REPORT OF THE SECURE FLIGHT WORKING GROUP

Private & Confidential Document

September 19, 2005

Presented to the

Transportation Security Administration

Report of the Secure Flight Working Group

Confidential Report Dated September 19, 2005

Preface

This report represents the collective effort and work of a nine-member advisory committee – termed the Secure Flight Working Group (SFWG) –a body of experts in privacy and security appointed by the Transportation and Security Administration of the United States of America. The report document was compiled by Ponemon Institute – a Michigan-based research organization dedicated to advancing responsible information management practices within business and government. The principal facilitator for this document is Dr. Larry Ponemon.

Ponemon Institute extends its sincere appreciation to the members of the SFWG for their individual contributions, counsel and support. We also wish to acknowledge the support of the Transportation Security Administration for providing confidential information and documents that allowed us to verify the factual content included in this document.

Table of Contents

I. Secure Flight Working Group Executive Summary

Secure Flight is the name of a proposed program to bring the passenger screening system function currently performed by private airlines under the federal umbrella. Section 4012 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) requires the Transportation Security Administration (TSA) to "assume the performance of the passenger screening function comparing passenger information to the automatic Selectee and No-Fly lists and utilize all appropriate records in the consolidated and integrated terrorist watch list maintained by the Federal Government in performing that function."

Secure Flight's purpose, in the broadest sense, is to make air travel safer by either preventing persons who pose a risk to airline safety from boarding airplanes, or subjecting them to an increased physical search designed to detect devices that could harm the plane or its passengers before they board.

Secure Flight faces a difficult and controversial task. It is difficult because no system will ever identify all travelers who present a risk to aircraft, because no list of those who pose a threat to aviation safety can ever be complete. In addition, there is not sufficient available intelligence to determine what characteristics indicate someone will be a threat. Even if it were possible to fix these limitations, any system can be compromised by someone sufficiently motivated.

Secure Flight is controversial for two reasons. First, such a system requires government collection of some personally identifiable information of the massive numbers of people who fly each year. Second, intuition suggests that the more data collected, the more likely it is that the risk-identification process will succeed. However, there is no evidence available to validate this proposition, or to quantify how much more data about an individual would result in greater safety. Many citizens and organizations objected to Secure Flight's predecessor CAPPS II because of the invasion of privacy posed by large-scale government collection of personal information, and because of concerns that the data collection process would be abused. CAPPS II was abandoned in August 2004 and Secure Flight emerged as its successor.

Private organizations and government agencies continue to be concerned about the privacy impact of Secure Flight. In March 2005, a Congressionally mandated report from the Government Accountability Office (GAO) gave TSA a failing grade on almost every privacy vector evaluated by them:

> *Until TSA fully defines its operational plans for Secure Flight . . . it will remain difficult to determine whether the planned system will offer reasonable privacy protections to passengers who are subject to prescreening or mitigate potential impacts on passengers' privacy.*[1]

[1] GAO, "Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed," GAO-05-356, March 28, 2005, p. 11.

Our advisory body – the SFWG – was convened to meet in private with TSA officials in order to evaluate the proposed Secure Flight system by drawing upon the privacy and security expertise of individual members.

While we hold differing views on the desirability of any passenger pre-screening program, we came together on a nine-month project to provide an independent and objective assessment of whether the proposed system minimizes government invasion of the privacy of U.S. citizens and builds in effective security for the personal data it will use. We met face-to-face three times in Washington, D.C., and engaged in many phone and e-mail conversations. Members received security clearances to review confidential information. All meetings and other discussions took place between January and September 2005.

This report offers the SFWG's conclusions about the Secure Flight passenger screening system. It also makes certain recommendations for the further development of Secure Flight on the following topics: Architecture; Identity Matching; Policy, Regulatory and Oversight Structure; Watch Lists; Test Phase—Commercial data; Passenger Screening; Passenger Name Record; Push vs. Pull Models for Passenger Data; and Data Retention Issues.

II. Questions

The SFWG found that TSA has failed to answer certain key questions about Secure Flight: First and foremost, TSA has not articulated what the specific goals of Secure Flight are. Based on the limited test results presented to us, we cannot assess whether even the general goal of evaluating passengers for the risk they represent to aviation security is a realistic or feasible one or how TSA proposes to achieve it. We do not know how much or what kind of personal information the system will collect or how data from various sources will flow through the system.

Until TSA answers these questions, it is impossible to evaluate the potential privacy or security impact of the program, including:

- Minimizing false positives and dealing with them when they occur.
- Misuse of information in the system.
- Inappropriate or illegal access by persons with and without permissions.
- Preventing use of the system and information processed through it for purposes other than airline passenger screening.

The following broadly defined questions represent the critical issues we believe TSA must address before we or any other advisory body can effectively evaluate the privacy and security impact of Secure Flight on the public.

1. What is the goal or goals of Secure Flight? The TSA is under a Congressional mandate to match domestic airline passenger lists against the consolidated terrorist watch list. TSA has failed to specify with consistency whether watch list matching is the only goal of Secure Flight at this stage. The Secure Flight Capabilities and Testing Overview, dated February 9, 2005 (a non-public document given to the SFWG), states in the Appendix that the program is not looking for unknown terrorists and has no intention of doing so. On June 29, 2005, Justin Oberman (Assistant Administrator, Secure Flight/Registered Traveler) testified to a Congressional committee that "Another goal proposed for Secure Flight is its use to establish "Mechanisms for … violent criminal data vetting."[2] Finally, TSA has never been forthcoming about whether it has an additional, implicit goal – the tracking of terrorism suspects (whose presence on the terrorist watch list does not necessarily signify intention to commit violence on a flight).

While the problem of failing to establish clear goals for Secure Flight at a given point in time may arise from not recognizing the difference between program definition and program evolution, it is clearly an issue the TSA must address if Secure Flight is to proceed.

2. What is the architecture of the Secure Flight system? The Working Group received limited information about the technical architecture of Secure Flight and none about how software and hardware choices were made. We know very little about how data will be collected, transferred, analyzed, stored or deleted. Although we are charged with evaluating the privacy and security of the system, we saw no statements of privacy policies and procedures other than Privacy Act notices published in the Federal Register for Secure Flight testing. No data management plan either for the test phase or the program as implemented was provided or discussed.

[2] Working Draft, OMB submission, dated February 9, 2005, p. 8.

3. **Will Secure Flight be linked to other TSA applications?** Linkage with other screening programs (such as Registered Traveler, Transportation Worker Identification and Credentialing (TWIC), and Customs and Border Patrol systems like U.S.-VISIT) that may operate on the same platform as Secure Flight is another aspect of the architecture and security question. Unanswered questions remain about how Secure Flight will interact with other vetting programs operating on the same platform; how it will ensure that its policies on data collection, use and retention will be implemented and enforced on a platform that also operates programs with significantly different policies in these areas; and how it will interact with the vetting of passengers on international flights?

4. **How will commercial data sources be used?** One of the most controversial elements of Secure Flight has been the possible uses of commercial data. TSA has never clearly defined two threshold issues: what it means by "commercial data;" and how it might use commercial data sources in the implementation of Secure Flight. TSA has never clearly distinguished among various possible uses of commercial data, which all have different implications.

Possible uses of commercial data sometimes described by TSA include: (1) identity verification or authentication; (2) reducing false positives by augmenting passenger records indicating a possible match with data that could help distinguish an innocent passenger from someone on a watch list; (3) reducing false negatives by augmenting all passenger records with data that could suggest a match that would otherwise have been missed; (4) identifying sleepers, which itself includes: (a) identifying false identities; and (b) identifying behaviors indicative of terrorist activity. A fifth possibility has not been discussed by TSA: using commercial data to augment watch list entries to improve their fidelity. Assuming that identity verification is part of Secure Flight, what are the consequences if an identity cannot be verified with a certain level of assurance?

It is important to note that TSA never presented the SFWG with the results of its commercial data tests. Until these test results are available and have been independently analyzed, commercial data should not be utilized in the Secure Flight program.

