STATEMENT OF
JAMES C. MAY
PRESIDENT AND CEO
AIR TRANSPORT ASSOCIATION OF AMERICA, INC.
BEFORE THE
SENATE COMMERCE, SCIENCE AND TRANSPORTATION COMMITTEE
ABOUT THE SECURE FLIGHT PROGRAM AND REGISTERED TRAVELER PROGRAM
FEBRUARY 9, 2006

No consumer service industry is affected by security requirements like the U.S. airline industry. That central fact significantly shapes the economics of providing air transportation. Yet the airline does not control this situation because civil aviation security in the United States is a Federal responsibility. This is as it should be but does not diminish the airline industry's very legitimate interest in seeing that security-related measures are effectively conceived and properly and economically implemented.

In the last several years, the Transportation Security Administration has clearly improved its screening of passengers and their baggage. Anyone who regularly travels by air has witnessed that improvement. And TSA has emphasized its commitment to using risk analysis to establish security priorities. These developments are encouraging and should be recognized.

Nevertheless, important elements of the government's aviation security programs are not nearly as cohesive or well founded as they could be. There is no justification for this. Aviation security is obviously dynamic but in these matters, to mix a metaphor, we should have gotten our sea legs by now. We need to do so quickly.

Today's hearing is thus exceptionally important and timely. It is an opportunity for us to focus attention not only on the Secure Flight Program and the Registered Traveler Program but, equally important, also on other existing and emerging aviation security programs that will impose substantial new information demands on passengers and airlines. The characteristic that is common to these programs is their dependence on passenger information. That is where the commonality ends. These programs are uncoordinated, which is inexplicable and should attract close attention. Intuitively, most of us would assume that considerations of efficiency would have produced far more commonality among Federal programs that are both security oriented and data dependent. The fact that this has not happened should prompt an examination of their *efficacy*—how well they achieve their stated aviation security objectives; their *efficiency*—how economically they accomplish those objectives and whether less costly alternatives exist; and their *protection of privacy*—how thoroughly they preserve passengers' expectations of privacy, and how adequately and transparently they delimit governmental agencies' use of personal information.

TSA's Secure Flight Program and its Registered Traveler Program illustrate the complexities of data-based security programs and, in the case of Registered Traveler, the need to return to first principles when evaluating them.

Secure Flight is intended to pre-screen airline passengers. As envisioned, an airline would submit to TSA certain passenger information whenever a reservation is made for a domestic flight. It would enable TSA to compare reservation information with the Federal Government's no-fly and selectee lists. TSA expects that this arrangement will enhance security, improve pre-screening efficiency and reduce the number of passengers subjected to secondary screening. Each of these outcomes would be very desirable.

Airlines and ATA have worked with TSA at several points in its development of Secure Flight. We have also worked with CBP and CDC on their passenger information needs. This experience has left two important impressions. First, coordination between government agencies and airlines is essential. Any program that involves government access to reservation information generates substantial data content, format and transmission issues. You cannot simply push a button to get passenger data that would be useful to TSA or any other Federal agency. Second, privacy issues are of the utmost significance in any government program to access passenger data. Privacy issues are an immutable part of the landscape.

The nature of Secure Flight is such that the airline industry's involvement with TSA about it, necessarily, has been limited. Nevertheless, we are hopeful that its benefits can be soon realized.

In contrast to our hopes about the Secure Flight Program, the Registered Traveler Program has turned into a shifting and dispiriting exercise. It compels you to ask, "Where's the beef?"

The airlines were early and ardent advocates of the registered traveler concept. Four years ago we urged the development of a government system that would speed the screening of those passengers who did not present security concerns and thereby facilitate the processing of the vast majority of travelers. Today's Registered Traveler Program promises no such benefits to our customers. Indeed, the Registered Traveler Program as currently constituted has become even less attractive because it has been morphed into an orphan program; TSA has largely lateraled it to the private sector. Finally, the systemwide improvement in passenger screening that TSA has accomplished in the last few years begs the question of why this sorry state of affairs should continue.

We are unaware of any evidence that Registered Traveler will produce the tangible and widely available benefits to passengers that we had envisioned in 2002; or that it will attract significant numbers of registrants; or that it will generate a pronounced improvement in overall security; or that vendor interoperability issues will be overcome; or that systemwide passenger wait times will diminish; or that passenger privacy issues have been confronted and satisfactorily resolved. We, however, do know that what was originally conceived as a straightforward governmental program to benefit the vast majority of passengers has been transformed into a commercial enterprise for what increasingly looks like the few.

Registered Traveler neither offers the benefits to passengers nor the breadth of use that justify its introduction as a permanent program. It should be eliminated.

As I observed at the beginning of my testimony, other existing and contemplated aviation security programs rely or will rely on government access to passenger information. Expanding passenger information requirements create substantial new demands on governmental agencies, airlines, and travelers. The problem is that government passenger information requirements thus far have only produced a mosaic. It remains to be seen if a coherent a picture will emerge.

