

**DEPARTMENT OF HOMELAND SECURITY****Transportation Security Administration****49 CFR Parts 1540, 1544, and 1560**

[Docket No. TSA-2007-28572; Amendment Nos. 1540-9, 1544-8, and 1560-(New)]

RIN 1652-AA45

**Secure Flight Program****AGENCY:** Transportation Security Administration, DHS.**ACTION:** Final rule.

**SUMMARY:** The Intelligence Reform and Terrorism Prevention Act 2004 (IRTPA) requires the Department of Homeland Security (DHS) to assume from aircraft operators the function of conducting pre-flight comparisons of airline passenger information to Federal government watch lists for domestic flights and international flights to, from, and overflying the United States. The Transportation Security Administration (TSA) is issuing this final rule to implement that congressional mandate.

This final rule allows TSA to begin implementation of the Secure Flight program, under which TSA will receive passenger and certain non-traveler information, conduct watch list matching against the No Fly and Selectee portions of the Federal government's consolidated terrorist watch list, and transmit a boarding pass printing result back to aircraft operators. TSA will do so in a consistent and accurate manner while minimizing false matches and protecting personally identifiable information.

On August 23, 2007, U.S. Customs and Border Protection (CBP) published a final rule to implement pre-departure advance passenger and crew manifest requirements for international flights and voyages departing from or arriving in the United States using CBP's Advance Passenger Information System (APIS). These rules are related. After the compliance date of this Secure Flight final rule, aircraft operators will submit passenger information to DHS through a single DHS portal for both the Secure Flight and APIS programs. This will allow DHS to integrate the watch list matching component of APIS into Secure Flight, resulting in one DHS system responsible for watch list matching for aviation passengers.

**DATES:** Effective December 29, 2008.

**FOR FURTHER INFORMATION CONTACT:** Kevin Knott, Policy Manager, Secure Flight, Office of Transportation Threat Assessment and Credentialing, TSA-19, Transportation Security Administration,

601 South 12th Street, Arlington, VA 22202-4220, telephone (240) 568-5611.

**SUPPLEMENTARY INFORMATION:****Availability of Rulemaking Documents**

You can get an electronic copy using the Internet by—

(1) Searching the electronic Federal Docket Management System (FDMS) Web page at <http://www.regulations.gov>;

(2) Accessing the Government Printing Office's Web page at <http://www.gpoaccess.gov/fr/index.html>; or

(3) Visiting TSA's Security Regulations Web page at <http://www.tsa.gov> and accessing the link for "Research Center" at the top of the page.

In addition, copies are available by writing or calling the individual in the **FOR FURTHER INFORMATION CONTACT** section. Be sure to identify the docket number of this rulemaking.

**Small Entity Inquiries**

The Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996 requires TSA to comply with small entity requests for information and advice about compliance with statutes and regulations within TSA's jurisdiction. Any small entity that has a question regarding this document may contact the person listed in **FOR FURTHER INFORMATION CONTACT**. Persons can obtain further information regarding SBREFA on the Small Business Administration's Web page at [http://www.sba.gov/advo/laws/law\\_lib.html](http://www.sba.gov/advo/laws/law_lib.html).

**Abbreviations and Terms Used in This Preamble**

APIS—Advance Passenger Information System  
 ATSA—Aviation and Transportation Security Act of 2001  
 AOIP—Aircraft Operator Implementation Plan  
 CBP—U.S. Customs and Border Protection  
 DHS—Department of Homeland Security  
 2006 DHS Appropriations Act—Department of Homeland Security Appropriations Act, 2006  
 2007 DHS Appropriations Act—Department of Homeland Security Appropriations Act, 2007  
 DHS TRIP—Department of Homeland Security Traveler Redress Inquiry Program  
 FBI—Federal Bureau of Investigation  
 FISMA—Federal Information Security Management Act  
 GAO—Government Accountability Office  
 HSPD—Homeland Security Presidential Directive  
 IASTA—International Air Services Transit Agreement  
 IATA—International Air Transport Association  
 IRTPA—Intelligence Reform and Terrorism Prevention Act of 2004

