fans that flocked to see their arrival.

AOPA Questions Future FAA Policy on Data Sharing

In the broader context of information and data sharing, AOPA is extremely concerned with policy change discussions of outsourcing all current FAA data feeds and data to one specific vendor. AOPA contends that any and all changes with regard to government data – especially if that data will no longer be available directly from the government - should be vetted publicly and allow for a minimum of a 60 day comment period. Additionally, AOPA believes DOT's policy on the release of personal information, in this case flight plan data, should be changed to an "Opt In" program in which the government needs the permission of the individual prior to it being disclosed publically.

Summary

AOPA strongly recommends that the FAA reconsider the proposed changes in light of the implications on operator privacy, security and personal safety that will result from these modifications. The BARR program as currently operated is effective in balancing the interests of private aircraft owner security and privacy while allowing for information sharing as necessary. AOPA appreciates the opportunity to share these concerns and anticipates the FAA taking action to ensure individual privacy, confidentiality, and security provisions are maintained.

Sincerely,

A handwritten signature in black ink, appearing to read "Melissa Rudinger". The signature is fluid and cursive, with the first name "Melissa" and last name "Rudinger" clearly distinguishable.

Melissa Rudinger
Senior Vice President, Government Affairs