



Homeland Security

The following document was received by the DHS Privacy Office on behalf of the DHS Data Privacy and Integrity Advisory Committee.

Anna Slomovic
Secure Flight Working Group
"Written Testimony"

For more information please visit: www.dhs.gov/privacy or email the DHS Privacy Office: privacy@dhs.gov or the DHS Data Privacy and Integrity Advisory Committee: privacycommittee@dhs.gov.

Additional Contact Information:

Data Privacy and Integrity Advisory Committee
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Telephone: 571-227-3813
Fax: 571-227-4171

Ladies and gentlemen,

Thank you for giving me an opportunity to talk with you about the report of the Secure Flight Working Group.

As you know, the Secure Flight Working Group was chartered under the Aviation Security Advisory Committee of TSA. The group, composed of privacy and security experts from industry, academia and the advocacy community, was asked to review privacy and security provisions of the Secure Flight Program. All members of the Working Group were required to go through a security clearance process and to sign non-disclosure agreements.

Our report was presented to ASAC last week.

I would like to give you a brief summary of our findings and to spend most of my allotted time answering any questions you might have.

The bottom line in our nine-month review of the Secure Flight program is that the program is not ready for implementation because some fundamental questions have not been clearly answered. Because these questions were not answered, it was not possible for us to evaluate the program's privacy and security provisions.

First and foremost, we never got a clear answer about the **goal or goals** of Secure Flight. There are at least four possible sets of goals.

- We were told that Secure Flight is a matching program that matched the identifying information of those who fly to identifying information of known and suspected terrorists on the government's consolidated watch list.
- However, a somewhat different goal appeared in the documents that we examined as part of our work. The draft OMB Exhibit 300, dated February 9, 2005, says that in addition to watch list matching, "violent criminal data vetting has been envisioned" for Secure Flight. Such vetting would make Secure Flight more of a general purpose law enforcement tool than a focused terrorist watch list matching program.
- Yet another possible goal for Secure Flight was stated by Mr. Justin Oberman in his Congressional testimony on June 29, 2005. That testimony implies that Secure Flight is headed towards looking for "sleeper cells" and those who are not on the watch list. I quote from Mr. Oberman's testimony: "It [Secure Flight] will identify people who are known or suspected terrorists contained in the terrorist screening database, and it ought to be able to identify people who may not be on the watch list. It ought to be able to do that. We're not in a position today to say that it does, but we think it's absolutely critical that it be able to do that. And so we are conducting this test of commercially available data to get at that exact issue." A bit further in his testimony Mr. Oberman continued, "That's precisely the reason we have been conducting this commercial data test, why we've extended the testing period, and why we're very hopeful that the results will prove fruitful to us." Even putting aside the question of whether the goal of looking for "sleepers" was articulated in TSA's System of Records Notice and Privacy Impact Assessment for Secure Flight Testing, the goal of

searching for unknowns “sleepers” is clearly different from a goal of matching passengers to names on the watch list of known or suspected terrorists.

- Finally, TSA was never explicit about the use of Secure Flight as an intelligence tool that permits the government to track the movements of known and suspected terrorists.

Because different program goals require different data collection and analysis, it was not possible for us to address privacy provisions of Secure Flight without knowing what goals the program was trying to accomplish.

Furthermore, TSA did not share with us a comprehensive **policy document** that defines oversight and governance responsibilities for the Secure Flight program.

Our second major question had to do with the **architecture** of Secure Flight. The Working Group was given very limited information about the program’s architecture. We did not learn much about software and hardware being used, or about how data will be collected, transferred, analyzed, stored and deleted.

TSA did not provide us any test results that showed the **effectiveness of algorithms** used to match passenger names to the watch list, although a major claim for Secure Flight is that it will improve the accuracy of matching because the program will use much better matching technology than is now in use. This improvement in matching is claimed to be a form of compensation for privacy loss resulting from government collection of

personal information from travelers. We were never given any information about the criteria used to select matching algorithms or about their effectiveness.

Although SORNs and PIAs were published for the test phase, we were told that we could not see such documents for the Secure Flight program itself because the documents were still in the rulemaking process and the nature of the process precluded the disclosure of the documents outside DHS. We did not see privacy policies, security plans, or data management plans for the program.

Third, we did not get information about how Secure Flight is going to **interact with other vetting applications** running on the same platform. Various documents contain hints that Secure Flight would interact with Registered Traveler and other programs in order to reduce the number of false positives, and possibly in order to make sure that someone on one of the “cleared” lists did not show up on a watch list. However, neither the purposes nor the nature of this interaction between the programs was ever discussed with us. Given that different vetting programs collect different personal information and operate under different data retention and other policies, we could not determine the privacy impact of these interactions on Secure Flight.

Finally, we did not get any information on the way **commercial data** sources would be used or see the results of commercial data testing conducted by TSA over the past several months.

Because we were provided only limited information, we were not able to do a substantive evaluation of the Secure Flight program's privacy and security provisions. We do have some recommendations, however.

Because all the other issues flow from the definition of the program, we recommend that there should be a written statement of the goals of Secure Flight, signed by the Secretary of DHS. This statement should only be changed on the Secretary's order. Even if the program's goals evolve over time, there should be one, unambiguous statement of goals at any given time.

Documentation accompanying the statement should include: (1) a description of the technology, policy and processes in place to ensure that the system is only used to achieve the stated goals; (2) a schematic that describes exactly what data is collected, from what entities, and how it flows through the system; (3) rules that describe who has access to the data and under what circumstances; and (4) specific procedures for destruction of the data. There should also be assurance that someone has been appointed with sufficient independence and power to ensure that the system development and subsequent use follow the documented procedures.

This concludes my remarks. At this point, I would be happy to answer questions.