NARA—National Archives and Records Administration  
 PNR—Passenger Name Record  
 PRI—Passenger Resolution Information  
 PIA—Privacy Impact Assessment  
 SFPD—Secure Flight Passenger Data  
 SSI—Sensitive Security Information  
 SORN—System of Records Notice  
 TSA—Transportation Security Administration  
 TSC—Terrorist Screening Center  
 TSDB—Terrorist Screening Database  
 VID—Verifying Identity Document

**Outline of Final Rule**

- I. Background
- II. Secure Flight Program Summary
  - A. Differences Between the Proposed Rule and the Final Rule
  - B. Secure Flight Passenger Data
  - C. 72-Hour Requirement
  - D. Instructions to Covered Aircraft Operators
  - E. Summary of Requirements
  - F. Implementation Phases of Secure Flight
    1. Implementation of Secure Flight for Domestic Flights
    2. Implementation of Secure Flight for Overflights and International Flights
  - G. Privacy Documents
  - H. The Watch List Matching Process Under Secure Flight
    - I. Operational Testing of Secure Flight
- III. Response to Comments
  - A. Scope of the Rulemaking
    1. Overflights and Foreign Air Carriers
    2. Include Other Aircraft Operators in Secure Flight Program
  - B. Coordination with CBP and Other Government Agencies
  - C. Implementation and Compliance
  - D. Secure Flight Passenger Data (SFPD)
    1. General
    2. SFPD Is Not Passenger Name Record (PNR)
    3. Date of Birth and Gender
    4. Redress Number and Known Traveler Number
  - E. Watch List Matching Process
    1. Transmission of SFPD
    2. 72-Hour Requirement
    3. Boarding Pass Issuance
    4. Passenger Resolution
    5. Use of the Terrorist Screening Database (TSDB)
  6. Non-Traveling Individuals
  7. General Comments
  - F. Privacy
    1. General Comments
    2. Required Privacy Notice
    3. Privacy Impact Assessment (PIA)
    4. Privacy Act Exemptions
    5. System of Records Notice (SORN)
    6. Retention of Data
    7. Sharing of Data with Other Agencies
    8. Collection and Use by Private Entities
  - G. Redress
  - H. Consolidated User Guide/Aircraft Operator Implementation Plan (AOIP)
    - I. Testing
    - J. Identification Requirements
    - K. Economic Comments
    - L. General Comments
    - M. Comments Beyond the Scope of the Rulemaking
- IV. Rulemaking Analyses and Notices

- A. Paperwork Reduction Act
- B. Regulatory Impact Analysis
- 1. Regulatory Evaluation Summary
- 2. E.O. 12866 Assessment
- 3. Final Regulatory Flexibility Analysis (FRFA)
- C. International Trade Impact Assessment
- D. Unfunded Mandates Assessment
- E. Executive Order 13132, Federalism
- F. Environmental Analysis
- G. Energy Impact
- H. International Compatibility

List of Subjects  
The Amendments

## I. Background

TSA performs passenger and baggage screening at the Nation's commercial airports.<sup>1</sup> Covered aircraft operators currently supplement this security screening by performing passenger watch list matching using the Federal No Fly and Selectee portions of the consolidated terrorist watch list maintained by the Federal government, as required under security directives that TSA issued following the terrorist attacks of September 11, 2001. Covered aircraft operators also conduct this watch list matching process for non-traveling individuals authorized to enter the sterile area<sup>2</sup> of an airport within the United States in order to escort a passenger or for some other purpose approved by TSA.

Section 4012(a) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) requires DHS to assume from air carriers the comparison of passenger information to the Selectee and No Fly Lists and to utilize all appropriate records in the consolidated and integrated watch list that the Federal Government maintains.<sup>3</sup> The final report of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission Report) recommends that the watch list matching function "should be performed by TSA and it should utilize

the larger set of watch lists maintained by the Federal government." See 9/11 Commission Report at 393.