5. **Which matching algorithms work best?** TSA never presented the SFWG with test results showing the effectiveness of algorithms used to match passenger names to a watch list. One goal of bringing watch list matching inside the government was to ensure that the best available matching technology was used uniformly. The SFWG saw no evidence that TSA compared different products and competing solutions. As a threshold matter, TSA did not describe to the SFWG its criteria for determining how the optimal matching solution would be determined. There are obvious and probably not-so-obvious tradeoffs between false positives and false negatives, but TSA did not explain how it reconciled these concerns.

6. **What is the oversight structure and policy for Secure Flight?** TSA has not produced a comprehensive policy document for Secure Flight that defines oversight or governance responsibilities.

III. Architecture

The SFWG was provided limited information about the technical architecture of the Secure Flight application and about the platform on which the application will be executed. Limited information was provided to describe the architecture, the analytic software that will be used or other software and hardware that will be used for data collection, processing, storage or deletion. No copies of privacy policies and procedures were provided to SFWG except for the documents published in the Federal Register for Secure Flight testing. No data management plan either for the test phase or for the program was provided or discussed.

Based on the information provided to SFWG, it is impossible to determine whether or how the architecture will comply with the program's privacy policies (even to the limited degree those policies have been specified in published documents) or with data management plans that will be created in compliance with federal regulations. It is also impossible to determine how these policies will be enforced. However, the information provided to SFWG raises three types of potential privacy concerns.

- How will the Secure Flight program ensure that its policies on data collection, use and retention will be implemented and enforced on a platform that also operates programs with significantly different policies in these areas?
- How will the Secure Flight program interact with other vetting programs operating on the same platform?
- How will the Secure Flight program interact with Customs and Border Protection (CBP) systems which are used to bring Passenger Name Record (PNR) data from airline reservation systems into the government?

The information that was provided to SFWG states that the Secure Flight program will be executed on a multi-mission, multi-use Transportation Vetting Platform (TVP).[3] This platform has a modular and extensible architecture, which implements technologies and analytic software for multiple vetting programs. Other programs that operate on the same platform include Registered Traveler, Hazardous Materials Driver Screening, the Aviation Workers Credentialing System, and Airline Crew Vetting System.

As described in OMB Exhibit 300 draft,

> *"The TVP provides a reusable vetting service that allows policy driven design and implementation as well as dynamic configurations of workflow, models, rules, and scoring. It facilitates the auditing of compliance and enforcement of policies for data sharing. It permits easy integration of existing data sources (both government and commercial) without aggregating all information in one place (i.e., leveraging the data and the expertise where they exist). This open design implies that processes and tools can be easily removed and inserted ("plug and play"), which provides savings in development and maintenance costs. Finally, the architecture is founded on proven commercial products for data exchange, workflow, analysis, and reporting to leverage commercial industry best practice and R&D in integrated systems."*[4]

[3] OTVC, Secure Flight Program Overview dated December 21, 2004, p. 6; Working Draft OMB Exhibit 300 submission, dated February 9, 2005, pp. 10-11.
[4] Working Draft OMB Ex. 300, op. cit.

While the use of common architecture and software for multiple vetting applications could lead to cost savings and greater efficiency for the government, its raises privacy concerns. Secure Flight has been presented to the SFWG as a tightly focused program that uses limited personal information to vet airline passengers against specific terrorist screening databases.[5] However, Secure Flight operates on the same TVP platform and uses the same software as applications that use more extensive personal information, perform risk scoring on individuals, and retain information for significantly longer time periods.[6] The platform is also described as being programmable "in real-time as threat priorities change and as intelligence inputs evolve."[7]

For example, the current data storage period of airline passenger data is configurable and may be changed from the currently anticipated 72 hours after the completion of the last flight in the itinerary to a period of any length.[8] TSA has not provided information to the SFWG on the way in which the platform will support the more limited Secure Flight data collection, uses and retention periods, or what technical controls will be implemented to enforce these limitations.

The Secure Flight Level 3 Test Plan and Test Procedure indicate that name matching software to be used by Secure Flight is Infoglide's Bladeworks.[9] Infoglide's Search Server (ISS), which will interface with search databases,[10] is the same software used for other vetting applications and the same software that was used in CAPPS II.[11]

[5] Untitled TSA document GAO-94-SF-Testing-v82.doc, February 9, 2005, Appendix. There is, of course, a risk assessment produced by possible matches to watch lists and by applying CAPP's behavioral rules to PNR data.

[6] For example, the Registered Traveler program pilot collects "full name, Social Security Number, other names used, home address, home telephone number, cell phone number, email address, date of birth, place of birth, nationality, gender, prior addresses (for the past five years, driver's license number, and biometric identifiers (fingerprints and/or iris scan)." The same Privacy Impact Assessment goes on to talk about the use of the information for "security threat assessment." No retention period is included in the document. [Registered Traveler Pilot Privacy Impact Assessment, June 24, 2004, available at <http://www.tsa.gov/interweb/assetlibrary/PIA_RT_OMB.pdf>, last visited May 23, 2005.] Hazardous Materials Endorsement for Driver's License program collects "full name (as well as any aliases), current and three previous home addresses, mailing address (if different from home address), data of birth, Social Security Number, gender, height, weight, eye color, hair color, issuing State, Commercial Driver's License number, HAZMAT endorsement type, place of birth, country of citizenship, and alien registration number. … Additionally, in the event that the assessment identifies an individual as a match to a name from a terrorist-related database and the individual believes that such identification is in error, that individual may be required to submit fingerprints and other information to verify identity and disprove the adverse information." The information is collected to perform a security threat assessment on the individual. The Privacy Impact Assessment does not state a retention period, although it states that TSA has requested a "short" retention period from NARA. [Security Threat Assessment for Individuals Holding a Hazardous Materials Endorsement for a Commercial Driver's License, Revised Privacy Impact Assessment, June 1, 2004, available at <http://www.dhs.gov/interweb/assetlibrary/privacy_pia_hazmat.pdf>, last visited on May 23, 2005.

[7] Working Draft OMB Exhibit 300, p.10.

[8] OTVC Secure Flight Program Overview dated December 12, 2004, p. 17.

[9] OTVC, Secure Flight PNR Testing, Level 3 Test Plan and Test Procedures.V.1.1, January 4, 2005, p. 28.

[10] OTVC, Level 3 Test Plan, op. cit., p. 25.

[11] As noted elsewhere, TSA did not provide the SFWG with data justifying the selection of InfoGlide's product. A goal of bringing watch list matching inside the government was to ensure that the best available matching technology was used uniformly. The WG saw no evidence comparing InfoGlide's product with other products. As a threshold matter, TSA did not describe to the WG its criteria for determining the optimal matching software. There are obvious and probably not-so-obvious tradeoffs between false positives and false negatives, but TSA did not explain how it reconciled those concerns.

Infoglide's product description states that:

> *"ISS is also the tool that enables Bladeworks to search multiple, disparate, remote databases. By employing Similarity Search Agents™ (SSA) to access data wherever it resides, databases with different formats, platforms, locations, and data types can be searched. ..Infoglide Software has developed a highly flexible, completely open framework for aggregating data from multiple sources; an SSA is installed on each search database, leaving a virtually unnoticeable footprint, allowing an unlimited number of data sources to be used in the risk assessment, ID authentication, or fraud detection process. This ability to search data without having to combine databases solves issues of data access and ownership between organizations, thereby solving privacy, political, and legal issues. If desired, only a score can be returned, without the data record and its inherent values. This ensures the privacy and security of the underlying information."*[12]

The limited descriptions of TVP and ISS do not indicate any technical impediments to a significant increase in the scope and intrusiveness of Secure Flight vetting. Audit controls are not adequate as the sole policy enforcement mechanism because even regular audits find problems only after they have occurred.

An additional privacy concern is the possible linking between Secure Flight and other applications which operate on the same platform, such as Registered Traveler. It appears that various vetting programs will be linked in some way. According to an unnamed TSA document provided to the SFWG, the Secure Flight Master Files will contain "lists of trusted individuals that have been previously screened and cleared as a result of either redress or credentialing programs (e.g., Registered Traveler, Federal Flight Deck Officers, Armed Law Enforcement Officers)… to facilitate the screening process and minimize the number of passengers erroneously identified for secondary screening."[13] SFWG was not provided sufficient information to permit an evaluation of the way verification against "trusted traveler" lists will be conducted in order to evaluate whether such verification presents privacy concerns.