This is a serious situation. Given the security threats confronting civil aviation, there is no reason to believe that that the government's passenger information needs will abate. Passenger data will be required for the Secure Flight Program and the Registered Traveler Program. In addition, passenger information is currently required for CBP's Advance Passenger Information System and CBP's passenger reservation information access program. Moreover, foreign governments are imposing similar demands on airlines flying to their countries, including U.S. air carriers. This unmistakable international trend is most evident with the ever-increasing number of countries that require APIS information but also is reflected in the Canadian requirement for access to passenger reservation information for international flights bound for Canada, including flights from the United States. Finally, the Centers for Disease Control has proposed a rule that would require that airlines collect and store broad new categories of passenger contact information.

Information management is precisely where the government should be able to achieve a coherent policy. We appreciate the ongoing efforts of CBP and TSA to more closely align APIS and Secure Flight data requirements. However, the continued absence of a comprehensive, government-wide passenger information access policy is a matter of real concern to us. Nor is there any indication that any element of the Federal Government is inclined to assume the responsibility to develop and oversee such a comprehensive policy.

This needs to change quickly. The U.S. Government must produce a uniform passenger information collection policy that applies to all of its civil aviation security and facilitation programs. Our government should also lead an effort to create such a policy for worldwide application.

A workable government-wide passenger information policy should be predicated on four fundamental considerations.

The first consideration is the recognition that a uniform policy is indispensable to the efficient collection, retention and use of passenger information. Multiple, uncoordinated information demands do not advance aviation security. Instead, they create unneeded complexity, wasteful duplication, and unjustifiable costs to the government, customers and airlines.

The second consideration is that a uniform policy must be based on a single passenger information template that contains the only authorized categories of data that a Federal agency can require collection of or access to. Agencies should be prohibited from imposing unilateral data requirements that go beyond the template. A uniform policy means no ad hoc data requirements.

Similarly, uncoordinated methods of data transmission are unnecessarily complex and costly. This is not the forum to explore how best to resolve this issue. But I want to highlight the importance of working as best we can to develop a single "pipeline" to transmit passenger data to Federal agencies. Independent transmission channels to multiple Federal agencies mean duplicative work for both airlines and the government, and the unnecessary cost and drain on scarce resources that inevitably result from such inefficiency.

The third consideration is that the justification for every passenger information collection program should be evaluated under uniform criteria. The needs of individual agencies may vary but the conditions under which any agency is permitted to collect or access passenger information should not vary. Six basic criteria should be relied upon:

- **Demonstrate civil aviation security or facilitation need.** A clear, direct relationship between the security threat or facilitation need and the information sought should be demonstrated. Presumably, this will be tied to the agency's risk assessment. Data needs not associated with security or facilitation should not be part of any passenger information program.
- **Minimize data demand.** Data required should be the minimum necessary to fulfill an agency's needs. This will reduce impositions on passenger privacy and diminish airline compliance costs.
- **Use existing information sources.** To the extent feasible, agencies should rely on existing government passenger information programs to fulfill their data needs.
- **Avoid adverse effects on passenger processing.** Information collection requirements must avoid adversely affecting passenger processing, whether during the reservations process, airport check-in, security screening, or arrival in the United States from overseas.
- **Conduct thorough cost evaluation.** Passenger information collection, storage and transmission costs, as well as individual passenger compliance costs must be recognized and carefully evaluated. A cost-benefit analysis based on these factors should be undertaken for each information collection or access program.
- **Minimize false hits.** If passenger information is used to evaluate a passenger for security purposes, the program must contain measures that minimize false hits and enable the agency to evaluate its false hit experience.

The fourth consideration is that the privacy implications of any proposed passenger information requirement must be rigorously examined before the implementation of such a program. This is a matter of both accountability and legitimacy. It is a matter of accountability because the government should not demand personal information without performing such a careful analysis. It is a matter of legitimacy because the traveling program will not long support a government-imposed information program that it believes does not scrupulously protect an individual's privacy.

At the very least, this means that government programs must adhere to privacy principles that focus on information collection purpose, content, retention and onward transmission limitations. In addition, a prompt and effective redress mechanism must be available to those customers who believe that they have been adversely treated.

Foreign governments' data privacy principles must also be taken into account because U.S. airlines that operate overseas are subject to them. Compliance in other nations is often enforced through both civil and criminal penalties. No U.S. airline should be subject to the conflicting requirements of the U.S. government and a foreign government. This concern is very concrete. U.S. airlines operating to Europe confronted that prospect several years ago when European governments expressed skepticism about the adequacy of CBP's protection and use of passenger reservation information that it accesses. That situation has been resolved for the time being. It, however, left us with the clear realization that the U.S. Government—and not the U.S. airline industry—has the responsibility for resolving conflicts between its information requirements and the data privacy regulations of other nations.

My experience over the last several years with security issues has convinced me of several things. First, coordination between the government and industry at the outset of the development of any aviation security program is critical and is plainly in the interest of the government, customers, and airlines. Second, we know how to measure the effectiveness of these programs; we should not be afraid to apply to them appropriate metrics—including risk and cost-benefit analyses. Third, we need to formulate, in very short order, a coherent government-wide policy about passenger information collection requirements. Fourth, resolution of privacy issues is crucial to the success of these programs and that resolution is the government's responsibility.

Aviation security needs will change over time but the considerations that I have described in my testimony should facilitate prompt and effective responses to them, no matter how they may evolve.