Statement of

John M. Meenan
Executive Vice President and COO
Air Transport Association, Inc.
before the
Subcommittee on Intelligence, Information Sharing
and Terrorism Risk Assessment
Committee on Homeland Security

July 26, 2007

Madam Chairman and members of the subcommittee let me begin by thanking you for the opportunity to appear today. On behalf of our airline members, I would note at the outset that the focus of this subcommittee on information sharing and the associated application of analytical tools to understanding, managing and mitigating the risks of terrorism, is of paramount importance. The Air Transport Association and our member airlines are committed to providing you with our full support.

With specific reference to the subject of today's hearing – the sharing of critical homeland security information – I am pleased to report that from the perspective of the airline industry, that system is working very effectively and efficiently. Over the past six years since 9/11, the relationships, lines of communication, timeliness, quality and mutuality of the information exchange between government and industry has developed very positively. While we fully appreciate the principle behind the development of a more structured Homeland Security Information Network (HSIN), we are very concerned that, in doing so, we do not in any way inhibit or interfere with the effective system we rely upon today.

The relationship between the airline industry, the Transportation Security Administration (TSA), the Department of Homeland Security (DHS) and the broader law enforcement and intelligence communities is, of course, significantly more developed than that of other sectors. For some forty years we have been the subject of federal government regulation and direction relating to aviation security matters. Since 9/11, and with the establishment of both TSA and DHS, that relationship, of course, has reached even higher levels of sophistication.

We currently have in place well established conduits for the flow of information back and forth between industry and government. These conduits include routine reporting, telephone and electronic exchanges of information, the posting of Sensitive Security Information (SSI) on a TSA secure Web board, and classified briefings to the industry on a regular basis, as well as "need to know" briefings on developing situations. In addition, airline-specific information is conveyed through direct, secure communication (STU calls), as well as through local security briefings.

The Security Directive system and emergency program changes are communicated electronically to provide real-time updates resulting from actionable intelligence. Joint DHS and Federal Bureau of Investigation reports are provided to the industry as deemed necessary along with Homeland Infrastructure Threat and Risk Assessment Center reports. Finally, of course, the airlines are the only sector we are aware of that is required to provide TSA, are with reports of suspicious activity. These reports, once scrutinized, analyzed and processed by TSA then returned to the industry in the form of weekly suspicious incident reports.

In sum, the system we have in place is highly developed and specialized to accommodate the unique relationship between the airline industry and the responsible government authorities. We appreciate the importance of developing analogous systems for other sectors, and would welcome the opportunity to share our experience. We would, however, caution against any well intentioned but misguided effort to conform this specialized aviation system with a "one size fits all" approach applicable to all critical infrastructure sectors. We would be very concerned with requirements, through HSIN or in other ways, for duplicative, unnecessary or extraneous reporting – or any requirements that either slow the flow of information or inhibit the candid exchanges that are the hallmarks of our existing system.

Our government's approach to civil aviation security is multilayered. This is the most sensible response to the shifting threats that our nation confronts. An integral element of that approach is the government's collection and analysis of passenger information for both domestic and international flights. Vetting passengers against government watch lists – in accordance with strict procedures that recognize that such lists need to be carefully "scrubbed" – safeguards customer privacy and provides redress opportunities, substantially enhancing security for passengers and crew members alike.

These information-centric passenger vetting programs are expanding – both here and overseas. They will create substantial new demands on governmental agencies, airlines and travelers. The problem is that these governmental passenger-information requirements, thus far, have only produced a mosaic. It remains to be seen if a coherent a picture will emerge.

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 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. The continued absence of a comprehensive, governmentwide 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 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.

In conclusion, I would reiterate that from the perspective of the airline industry, we believe that our highly evolved information-sharing system is working very efficiently and effectively. Given the extensive experience that has gone into its development, we believe it could well serve as a guide to facilitate appropriate sharing by other sectors. We look forward to continuing to adjust and fine-tune our system in close consultation with our TSA and DHS counterparts. We would, however, caution strongly against any program that seeks to force changes in this highly functional system simply for the sake of cross-sectoral consistency. At the same time, with respect to the collection of passenger data as opposed to the sharing of intelligence or suspicious incident reporting, we believe that better coordination between government agencies is imperative.

Thank you very much for the opportunity to express our views on this important matter.