Finally, there may be a privacy concern because of sharing of passenger data between TSA and CBP. SFWG was informed that passenger data will be collected via the existing CBP connection with airline reservation systems. No further information was provided about the interaction between the Secure Flight application and CBP systems or applications, or between the Secure Flight program and CBP's international passenger vetting activities. It is, therefore, impossible to evaluate whether this use of systems outside the control of the Secure Flight program or OTVC presents additional privacy concerns.

[12] InfoGlide Corporation, Bladeworks White Paper, December 2003, p. 5, available at <http://www.infoGlide.com/images/Bladeworks.pdf>, last visited May 23, 2005.

[13] Unnamed document, 2900.4, Par. B.

IV. Identity Matching

The challenge of Secure Flight is to reliably match passenger records to watch list records. In the context of 1.8 million passengers a day and a TSA watch list of 70,000 – 160,000 names, merely comparing the two sets of names is almost worthless in two directions: because names on one list or the other may be misspelled, or because a single name can be written in various ways (Robert Smith, R. Smith, Bob Smith). A direct match misses valid matches (produces too many false negatives), while, at the same time, because there are many common names, it produces an intolerable number of false positives.

To avoid false negatives, a name search must use fuzzy matches, comparing multiple variations of names to compensate for variations like Robert and Bob. To avoid false positives, a match must look at more information than name. A major finding of the Secure Flight test is that the passenger name records (PNRs) compiled by airlines do not have the information necessary for a reliable match. In particular, because the second most common element in the Terrorist Screening Database (TSDB) is date of birth (DOB), the most useful piece of information for resolving false positives would be DOB, but PNRs do not contain DOB. Conversely, PNRs contain a lot of extraneous data of no value to matching.

A search on any broad name-based database will demonstrate that many individuals share the same names. Trying to determine whether this Emily Williams, Robert Jackson or Mark Whitaker is the actual Emily, Robert or Mark you are looking for has always been a major challenge. This challenge has been exacerbated by our tendency to use nicknames and for clerks to misread handwritten information or just mistype the information they see or hear. Foreign names add complexity.

Credit reporting reform in the early 1990's culminating in 1996 amendments to the Fair Credit Reporting Act was driven to a significant extent by credit files that were either fragments (data missing) or mixed (data from more than one individual). A fragment meant that a consumer might be hurt by missing positive information, while a lender would be hurt by either missing positive information (a good credit) or negative information (a potential bad credit). A merged file might lead to a consumer losing a credit opportunity because of someone else's negative behavior. By requiring more data when requesting or submitting data the credit reporting agencies were able to develop matching algorithms that reduced fragments and mixed files.

The costs associated with mismatched data in Secure Flight are more dramatic. A false negative is a risk to aviation safety, while a false positive might result in an individual losing the freedom to travel. Nevertheless, Secure Flight poses issues similar to those that have faced the credit industry. To be successful, Secure Flight must match a passenger record from an airline with a list of individuals who must not fly (No-Fly list) and those requiring additional screening (Selectee list). To match with minimal false positives and false negatives, Secure Flight is dependent on the adequacy of data in the passenger record, No-Fly list and Selectee lists.

TSA has the ability to enhance these records with private sector information. Of course, the added data must be the correct data. Credit reporting was improved when full first name and Social Security number (SSN) were added more consistently to the matching process. SSNs are not applicable to the Secure Flight context, because SSNs are available on very few if any suspected terrorists in the TSDB. TSA has concluded from the Secure Flight test that the one element of data that would add the greatest value to matching reliability is date of birth, which is in a large percentage of records in the TSDB. It isn't clear what if any other elements would add reliability. The more data added and the more sensitive the data, the greater the security and privacy risks would be.

The effectiveness of name matching processes also depends on the choice of matching algorithm. The effectiveness of the algorithms is in turn dependent on the assumptions and judgments made by the statisticians and analysts building the models. For example, algorithms that are built based on matching U.S.-structured identities might not be as efficient in processing variations of foreign identities, as compared with models built based on those foreign variables. However, no test results have been shared with SFWG comparing the effectiveness of different algorithms applied to databases of foreign names.

The private sector has used analytic processes to improve data matching over the past 15 years. These systems use the elements of an identity to match that identity to identities the system has seen in the past. While each matching system is different, they are all based on matching as many elements as possible. Those elements include last name, first name, and middle initial, current address, past addresses, telephone numbers, SSN, driver's license number, and proprietary information. The systems conduct both exact matches (the information matches exactly) or logical matches based on a mixture of exact matches and matches that while different are probable. An example is the nickname Peggy being a match for the proper name Margaret if the other variables match. The more elements that match the more assured one will be that identities match.

The TSA has acknowledged that PNR data flows from the airlines are inadequate as a basis for watch list matching, in particular because the PNR does not include the same categories of information that are on the watch list – especially DOB. Therefore the TSA is considering requiring from the airlines specific data elements (full name and date of birth) that will assist in matching names on the watch lists. Also, TSA is considering the use of commercial data providers to improve the matching process. Unfortunately the TSA has not shared with the SFWG – and we believe TSA has not defined even internally – either the process by which commercial data would be used by the government or by its commercial contractors or the results of its tests of commercial data.

Most fundamentally, TSA has not stated – and seems not to have decided internally – whether it sees value in using commercial data: (a) to verify or authenticate identification or (b) to augment airline-supplied data in order to improve the reliability of matches. Identity verification and match reliability are two different things. Commercial data can be used to verify that a claimed set of identifiers correspond to a known identity. (A different question is whether a person with a valid set of identifiers is in fact who he claims to be.) Match reliability is a different question.

Commercial services are very good at augmenting missing data, and by using broader data sets, commercial services are often able to determine the probability that two identities actually match. However, private sector services are only as good as the input data they receive. If a commercial service only has limited information from an airline, the service will be limited in its ability to reduce false negatives and positives, or to supply additional information that the TSA could then use to reduce false positives and negatives. The TSA has not shared test results so we cannot make a judgment on how well the elements matched in the private sector test.

The TSA has discussed using logical systems that sound out a name and match with the spelling of other names associated with that name. This would likely reduce false negatives, but not false positives.

TSA has not discussed with us the other side of the matching equation: use of commercial data to augment the watch lists. One of the greatest limitations of Secure Flight as described to the SFWG seems to be that not much identifying information is available on most suspected terrorists. Augmenting passenger lists with a lot of commercial data, however accurate this data is, will not improve the quality of matches unless there is a corresponding increase in the amount of data on the watch list side.

Synthetic and Stolen Identities

Synthetic identities are a leading contributor to, and the fastest growing segment of, the ID fraud problem in the United States. These are fabricated identities that take real identity elements, change them slightly so that they are plausible, and then build a history around the fake identities. The methodologies and data elements needed to commit these crimes are shared by fraudsters. There is no reason to believe these skills have not also been shared with terrorists. The TSA has not provided this group with any information that would suggest these new forms of identity fraud have been factored in to the Secure Flight vetting process.

Another problem is stolen identities. In order to steal an identity in the U.S., one needs full name and SSN. One can gather those two pieces of information from many sources, including a black market for identity elements. Once one has these two pieces of information, one can then use them to create false credentials, such as a driver's license. The skills to commit these crimes are also shared by fraudsters.

Effectiveness and Privacy

The first step in determining whether a system meets appropriate privacy and information security standards is by measuring whether the system is effective in meeting its business objectives. In the case of Secure Flight, that means passenger information submitted by airlines must be matched against a growing list of risky identities with a low incidence of false negatives and a manageable level of false positives.

The history of other vetting programs would lead one to believe that matching only on name and DOB would surely lead to a high number of false positives. Furthermore, matching only on those two elements would make it fairly easy to build false credentials that would not match the file, leading to false negatives. Experience with other systems would lead one to suggest that matching on a broader element set would both reduce false positives and negatives. Furthermore, matching on broader number of elements would increase the effectiveness of third party data services. Our committee did not have information from the third party tests necessary to determine how much additional information would be needed from the PNRs to improve the third party match process.