Consequently, pursuant to sec. 4012 (a) of the IRTPA, TSA issues this final rule to implement the Secure Flight program. Under the program, TSA will receive passenger and certain non-traveler information from aircraft operators. After conducting watch list matching, TSA will transmit boarding pass printing results based on watch list matching results back to aircraft operators.

## II. Secure Flight Program Summary

This final rule will affect all covered flights operated by U.S. aircraft operators that are required to have a full program under 49 CFR 1544.101(a),<sup>4</sup> and covered flights operated by foreign air carriers that are required to have a security program under 49 CFR 1546.101(a) or (b). These aircraft operators generally are the passenger airlines that offer scheduled and public charter flights from commercial airports. This final rule refers to them as "covered U.S. aircraft operators" and "covered foreign air carriers" respectively, and "covered aircraft operators" collectively.

TSA will assume the watch list matching function from aircraft operators to more effectively and consistently prevent certain known or suspected terrorists from boarding aircraft where they may jeopardize the lives of passengers and others. The Secure Flight program is designed to better focus enhanced passenger screening efforts on individuals likely to pose a threat to civil aviation, and to facilitate the secure and efficient travel of the vast majority of the traveling public by distinguishing them from individuals on the watch list.

In general, the Secure Flight program will compare passenger information only to the No Fly and Selectee List components of the Terrorist Screening Database (TSDB), which contains the Government's consolidated terrorist watch list, maintained by the Terrorist Screening Center (TSC).<sup>5</sup> In general,

comparing passenger information against the No Fly and Selectee components of the TSDB during normal security circumstances will be satisfactory to counter the security threat versus using the entire TSDB. The No Fly and Selectee Lists are based on all the records in the TSDB and the No Fly and Selectee Lists represent the subset of names who meet the criteria of the No Fly and Selectee designations. However, as recommended by the 9/11 Commission and as required under the IRTPA, TSA may use "the larger set of watch lists maintained by the Federal government" when warranted by security considerations. For example, TSA may learn that flights on a particular route may be subject to increased security risk. Under this circumstance, TSA may decide to compare passenger information on some or all of the flights on that route against the full TSDB or other government databases, such as intelligence or law enforcement databases. Thus, TSA defines "watch list" for purposes of the Secure Flight program as the No Fly and Selectee List components of the Terrorist Screening Database maintained by the Terrorist Screening Center. For certain flights, the "watch list" may include the larger set of watch lists maintained by the Federal government as warranted by security considerations.

After the Secure Flight program completes the comparison of passenger information, TSA will return to the covered aircraft operators the boarding pass printing result to allow the aircraft operators to begin the process for issuing boarding passes to passengers. The boarding pass printing result for each passenger will return one of the following instructions to the covered aircraft operator regarding that passenger: (1) The covered aircraft operator may issue an unrestricted boarding pass; (2) the aircraft operator may issue a boarding pass indicating that the passenger has been selected for enhanced screening; (3) or the covered aircraft operator may not issue a boarding pass to the passenger, and the passenger must come to the airport for resolution. If TSA instructs the covered aircraft operator not to issue a boarding pass to a passenger, the covered aircraft operator must comply with procedures in its security program for requesting the passenger to present a verifying identity document when the passenger checks in at the airport. The covered aircraft operator may issue a boarding pass to that passenger only after

<sup>1</sup> See the Aviation and Transportation Security Act (ATSA) (Pub. L. 107-71, 115 Stat. 597, Nov. 19, 2001).

<sup>2</sup> "Non-traveling individual" means as an individual to whom a covered aircraft operator or covered airport operator seeks to issue an authorization to enter the sterile area of an airport in order to escort a minor or a passenger with disabilities or for some other purpose permitted by TSA. It would not include employees or agents of airport or aircraft operators or other individuals whose access to a sterile area is governed by another TSA regulation or security directive. 49 CFR 1540.3.

