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

> Recommendations on the Secure Flight Program, Adopted December 6, 2005. The Data Privacy and Integrity Advisory Committee (the Committee) has examined the Secure Flight Program and issues this report to the Secretary and the Chief Privacy Officer of the Department of Homeland Security (DHS).

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

REPORT OF THE DEPARTMENT OF HOMELAND SECURITY
DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE
Report No. 2005-02

RECOMMENDATIONS ON THE SECURE FLIGHT PROGRAM

Adopted 12-6-2005

INTRODUCTION

The Data Privacy and Integrity Advisory Committee (the Committee) has examined the Secure Flight Program and issues this report to the Secretary and the Chief Privacy Officer of the Department of Homeland Security (DHS).

The Secure Flight program is intended to screen passengers boarding domestic flights. Crucial data for Secure Flight are the No-Fly and Selectee lists maintained by the Terrorist Screening Center (TSC). Names are submitted by nominating agencies and reviewed by TSC for consistency with the underlying criteria. Although members of the committee have examined the criteria and the process for maintaining these lists, we have evaluated Secure Flight as a means of identifying people on those lists rather than evaluating the lists themselves.

Because the program is not yet fully defined, we have not attempted to describe in detail how it should operate to address privacy concerns. However, based on our review of numerous program documents, including the results of the test program, and after numerous discussions with the program staff at the Transportation Security Administration (TSA), the Committee has concluded that several key principles should frame further decisions concerning the development of the program.

RECOMMENDATIONS

1. Secure Flight should be transparent.

The purpose and details of the program should be transparent to two key groups: the public and the airlines. For the public, it is vital for TSA to identify with specificity exactly what Secure Flight does. Recognizing that security concerns limit the disclosure of some operational details, TSA should specify what information Secure Flight will use and how it will handle that information. Ambiguity will only feed fears of unwarranted invasions of privacy. For the airlines, TSA should be clear about what information it needs now and what information it may consider in the future, to enable airlines to avoid sequential revisions of data handling systems. As discussed in recommendation three, below, TSA should only collect information that it can document is necessary to support the Secure Flight mission.

2. Secure Flight should be narrowly focused.

TSA should limit Secure Flight's mission to correctly identifying individuals in the traveling public who are on the Do Not Fly and Selectee lists. The case has not been made for any expansion of the mission of Secure Flight beyond identification of individuals on those lists.

3. Secure Flight should minimize data collection.

Secure Flight should limit its data collection to the information necessary to fulfill its mission. It should use and retain only this information even if airlines provide additional information from existing records. At present, there is a solid case for collecting only full name and date of birth, the information available for most names on the watch list. When passport number is available as part of the passenger name record because, for example, the domestic flight connects with an international flight, that information may also be useful. Secure Flight should not request airlines to ask purely domestic passengers for passport numbers and should not seek to obtain that information from, for example, airline frequent flier records.

The testing performed to date does not provide a reasonable case for utilizing commercial data as part of Secure Flight. If TSA considers using commercial data in the future, it should consider the Committee's previous recommendations on the use of commercial data to reduce false positives.

4. Secure Flight must provide proactive redress.

A key Secure Flight objective must be to provide effective redress mechanisms for those who have been wrongly delayed or prohibited from boarding a flight. The determination and any resulting corrections must be made in a timely manner and corrections must be rapidly disseminated throughout the Secure Flight system (and any other systems that are used to populate the watch lists). Recognizing that a credentialing process for clearing such individuals can pose security risks, the goal should nevertheless be to avoid, or at least minimize, repeated delays or other adverse consequences to individuals who have been cleared.

5. Secure Flight must be understood and managed holistically.

Interdependency and complexity may increase program risk as well as the complexity of risk mitigation. In light of the complexity and interdependency of Secure Flight, documentation of the various system components is necessary, as is documentation that addresses system-wide risk issues. To help ensure that program and oversight officials fully understand these issues, there must be an overall system description that addresses all aspects of the Secure Flight system including external supporting systems, policies, applications and infrastructures, as well as related business processes managed by entities external to the Secure Flight program office.

Documentation for the operational phase of Secure Flight should describe and assess the system as a whole, including the airline-managed systems, and how all the parts work together. This overall system description is needed and must be reviewed prior to using live data.

Secure Flight makes extensive use of existing DHS and private sector infrastructure and systems (including those operated by airlines) that are outside the management purview of the Secure Flight program office. Consequently, we believe that the Secure Flight operational system must include a security and privacy risk assessment, security plan, documented security and privacy controls, and appropriate certification and accreditation documentation for the group of interconnected systems supporting the secure Flight program. Documentation available from DHS, government and private sector entities for specific components can be used for this purpose, but it must demonstrate how key elements are being addressed, rather than simply assuming that they are addressed.

Finally, the total system should be audited routinely by the DHS Privacy Office.