In particular, our group received no information from TSA indicating that commercial databases have the kind of data necessary to resolve the Secure Flight dilemma: matching identifying information on passenger lists comprised almost primarily of U.S. residents with lists of suspected terrorists comprised largely of non-US residents.

V. Policy, Regulatory and Oversight Structure

Secure Flight is part of a multi-layered security program and should be developed and implemented as such. So far, however, Secure Flight is being developed without the authorization and guidance of a clear, comprehensive and published policy document issued by a politically accountable senior official, stating the goals of Secure Flight clearly and to the exclusion of other goals, until such time as that basic policy document is amended.

The inability of the TSA to implement Secure Flight can be traced directly to the absence of such a document. The collection of personal data without plan or processes is by definition inconsistent with adequate privacy and security processes.

The basic policy document should cover several basic points:

- That there is a program called Secure Flight;
- That the program is part of a multi-layered aviation security program;
- A basic description of the goals of the Secure Flight program;
- That the Secure Flight program is to be administered by the Department of Homeland Security (DHS) in coordination with the Department of Transportation (DOT) and the Director of National Intelligence (DNI);
- That the Secure Flight program, insofar as it required or used personal information of travelers, would be governed by procedures approved by the Secretary of DHS in consultation with the Attorney General;
- That there would be certain data and statistics maintained, both to measure the effectiveness of the Secure Flight program and to allow the assessment of the impact of the program on privacy;
- That there would be an annual report on all aspects of the Secure Flight program, prepared in both an unclassified and a classified version, to be provided to the President and relevant and interested Committees of Congress.

Regulatory Structure

The regulatory structure for Secure Flight derives from the Aviation and Transportation Security Act of 2001 and Section 4012 of the Intelligence Reform and Terrorism Prevention Act of 2004.

The Secure Flight regulatory structure is governed by the Privacy Act, the Federal Register public commentary process and the Privacy Impact Assessment requirements of the E-Government Act of 2004.

Oversight Structure

The oversight structure for Secure Flight should be focused on the effectiveness and privacy aspects of the program. The Secure Flight oversight structure could possibly borrow from the oversight regimes for federal law enforcement and U.S. intelligence activities.

While much of the Secure Flight oversight structure could be rule-based, some of it would have to be procedure-based, with specific articulation, request, approval and reporting required. However, this latter function should be part of the operational aspect of Secure Flight, whether in the field or as part of the implementation or regulatory process. The oversight structure should be developed in coordination with the Attorney General and DNI.

The oversight structure could also include the Secure Flight appeal and review process to afford redress for individual passengers; but such process could be also be part of another bureaucratic function.

Public Trust

The importance of public trust in all levels of Secure Flight activity and responsibility in the government simply cannot be overemphasized. Every Secure Flight policy, regulatory and oversight related document, event act or process should be developed and implemented in a manner conducive to fostering public confidence.

VI. Watch Lists

There are two categories of watch-listed names relevant to aviation security: “No-Fly” and “Selectee.” Persons on a No-Fly list are forbidden to board aircraft; if they are encountered, law enforcement is called and the passenger will be questioned and possibly detained. A Selectee list consists of persons who may be permitted to board aircraft, but must first undergo secondary screening. Both the No-Fly and Selectee lists are administered by TSA’s Transportation Security Intelligence Service (TSIS). The No-Fly and Selectee lists comprise a subset of the consolidated watch list administered by the Terrorist Screening Center (TSC) at the FBI.

The SFWG was not provided with the criteria for placing names on the TSC watch list or on the No-Fly and Selectee subsets. The SFWG understands that such criteria do exist, but to the knowledge of the SFWG they have never been validated outside the government.

As orally described to the SFWG, and as described in the June 2005 report of the Department of Justice Inspector General, the process for nominating and placing passengers on the consolidated watch list maintained by the TSC involves many federal agencies. Domestic nominations are submitted to and screened by the TSC; international nominations are submitted to and screened by the National Counter-Terrorism Center (NCTC).[14]

Based on intelligence, the Central Intelligence Agency (CIA), the FBI, the Department of State, the Department of Defense and the Department of Homeland Security, nominate individuals to the international terrorist watch list through the NCTC. The NCTC vets the intelligence that provides the basis for nominating an individual to verify that the individual should be placed in the database. The NCTC maintains the classified list of suspected and known international terrorists for the U.S. government, plus the backup information about the individual. NCTC exports to the TSC a sensitive but unclassified database of identifying information on individuals known to the NCTC. For domestic terrorists (members of homegrown groups with no ties abroad), domestic agencies (mainly the FBI) nominate individuals to the TSC. The combined list of names and associated identifying information submitted to TSC directly and via the NCTC together constitute the TSDB.

TSC in turn provides watch-listed names to the Transportation Security Intelligence Service (TSIS), which administers the No-Fly and Selectee watch lists. The No-Fly and Selectee lists are subsets of the TSDB. All entries on the No-Fly and Selectee lists must contain full first and last name and date of birth. Passengers on the Selectee list may be allowed to board but will have to undergo additional screening.[15] TSA airport screeners will not be notified why a Selectee has been chosen. For those identified as No-Flys, law enforcement is called and may arrest the individual if they find a reason to arrest.[16] Even if law enforcement finds no reason to arrest, individuals on the No-Fly list will not be allowed to board or charter a plane.[17]

[14] U.S. Department of Justice, Office of the Inspector General, Audit Division (DOJ IG Report), “Review of the Terrorist Screening Center,” (redacted for public release), Audit Report 05-27, June 2005, p. 41.
[15] Ibid., p. 48
[16] Ibid. pp. 51, 54.
[17] Ibid. pp. 54-55.

Rick Coffin of TSA explained the watch-listing process:

> *"When an individual is nominated for the TSDB, that nomination is reviewed by TSA to determine if that individual represents a threat to transportation security, and, based on the threat they represent, they may be placed on a Selectee or on the No-Fly list And, so, TSA looks at all of the nominees and decides which ones are on the subset. If you're nominated or recommended to be a Selectee or a No-Fly, that puts you in one of two clear categories on the list that have implications for airport screening. All the others who were determined not to be a threat to transportation security, and we're working this out with TSC, there may be different notification requirements if you encounter this individual because they are on, in the terrorist screening database. We may take no action. He or she may be the second cousin, twice removed of a suspected terrorism financier, not a threat to transportation security. An information requirement for the TSC and those notification requirements will be quantified in the con ops and in our MOUs with the other agencies. So, where we may match against the entire TSDB, or the usable portion of it, we only take action on those that are Selectees or No-Flys, other than the required notification."*[18]

As of spring 2005, there were about 270,000 entries in the TSBD, many of them aliases of the same individual. Of these, about 30,000-40,000 were on the No-Fly list, and 30,000-40,000 were on the Selectee list, for a combined total of about 70,000. As the TSDB and TSA lists are further scrubbed, TSA officials predict that the number of No-Flys might be reduced to as few as 20,000. However, the number of Selectees was expected to increase substantially,[19] so that the total of the No-Fly and Selectee lists might be about 160,000 persons.[20]

In 2004, "the White House Homeland Security Council (HSC) approved new criteria for inclusion of names on the No-Fly and Selectee lists used for screening passengers on commercial airlines."[21] In addition to the criteria themselves, HSC has published guidance on how the criteria are to be applied. TSA officials were not able to clearly describe the criteria or the guidance to the SFWG, nor were the criteria or guidance provided to the SFWG. As orally described to the SFWG, individuals who are considered threats to civil aviation are placed on the No-Fly list, while "individuals who…might in some way affect the safe operation of an aircraft," are categorized as Selectees.[22] Justin Oberman, Assistant Administrator of Secure Flight, said that the definition of "supporting terrorism" was a shifting one,[23] and that counterterrorism is "very murky." He noted that in his experience, membership in the TSDB database almost always requires actual support, rather than more tacit support such as writing a supporting Op-Ed.[24] [25] He never referenced the HSC standards for list membership.[26]

[18] Secure Flight, SFWG transcript, 2005a, p. 170.
[19] Secure Flight, SFWG transcript, 2005c, p. 5-8.
[20] Secure Flight, SFWG transcript, 2005c, p. 18.
[21] DOJ IG Report, op. cit., p. 99.
[22] Secure Flight, SFWG transcript, 2005b, p.239.
[23] Secure Flight, SFWG transcript, 2005b, p. 32-33.
[24] Secure Flight, SFWG transcript, 2005b, p. 37.
[25] Secure Flight, SFWG transcript, 2005b, p. 34.
[26] Secure Flight, SFWG transcript, 2005b, p. 38.