"Sterile Area" means a portion of airport defined in the airport security program that provides passengers access to boarding aircraft and to which the access generally is controlled by TSA, or by an aircraft operator under part 1544 of this chapter or a foreign air carrier under part 1546 of this chapter, through the screening of persons and property. 49 CFR 1540.5.

<sup>3</sup> Pub. L. 108-458, 118 Stat. 3638, Dec. 17, 2004; 49 U.S.C. 44903(j)(2).

<sup>4</sup> Covered U.S. aircraft operators who also operate flights under other security programs in 49 CFR 1544.101 may submit Secure Flight Passenger Data (SFPD) for their operations to TSA. 49 CFR 1560.101(a)(5).

<sup>5</sup> The TSC was established by the Attorney General in coordination with the Secretary of State, the Secretary of Homeland Security, the Director of the Central Intelligence Agency, the Secretary of the Treasury, and the Secretary of Defense. The Attorney General, acting through the Director of the Federal Bureau of Investigation (FBI), established the TSC pursuant to Homeland Security Presidential Directive 6 (HSPD-6), dated September 16, 2003, which required the Attorney General to establish an organization to consolidate the Federal

government's approach to terrorism screening and provide for the appropriate and lawful use of terrorist information in screening processes.

receiving a boarding pass printing result indicating that the passenger is cleared or has been selected for enhanced screening.

The final rule covers all flights conducted by covered U.S. aircraft operators, as well as all flights conducted by a covered foreign air carrier arriving in or departing from the United States, or overflying the continental United States, defined as the lower contiguous 48 states. The final rule collectively refers to the flights conducted by U.S. carriers and covered international flights that are regulated under this final rule as “covered flights.”

IRTPA also requires DHS to assume from air carriers the task of comparing passenger information for international flights to or from the United States against the Federal government’s consolidated and integrated terrorist watch list before departure of such flights. Initially, CBP will implement this requirement and conduct pre-departure watch list matching for international flights, through the Advance Passenger Information System (APIS). APIS is a widely used electronic data interchange system that

commercial carriers with flights or vessel voyages arriving to or departing from the United States use to transmit electronically to CBP certain data on passengers and crew members. The former U.S. Customs Service, in cooperation with the former Immigration and Naturalization Service (INS) and the airline industry, developed APIS in 1988. On August 23, 2007, CBP published the Advance Electronic Transmission of Passenger and Crew Member Manifests for Commercial Aircraft and Vessels final rule (APIS Pre-Departure final rule) that requires air and vessel carriers to submit to CBP passenger manifest information before departure of a flight to or from the United States and for voyages from the United States to enable the DHS system to conduct watch list matching on passengers before they board an international flight or depart on certain voyages.<sup>6</sup>

In response to a substantial number of comments from the aviation industry, DHS has developed a unified approach to watch list matching for international and domestic passenger flights, to avoid unnecessary duplication of watch list matching efforts and resources and

reduce the burden on aircraft operators. Pursuant to the APIS Pre-Departure final rule, the CBP system currently performs the watch list matching function for international flights to or from the United States as part of its overall screening of travelers. Ultimately, the watch list matching function for covered flights that are international air arrivals and departures will be transferred to TSA through the phased implementation of the Secure Flight rule. TSA will assume the aviation passenger watch list matching function for domestic and international passengers covered by this rule, while CBP will continue to conduct border enforcement functions. To streamline the transmission of passenger information, DHS has established one portal through which aircraft operators will send their passenger information for both programs and receive a printing result.

*A. Differences Between the Proposed Rule and the Final Rule*

Below is a table, which summarizes the difference between the proposed rule text in the Secure Flight NPRM and the rule text in this final rule.