According to Nick Grant of the TSA's Transportation Security Intelligence Services (TSIS) to remove a person from the No-Fly and Selectee list, TSIS must coordinate an inverse process that traces back to the original nominating agency. TSA also uses the No-Fly and Selectee lists to vet air carrier employees (including pilots of cargo and charter airlines), cockpit crews, and airport employees. Also, there has been discussion about allowing cruise lines to use a similar list.[27]

One of the main challenges of Secure Flight is that the watch lists are primarily comprised of foreign nationals, while the domestic airline passengers the system applies to are overwhelmingly U.S. citizens. This means that TSA will collect information on millions of innocent Americans while looking for a few suspected foreigners. This fact heightens the importance of minimizing the privacy intrusion on those millions of innocent citizens.

It is clear to SFWG members that the watch listing of individuals is an inexact process. It is also clear that watch listing criteria change from time to time, and that the reliability of the information upon which nominations and listings are based is often uncertain. To some extent these problems are inherent in the nature of the intelligence process. It is of concern, however, that TSA officials were not able to describe the criteria and the process with clarity. Moreover, the problems demonstrate the limitations of the lists and heighten the importance of match criteria and redress processes.

Also, it is clear that the process of adding names to the TSDB requires further refinement. One thing that is crucial to both the mission of keeping terrorists off planes and the goal of minimizing the inconvenience to innocent travelers is improving the identifying information in watch list entries. This is not TSA's responsibility but it is crucial to the success of TSA. The watch lists, we now know, contain names like Edward Kennedy, John Lewis and Cal Thomas. Certainly, they also contain many common names of people of Middle Eastern origin. To distinguish innocent travelers from the suspected terrorists with these common names, more identifying information is needed. Agencies adding names to the watch list should investigate more fully beforehand who exactly is a terrorist and should anticipate the problems that will arise from listing common names, both for the sake of capturing true terrorists and to ensure that innocent people can go their way in an airport.

SFWG members expressed concern about mission creep with the "watch lists," specifically that persons convicted of non-terrorist related crimes would find themselves placed on no-fly and selectee lists.[28] These concerns were heightened by Justin Oberman,'s statement that Washington has a continuously shifting notion of what constitutes "supporting terrorism." That phrase again raises the question of whether mission creep will occur, and if one day, politically active Americans could find themselves singled out as "selectees."

The DHS privacy and civil liberties officers and relevant Congressional committees should seek regular detailed reports of who is being placed on the list, who has been stopped, and a report on how their cases have been handled.

[27] Grant, 2005; Secure Flight, SFWG transcript, 2005(b).
[28] Secure Flight, SFWG transcript, 2005b, p. 38.

VII. Test Phase – Commercial Data

The TSA announced that it would test Secure Flight using passenger records obtained from domestic flights that occurred during the month of June 2004[29] and it issued a Privacy Impact Assessment (PIA) for these tests in September 2004.[30] One of the stated goals of the new program, as described in the PIA, was to reduce the number of individuals who would need to undergo secondary screening while "fully" protecting the civil liberties and privacy of the passengers.[31] The section headlined "Secure Flight Testing Phase" explained that the TSA would use information obtained from commercial data aggregators to help verify the accuracy of the information obtained from passenger records, or PNRs.[32]

"Testing of these procedures will be governed by strict privacy and data security protections. TSA will not store the commercially available data that would be accessed by commercial data aggregators."[33] The findings of the test would be instrumental in determining how the TSA would use commercial data in Secure Flight and, therefore, would lead to the "publication of a subsequent System of Records Notice under the Privacy Act announcing the intended use of such data."[34]

The SFWG was never briefed on the results of TSA's commercial data tests, nor on the privacy and security aspects of how such data was handled, despite repeated requests for this information. Our assessment of the ways TSA used commercial data can only be based on news reports and a GAO letter to TSA concerning its testing of such data in ways beyond the scope of its Privacy Act notices.

The GAO in a July 22, 2005, letter to the ranking members of the Congressional committees charged with overseeing Secure Flight stated that the TSA failed to "fully disclose to the public its use of personal information in its fall 2004 privacy notices as required by the Privacy Act." The letter noted that a TSA contractor specifically "collected more than 100 million commercial data records containing personal information such as name, date of birth, and telephone number without informing the public. As a result of TSA's actions, the public did not receive the full protections of the Privacy Act."[35]

Contrary to the assertion made in its September 2004 statement in the Federal Register, the TSA had "collected and stored commercial data records."[36] "While TSA offered airline passengers who flew during June 2004 an opportunity to access or request to amend their PNR data, they did not make a similar provision for individuals represented

[29] RAND Corporation Secure Flight SFWG Analysis, prepared for the Transportation Security Administration. April, 2005; p. 1.
[30] Ibid.
[31] *The Federal Register,* Department of Homeland Security Transportation Security Administration. "Privacy Act of 1974; System of Records; Secure Flight Test Records." Docket No. TSA-2004-19160. Vol. 69, No. 185. September 24, 2004; 57346.
[32] Ibid.
[33] Ibid.
[34] Ibid.
[35] Government Accountability Office Letter to Congressional Committees. "Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public." GAO-05-864R. July 22, 2005; p. 2.
[36] Ibid., p. 4

in the commercial data that was collected," stated the GAO letter. "As a result, an unknown number of individuals whose personal information was collected were not notified as to how they might access or amend their personal data."[37]

This incident, which took place in spite of ongoing GAO review of privacy practices in Secure Flight testing, raises concerns about TSA's level of preparedness to provide appropriate protections for the records of millions of American travelers that TSA will collect when the program becomes operational.

[37] Ibid. p. 11.

VIII. Passenger Screening – Additional Background

Secure Flight is the successor to the controversial CAPPS II program which sought to engage in data mining of commercial records to identify travelers who posed a threat to aviation security. The color-coded labels (red, yellow, green) that would identify travelers by the level of risk they represented became a matter of great controversy.

Another source of controversy with privacy groups involved data transfers from airlines to the TSA to test the CAPPS II system. A DHS OIG report issued in March 2005 found that the TSA had been involved in 14 transfers of data involving more than 20 million records of air passengers during 2002 and 2003 during the development of CAPPS II. Representatives of the agency made false statements to the news media and delivered false testimony before Congress about TSA's involvement with data transfers. The report found, however, that no federal law had been violated. Because records of individuals were not specifically searched there was no violation of the Privacy Act.[38]

The Inspector General noted that as of March 2005, TSA "has evolved with respect to its approach to privacy" and that its "transition" was still underway. He recommended that clear procedures be developed in the handling of data and that specific individuals be vested with authority for oversight of the data collected and how it is used. This recommendation takes on greater importance in that one of the conclusions reached by the report about TSA's misstatements concerning its policies and actions in regard to the acquisition of data stemmed from "management changes" that resulted in significant changes in staff. The recommendation has specific relevance for Secure Flight because it is expected to be shifted from the TSA to a new branch within DHS called the Screening Coordination and Operations office.[39]

The current air security system, called CAPPS, has been in effect for seven years. Originally it was operated by the Federal Aviation Administration (FAA). CAPPS segregates passengers into two categories based on whether or not they require additional screening because their information is similar to those of suspected or known terrorists in the government's terrorist databases. Also, certain behavioral characteristics could trigger a passenger for extra scrutiny.[40] A significant problem with the current CAPPS program is that it gives the airlines access to the terrorist watch list.[41]

The National Commission on Terrorist Attacks Upon the United States (popularly known as the 9/11 Commission) issued a report in the summer of 2004 which assessed the vulnerabilities in immigration policy, intelligence and transportation security that enabled the 9/11 terrorists to succeed in their deadly missions. Its executive summary noted that two of the 9/11 hijackers were included in a terrorist watch list called TIPOFF but the FAA did not check their names against that database. "The hijackers had to beat only

[38] Source: Singel, Ryan. "TSA Work Sloppy, but Not Illegal" Wired News.com; March 26, 2005 http://www.wired.com/news/print/0,1294,67031,00.html

[39] Department of Homeland Security, Office of the Inspector General. "Review of the Transportation Security Administration's Role in the Use and Dissemination of Airline Passenger Data." OIG – 05-12, March 2005; pp. 51, 48. Also: Goo, Sara Kehaulani. "Proposed Budget would Strip TSA of Its Biggest Programs" The Washington Post. February 9, 2005; p. 6.

[40] Government Accountability Office. "Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges." GAO-04-385. February 2004; pp. 5-6.

[41] Ortiz, David, Shari Lawrence Pfleeger, Aruna D. Balakrishanan, Gordon D. Bitko, and Martin C. Libicki. "Secure Flight SFWG Analysis." Draft Project Memorandum. PM-1805-TSA. April 2005; p. 4.

one layer of security – the security checkpoint process. Even though several hijackers were selected for extra screening by the CAPPS system, this led only to greater scrutiny of their checked baggage," the Commission reported.[42]

CAPPS II was authorized by The Aviation and Transportation Security Act which called for the implementation of a computer prescreening system for passengers and which also created the TSA.[43] The TSA's ability to implement the CAPPS II program was questioned in a report issued by the Government Accounting Office in February 2004 called "Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges." CAPPS II called for combining PNR data with checks of government databases on terrorists and information from commercial databases to determine each passenger's color-coded risk rating. The report found that the development of CAPPS II was running well behind schedule:

> *"As of January 1, 2004, TSA has not fully addressed seven of the eight CAPPS II issues identified by the Congress as key areas of interest, due in part to the early stage of the system's development. These issues relate to: (1) the effective management and monitoring of the system's development and operation and (2) the public's acceptance of the system through the protection of passengers' privacy and enabling passengers to seek redress when errors occur. The DHS has addressed one of the eight issues by establishing an internal oversight board to review the development of major DHS systems, including CAPPS II. DHS and TSA are taking steps to address the remaining seven issues…"*[44]

Most notable from the privacy standpoint was the failure of the TSA to determine which databases they would use to establish the accuracy of the information they contained. TSA also failed to account for the privacy issues raised by its passenger screening system and did not establish and document an effective redress system for passengers who believed they were wrongly singled out for extra screening and perhaps not even allowed to board.[45] The report cast severe doubt as to whether CAPPS II would meet its promise: "Uncertainties surrounding the system's future functionality and schedule alone result in the potential that the system may not meet expected requirements, may experience delayed deployment, and may incur increased costs throughout the system's development."[46] It was announced in late August 2004 that two congressmen had a difficult time boarding flights because their names matched those on the watch lists.[47]

The 9/11 Commission Report called for a "layered security system" and specifically expressed concern that the airlines implemented the CAPPS program relying on the government watch lists in their possession. This led to the excising of names of suspected and known terrorists in fear that the information could be passed on to unfriendly sources. The Commission urged the TSA's plans to take over the checking of the watch lists not be delayed. The report recommended that there be no delay in the

[42] Final Report of the National Commission on Terrorist Attacks upon the United States. "Executive Summary"; p. 10-11**. http://www.9-11commission.gov/report/911Report_Exec.htm**
[43] Government Accounting Office "Aviation Security: Computer-Assisted Passenger Prescreening System," GAO 04-385, February 2004, p. 6.
[44] Ibid. p.4.
[45] Ibid.
[46] Ibid., p. 31.
[47] Goo, Sara Kehaulani and Robert O'Harrow, Jr. "TSA Readies Revised Aviation Screening." The Washington Post, August 26, 2004.

use of improved “No-Fly” and “Automatic Selectee” lists as the debate continued over the fate of the next passenger screening program and that it should be the TSA that performed the screening using expanded watch lists. “Air carriers should be required to supply the information needed to test and implement this new system,” the report stated.[48]

The TSA announced in late August 2004 that CAPPS II would be replaced by Secure Flight. Former TSA Administrator David M. Stone told the House Aviation Subcommittee that the agency was moving toward a “next-generation passenger screening program” that would meet the “goals of using the expanded No-Fly and Selectee lists to keep known or suspected terrorists off of planes, moving passengers through airport security screening more quickly, and reducing the number of individuals unnecessarily selected for secondary screening, all the while fully protecting passengers’ privacy and civil liberties.”[49]

A Privacy Impact Notice for the Secure Flight Test Phase was issued in the September 24, 2004, volume of the *Federal Register*. The statement promised that in its test phase the TSA would not only seek to compare passenger information with the information supplied by the TSC but also to assess how accurate commercial data is in ascertaining incorrect or inaccurate passenger information. The statement also said that before Secure Flight became operational, the TSA would develop a comprehensive passenger redress system and would ensure the privacy and civil liberties of passengers were protected.[50]

In the government’s own analysis of its progress to date, Secure Flight has not scored well. Not only did the OIG issue a report related to the Secure Flight program but the GAO followed suit in late March with a report titled “Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System is Further Developed.” The GAO report examined ten areas where Congress had expressed interest and determined that only one area – the establishment of an internal oversight board – had so far been addressed. Nine areas including the testing of the system to determine its “efficacy and accuracy,” “addressing all privacy concerns” and the redress process had only started to be addressed.[51] The report noted that the TSA had claimed several exemptions from the Privacy Act but had failed to inform the public as to why the exceptions were being sought.[52]

The GAO report said that on March 14, 2005, the TSA announced it would not claim Privacy Act exemptions, absolving itself of the need to issue a rule. However it would issue a “revised system of records notice.” After the data processing testing of Secure Flight concluded and analysis of the results was complete the TSA expected to “issue a Privacy Act exemption rule for the operational phase of the program that would

[48] Final Report of the National Commission on Terrorist Attacks upon the United States; p. 392-394.

[49] Stone, David M. “Testimony of David M. Stone, Assistant Secretary of Homeland Security, Before the Subcommittee on Aviation, Committee on Transportation and Infrastructure, United States House of Representatives, On 9/11 Recommendations on Civil Aviation Security. August 25, 2004. PDF File. p. 6. **http://www.house.gov/transportation/aviation/08-25-04/stone.pdf**

[50] Department of Homeland Security, “Privacy Act of 1974: System of Records; Secure Flight Test Records. Docket No. TSA-2004-19160, The Federal Register Vol. 69, No. 185; pp. 57345-7.

[51] Government Accountability Office, “Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System is Further Developed.” GAO—05-356. March 2005; p. 4.

[52] Ibid., pp. 54-55.

implement any exemptions claimed and explain the agency's basis for claiming such exemptions." The draft rules were expected to be issued in March 2005 for review by the OMB and the final rules and "privacy package" were expected in June 2005. The report stated, "A determination of whether Secure Flight will be in compliance with the Privacy Act cannot be made until such notices are issued."[53]

A July 22, 2005, memorandum by GAO, sent to the ranking members of the relevant Congressional committees charged with oversight of Secure Flight stated that, in the course of "ongoing review," the agency discovered, "TSA did not fully disclose to the public its use of personal information in its fall 2004 privacy notices as required by the Privacy Act."[54] TSA had filed notices in the *Federal Register* in the fall of 2004 announcing how the information it intended to collect would be used. The actual use of the data by the contractors was quite different from what had been described. The GAO said, "Specifically, TSA's contractors used PNR data supplemented with commercial data to determine if commercial data could be effective in eliminating incorrect matches against the government's consolidated terrorist watch lists."[55] The public was not informed that a TSA contractor obtained over 100 million commercial data records.[56]

The GAO faulted the TSA for failing to inform the public of:

- Who had their data collected;
- What type of data was included;
- Reason for collecting the data;
- How the data was to be stored and maintained; and
- How people whose data had been collected could access and correct their data.[57]

After GAO pointed out the failures of TSA to clearly identify its policies regarding commercial data, the agency revised its notices.[58] The TSA has also said it plans to develop and to implement better procedures that would require the TSA Privacy Officer and the TSA Counsel to determine if changes in testing policies would require revising the System of Records Notice (SORN) or privacy impact assessment of the Secure Flight system.