	Secure flight proposed rule	Secure flight final rule
Required Passenger Information in the SFPD (49 CFR 1540.107 and 1560.101).	1. Covered aircraft operators would be required to request individuals’ date of birth and gender to transmit this information, if available, to TSA. 2. Individuals would not be required to provide their date of birth and gender.	1. Covered aircraft operators must collect individuals’ date of birth and gender and transmit this information to TSA. 2. Individuals must provide their date of birth and gender.
Definition of Overflight (49 CFR 1560.3) .....	Overflights mean flights that overfly the continental United States.	The final rule clarifies that continental United States does not include Hawaii or Alaska.
Request for and Transmission of SFPD (49 CFR 1560.101).	Covered aircraft operators would not be able to accept a reservation or request to enter the sterile area unless the individual provides his or her full name.	Covered aircraft operators may accept a reservation without a full name, date of birth, or gender. For reservations made 72 hours prior to the scheduled time of departure for each covered flight, the covered aircraft operator may choose to collect full name, gender, and date of birth for each passenger when the reservation is made or at a time that is no later than 72 hours prior to the scheduled time of departure of the covered flight. For an individual that makes a reservation for a covered flight within 72 hours of the scheduled time of departure for the covered flight, the covered aircraft operator must collect the individual’s full name, date of birth, and gender at the time of reservation. Covered aircraft operators may not transmit SFPD to TSA without these data elements.
Implementation Schedule (49 CFR 1560.101)	1. Covered aircraft operators would be required to request passenger information 60 days after the effective date of the final rule. 2. Covered aircraft operators would be required to begin transmitting SFPD to TSA on the date set forth in their AOIP.	Implementation schedule will be set forth in the AOIP.

<sup>6</sup> 72 FR 48320 (Aug. 23, 2007).

	Secure flight proposed rule	Secure flight final rule
Boarding Pass Issuance for a Covered International Flight that was Connected to a Non-Covered Flight (49 CFR 1560.105).	A covered aircraft operator may not issue a boarding pass for a covered international flight in conjunction with issuing a boarding pass for the non-covered flight unless the covered aircraft operator has obtained a boarding pass printing result from TSA permitting it to issue a boarding pass for the covered international flight.	A covered aircraft operator may authorize the issuance of a boarding pass for a covered international flight in conjunction with issuing a boarding pass for the non-covered flight provided that the covered aircraft operator takes the required actions to confirm and to comply with the boarding pass printing result for the passenger prior to the passenger boarding the aircraft.
Presenting Verifying Identity Document (VID) (49 CFR 1560.105).	Covered aircraft operators must request VID from passengers for whom TSA has not provided a watch list matching result or has placed on inhibited status.	The final rule clarifies that covered aircraft operators must request the VID from passengers at the airport. The VID may be presented at a kiosk that is capable of determining that the identification is a valid VID, authenticating the VID, and reading and transmitting passenger information from the VID.
Aircraft Operator Implementation Plan (49 CFR 1560.109).	Covered aircraft operators would be required to submit their AOIP to TSA within 30 days of the effective date of the final rule for approval. Once approved, the AOIP would be part of the covered aircraft operator's security program.	TSA will provide the AOIP to each covered aircraft operator for them to adopt as an amendment to their security program.

### B. Secure Flight Passenger Data

Under the Secure Flight program, TSA requires covered aircraft operators to collect information from passengers, transmit passenger information to TSA for watch list matching purposes, and process passengers in accordance with TSA boarding pass printing results regarding watch list matching results. 49 CFR 1560.101 and 1560.105. TSA defines this passenger information, along with other information summarized below, as Secure Flight Passenger Data (SFPD). See 49 CFR 1560.3.

For passengers on covered flights, TSA requires covered aircraft operators to request a passenger's full name, gender, date of birth, and Redress Number<sup>7</sup> (if available) or Known Traveler Number<sup>8</sup> (if available once the known traveler program is implemented). Even though covered aircraft operators are required to request all of the above data elements from passengers, passengers are only required to provide their full name, date of birth, and gender to allow TSA to perform watch list matching. TSA is not

requiring individuals to provide the other data elements to aircraft operators. Covered aircraft operators must transmit to TSA the information provided by the passenger in response to the request described above.