Two findings of the 9/11 Commission are worth noting in relation to Secure Flight. The United States has prided itself on its avoidance of becoming a "checkpoint" society in the manner of Eastern Europe where the movements and activities of citizens were closely monitored by the national government. The Commission called for the protection of "privacy rights" but the issues confronted in screening air passengers – for matches on the watch list and luggage – could very well be employed in other modes of transportation and by other government agencies.

Given the changes to be made in driver's licenses under the Real ID Act, as well as to other sources of identification, the likelihood is that more and more American citizens will

[53] GAO; "Secure Flight;" p. 55.
[54] GAO; "Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public." GAO-05-864R Aviation Security, July 22, 2005 p.1.
[55] Ibid., p. 5.
[56] Ibid., p. 2.
[57] Ibid., p. 6.
[58] Ibid., p. 8.

have their movements scrutinized by the federal government as they travel. According to The Final Report of the National Commission on Terrorist Attacks upon the United States, the TSA is grappling with screening issues including profiling passengers "encountered by other agencies" and that if the TSA could resolve some of the problems associated with screening they could help other agencies too. At the same time, the 9/11 Commission noted that the overwhelming majority of the TSA budget is devoted to aviation, money which is being used to "fight the last war."[59]

The Commission noted there are also glaring security vulnerabilities in other modes of transportation including railroads and mass transportation. The former could include passengers and the latter most certainly does and there is concern in the privacy community that the enhanced screening system of Secure Flight could be transferred to surface transportation too.[60] The 9/11 Commission report states, "While commercial aviation remains a possible target, terrorists may turn their attention to other modes. Opportunities to do harm are as great, or greater, in maritime or surface transportation. Initiatives to secure shipping containers have just begun. Surface transportation systems such as railroads and mass transit remain hard to protect because they are so accessible and extensive."[61]

Testifying before a Congressional subcommittee, Deputy TSA Administrator Stephen McHale stated that the TSA had plans to implement a pilot program to screen rail passengers at the New Carrollton, Maryland, rail station but no mention was made of matching passengers against a watch list.[62] While the kind of passenger screening associated with Secure Flight has yet to take hold in rail or interstate highway transportation, could it? The Electronic Frontier Foundation expressed concern about "mission creep" with CAPPS II, asking "how many other modes of travel will eventually fall under the CAPPS II purview?"[63]

After the London bombings in July 2005, Michael Chertoff, Secretary of Homeland Security, suggested that this might be an unlikely prospect, at least for the duration of his tenure. Chertoff said, "The truth of the matter is, a fully loaded airplane with jet fuel, a commercial airliner, has the capacity to kill 3,000 people. A bomb in a subway car may kill 30 people. When you start to think about your priorities…you're going to think about making sure you don't have a catastrophic thing first."

[59] Final Report of the National Commission on Terrorist Attacks upon the United States, p. 393

[60] Ibid., pp. 391-393.

[61] Ibid., p. 391.

[62] See: McHale, Stephen M. "Statement of Stephen McHale, Deputy Administrator, TSA on Transportation Security before the Subcommittee on Infrastructure and Border Security, Select Committee on Homeland Security" May 12, 2004, p. 4. http://www.tsa.gov/public/display?content=09000519800a612f

[63] See: Electronic Frontier Foundation. "CAPPS II: Government Surveillance and Passenger Profiling." http://www.eff.org?Privacy/cappsii/background.php

IX. Passenger Name Record

The GAO's March 2005 report, "Aviation Security: Secure Flight Development and Testing Under Way but Risks Should Be Managed as System Is Further Developed," released when the initial Secure flight PNR test results were still being scrutinized, stated that the TSA officials asserted their findings indicated that Secure Flight would be better than the current system at singling out terrorists by matching PNR data with the names contained on the terrorist watch lists. "TSA officials further stated that test results indicate that adding date of birth to PNR data may further reduce the number of false positives."[64]

The GAO noted that it had been unable to verify the accuracy of the claims made by TSA. It also said that TSA had yet to determine what specific "data elements" needed to be collected from passenger data and what information would be required from the terrorist databases. The GAO observed that the information required as part of the PNR data could require an upgrading of airline reservation systems and their own survey of air carriers revealed a great deal of uncertainty within the airline industry about what changes implementation of Secure Flight would require them to make.

There was concern about the process of transferring the PNR data from the airlines to TSA. The GAO report states that the change necessary to meet Secure Flight requirements to collect PNR data could place a "significant strain on the industry."[65] The GAO also noted that plans to use commercial data to verify PNR data are clouded by uncertainty about the accuracy of commercial data. "If the data in commercial databases are determined to have an unacceptable level of accuracy to support Secure Flight operations, the usefulness of commercial data in augmenting data contained in PNRs may be limited."[66] Questions were also raised about the ability to easily facilitate the transfer of information between the carriers who collect the PNR data and the TSA.[67]

The GAO report, in its conclusion, made clear its difficulty in assessing whether Secure Flight would indeed live up to the Privacy Act requirement that data on an individual be relevant to the agency's purpose. TSA had indicated to the GAO that they needed to ascertain whether data elements such as date of birth would be needed to check against the data in the TSCD. The report said, "Until TSA determines which data elements will be required for Secure Flight operations, based on the results of these tests, whether TSA is collecting only relevant and necessary personal information cannot be determined."

[64] Government Accountability Office. "Aviation Security: Secure Flight Development and Testing Under Way but Risks Should Be Managed as System Is Further Developed." GAO-05-356. March 2005; p. 28
[65] Ibid, pp. 29-30; 46.
[66] Ibid., p. 32.
[67] Ibid., p. 47.

X. Push versus Pull Model for Passenger Data

TSA must decide either to have airlines "push" passenger data to the Secure Flight passenger-matching system or for TSA to "pull" data from the airline reservation systems.[68] Pulling the data raises questions of government access to the airlines' information systems and necessitates segregating PNR information so that only the specific data elements Secure Flight requires for name matching are pulled.

If Secure Flight uses a "push" model:

- The airlines maintain control over their passenger data and minimize data duplication; but
- The airlines must assume the cost of building and maintaining an application capable of selecting, formatting and transmitting the data, and of providing a network that can transmit the volume of data at the required speed.

If Secure Flight uses a "pull" model:

- Airlines will collect new data elements from passengers that are not included in the current PNR (including full name and date of birth); this may require reformatting of the PNR system at a cost to the airlines;
- TSA extracts only the data Secure Flight will use for passenger matching from the various data points provided by different PNR systems; but
- TSA bears the information-processing burden of receiving data in different formats and with different data fields; and
- Once the capability is built for TSA to reach into airline databases, it could more readily extract additional elements, making "mission creep" easier.

TSA stated that, as of the spring of 2005 (which may mean only prior to deciding whether to use a push or pull model), it did not expect the airlines to change their PNR databases to accommodate Secure Flight. TSA clearly reserves the option to do so and it is also implicit that this will have to be done if the system is to operate efficiently. Once the push or pull decision is made, TSA offers three options to the airlines for dealing with nonconforming formats:

1. It may require the airlines to provide passenger data to the government in a uniform format.
2. It may require airlines to transmit PNR data to a commercially developed filtering and formatting program that converts the data to a uniform format.
3. It may require airlines to transmit PNR data to a TSA-developed filtering and formatting program that converts the data to a uniform format.

All three approaches will require airlines to collect new data elements (full name and date of birth) not traditionally included in PNRs.

Push/Pull Conclusions

[68] The information the SFWG has been given about PNRs used in testing concerns only those records made by and received from individual airlines. A passenger screening system, however, whether it is Secure Flight or any successor, must also have access to PNRs from the computerized reservation systems (CRS), such as Galileo and Cendant. As far as the SFWG has been informed, TSA has done no testing of PNRs from any CRS.

Transfer to the government of passenger information is one of the fundamental elements of the Secure Flight system, but so far the method for accomplishing it has not been defined and sufficiently tested in a real environment. Instead, Secure Flight data have been tested under artificial (laboratory) conditions, with PNRs handed over to TSA on tape and only the most usable ones selected for testing.

Even this controlled test demonstrated that PNRs, as currently configured by the airlines, are not suitable for watch list matching. They do not have the right information (full name and date of birth) and they contain considerable extraneous data. Secure Flight requires the continuous transfer of large amounts of data, based on the standard estimate of passenger traffic as 1.8 million people per day. As far as the SFWG has been informed, no tests have been done to determine what application(s) or bandwidth would be necessary to operate with either a push or pull model, or what would be required to achieve format compatibility among the different types of PNRs and to filter unnecessary data at the likely volume of passenger traffic.

The GAO's March 23, 2005, report, "Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed,"[69] concludes that TSA has not yet resolved how passenger data would be transmitted from airlines to the TSA. Based on the GAO report and information given (or not given) to the SFWG, major questions about Secure Flight's underlying data transfer processes remain to be answered:

1. The cost of implementing either the push or pull method is unknown. According to the GAO, the cost of transferring PNR data was a key element that was not accounted for in CAPPS II[70] and, as far as the SFWG has been informed, has still not been accounted for with respect to Secure Flight.

2. Whether the system is push or pull, the SFWG has no information about a security plan to reduce opportunities for abuse of the passenger data transfer system or to explain how it will be protected from unauthorized access. Since the flow of data will be large and continuous, this is a crucial omission.

3. The SFWG has no information concerning oversight of the data transfer system. Given what has been publicly reported about TSA's mishandling of data in Secure Flight tests contrary to its published notices[71] (i.e., generating 200,000 variables on 43,000 names obtained from PNRs and comparing them against 100 million records obtained from commercial data brokers), it is a matter of concern that TSA could abuse its "pull" access to airline passenger records and cull information for additional or extraneous purposes. TSA Assistant Administrator Justin Oberman's June 2005 testimony to the Economic Security, Infrastructure Protection, and Cybersecurity Subcommittee of the House Homeland Security Committee does little to alleviate this concern. He states that Secure Flight "ought to be able to identify people who may

[69] http://www.gao.gov/highlights/d05356high.pdf

[70] "Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges," GAO, GAO 04-385, February. 2004; http://www.gao.gov/highlights/d04385high.pdf

[71] GAO, "Transportation Security Administration Did Not Fully Disclose Uses of Personal Information During Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public," GAO 05-864R, July 22, 2005; http://www.gao.gov/new.items/d05864r.pdf

not be on the watch list."[72] This represents a return to the behavioral profiling aspect of CAPPS II, which requires a great deal more information from the airlines than full name and date of birth, along with unknown quantities of information from commercial sources.

4. The SFWG was never given any information about whether TSA would obtain commercial data by a push or pull method. Media reports about commercial data testing described above, however, indicate that TSA gave or "pushed" its 243,000 original and enhanced PNRs to one contractor, which supplemented them with 100 million records from commercial data brokers.[73]

[72] http://www6.lexisnexis.com/publisher/EndUser?...

[73] "More Privacy Questions for Air Safety Agency," Eric Lipton, New York Times, June 16, 2005; http://www.nytimes.com/2005/06/16/national/16privacy.html. Note that TSA also retained the results of this PNR amplification on CDs given to it by Eagle Force, although it denied having them in a FOIA request made by four June 2004 Alaska Airlines passengers. (See http://www.alaskafreedom.com/home.html?ak=n for information about this FOIA request and the legal complaint filed to obtain the records TSA denies having).

XI. Data Retention Issues

TSA plans to collect passenger data 72 hours *before* the departure time of an outgoing flight, and will retain the data for 72 hours after the travel itinerary is completed, in case any passenger seeks redress.

Seventy-two hours before flight time is believed to be the point at which the majority of airline itineraries are final, and therefore an appropriate time to start batch-processing passenger data and begin the vetting process. No evidence was presented to the SFWG in support of retaining data for 72 hours versus 48 versus 24. Although, one can speculate that 72 hours might be needed for human intervention to resolve possible matches. Last minute itinerary changes and, presumably, last minute ticket purchases, will be processed in real time. Thus, at the outset, TSA will retain passenger data for a minimum of six days, and an unknown maximum number of days, weeks or months, depending on when a passenger completes his or her itinerary. In addition to the 72-hour post-completion of itinerary retention period that TSA calls for, there is also a provision to increase retention by another 10 days.[74]

Certain data retention issues were undecided at the time the information was presented to the SFWG. TSA did not know how it would handle the return leg of a passenger's itinerary. That is, whether it would retain a passenger's entire PNR until the itinerary is completed, which could be months or whether it would re-run the PNR and re-vet the passenger for the return leg.[75]

One goal of Secure Flight that affects data retention is to reduce the cost of operating the system by collecting data from the airlines only once. Retaining a PNR until the itinerary is completed could keep cost down, but does not solve the problem of watch lists changing in the meantime. A passenger with an extended itinerary would need to be checked again at some point, but at what point? Another factor that TSA has not accounted for is itineraries that are not round-trip, or that include more than just two flights. When does such an itinerary end, for data retention purposes?

TSA contends that it must retain data until 72 hours after the completion of any itinerary for redress purposes, including redress that arises from random selection. At the most, however, TSA would need to retain data only for "yellow" and "red" passengers (i.e., those who match a name on a watch list), because randomly searched passengers would, by definition, be those for whom no match existed, and who were, therefore, "cleared" as far as Secure Flight was concerned.

Another possible reason given for retention was the potential need to investigate false negatives. The idea is that if the system does not identify a terrorist or threat to aviation security, an investigation will be conducted to determine why not. TSA would need the data on the cleared passengers for such an investigation.[76] This argument, however, would justify retaining data only until the successful completion of each flight. Other backward-looking investigations could be accomplished with the airlines' archived PNRs

[74] Secure Flight, SFWG transcript, 2005b, p. 126.
[75] Secure Flight, SFWG transcript, 2005a, p. 250-251).
[76] Secure Flight, SFWG transcript, 2005b, p. 123-124).

In comparison to Secure Flight, Australia has implemented a passenger screening system that does not retain data after flight completion. In response to the public's privacy concerns expressed by the Australian Federal Privacy Commissioner, the Australian Customs Department, which has responsibility for passenger screening, stated: "Customs does not retain or store any passenger information unless the passenger has been identified undertaking an illegal activity or the information is needed as intelligence to assist in investigation of a suspected offense."[77]

Leaving aside the vagueness of what an "illegal activity" or "suspected offense" might be the Australians evidently do not find it necessary to retain PNR data for redress purposes. And even a 72-hour retention period is not very useful for a passenger subjected to multiple secondary screenings.

In any case, redress will require more information than is in the PNR or airline-supplied passenger list. A passenger seeking redress will be required to show multiple proofs of identification, which will all most likely include name, date of birth and a good deal more – in other words, all the information that would be in the passenger data supplied by the airlines anyway, plus additional data elements not in the PNR, to check against the watch lists and deal with the complaint. There does not seem to be any justification for retaining all PNRs until a passenger's itinerary is completed.

Overall, the SFWG is concerned about building a system designed to retain data, because of the inevitable issue of function creep. As long as the data is there, other uses will be found for it. Secondary uses of passenger data represent a potential cause of harm to the public.

[77] Article 29 Data Protection Working Party, "Opinion 1/2004 on the level of protection ensured in Australia for the transfer of Passenger Name Record data from airlines," 10031/03/EN WP 85; http://www.statewatch.org/news/2004/feb/WG29-Australie.pdf.

XII. Conclusion

We, the SFWG were not provided adequate information about the proposed program for Secure Flight. Therefore, we are unable to make any substantive recommendations at this time. We do, however, suggest the following actions:

Congress should prohibit live testing of Secure Flight until it receives the following from the Secretary of the Department of Homeland Security.

First, a written statement of the goals of Secure Flight signed by the Secretary of DHS that only can be changed on the Secretary's order. Accompanying documentation 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 an assurance that someone has been appointed with sufficient independence and power to ensure that the system development and subsequent use follow the documented procedures.

In conclusion, we believe live testing of Secure Flight should not commence until there has been adequate time to review, comment, and conduct a public debate on the additional documentation outlined above.

Respectfully,

Secure Flight Working Group

<u>List of Members</u>

- ✓ Martin Abrams
- ✓ Linda Ackerman
- ✓ James Dempsey
- ✓ Edward Felten
- ✓ Daniel Gallington
- ✓ Lauren Gelman
- ✓ Steven Lilienthal
- ✓ Bruce Schneier
- ✓ Anna Slomovic