TSA notes that one of the changes between the NPRM and the final rule is the addition of this requirement that individuals are required to provide their date of birth and gender to aircraft operators. In the Secure Flight NPRM, TSA had discussed its legal authority for this rule, in general. See 72 FR 48357. With respect to this changed provision, TSA notes that it has legal authority to do so under § 4012 of the IRTPA. Section 4012 mandates that TSA obtain passenger information in order to assume the function of conducting watch list matching comparisons. In addition, TSA has broad authority to do so under the Aviation and Transportation Security Act (ATSA) (Pub. L. 107-71, Nov 19, 2001). Specifically, TSA can assess threats to transportation; enforce security-related regulations and requirements; oversee the implementation, and ensure the adequacy, of security measures at airports and other transportation facilities; require background checks for airport security screening personnel, individuals with access to secure areas of airports, and other transportation security personnel; and carry out such duties, and exercise such other powers, relating to transportation security as appropriate. See 49 U.S.C. 114(f)(2), (7), (11), (12), and (15). In conjunction with these provisions, TSA also has authority specifically for the Secure Flight Program. Under 49 U.S.C.

44903(j)(2)(C)(iv), the Assistant Secretary "shall require air carriers to supply the Assistant Secretary the passenger information needed to begin implementing the advanced passenger prescreening system." Given that TSA is required to collect this information from air carriers, it follows that individuals must provide that information to air carriers. Air carriers would be unable to fulfill their obligation if there were not a corresponding obligation on individuals to provide their information to air carriers.

Covered aircraft operators also must transmit to TSA passport information, if available. Although TSA is not requiring covered aircraft operators to request passport information under this final rule, passengers may provide passport information pursuant to other travel requirements such as CBP APIS if a passenger is traveling abroad as part of the same reservation/itinerary. When passengers provide passport information to covered aircraft operators, the operators must transmit the passport information to a single DHS portal from which the appropriate information will be sent to TSA and CBP.

Additionally, covered aircraft operators must transmit to TSA certain non-personally identifiable information such as itinerary information and record locator numbers. This information will allow TSA to effectively prioritize watch list matching efforts, communicate with the covered aircraft operator, and facilitate an operational response, if necessary, to an individual who is on the watch list.

When a non-traveling individual seeks authorization from a covered

<sup>7</sup> A Redress Number is a unique number that DHS currently assigns to individuals who use the DHS Traveler Redress Inquiry Program (TRIP). Under the Secure Flight program, individuals will use the Redress Number in future correspondence with DHS and when making future travel reservations. The Redress Number is further discussed in the Secure Flight Information Collection Requirements section below. See § 1560.3.

<sup>8</sup> A Known Traveler Number would be a unique number assigned to "known travelers" for whom the Federal government has already conducted a threat assessment and has determined do not pose a security threat. The Known Traveler Number is further discussed in the Secure Flight Information Collection Requirements section. See § 1560.3.

aircraft operator to enter an airport sterile area in the United States (such as to escort a minor or assist a passenger with a disability), covered aircraft operators must request from the non-traveler and transmit to TSA the same information requested from passengers. Non-travelers are only required to

provide their full name, date of birth, and gender to allow TSA to perform watch list matching, as well as certain non-personally identifiable information, including the airport code for the sterile area in the U.S. to which the non-traveler seeks access. The following chart details the information that TSA requires covered

aircraft operators to request from passengers and certain non-traveling individuals, the information that those individuals are required to provide, and the information covered aircraft operators must transmit to TSA if available.

**INFORMATION COLLECTION REQUIREMENTS FOR SECURE FLIGHT**

Data elements	Covered aircraft operators must request from passengers and certain non-travelers	Passengers and certain non-travelers must provide at time of reservation	Covered aircraft operators must transmit to TSA if available
Full Name .....	X	X	X
Date of Birth .....	X	X	X
Gender .....	X	X	X
Redress Number or Known Traveler Number .....	X	.....	X
Passport Information <sup>9</sup> .....	.....	.....	X
Itinerary Information <sup>10</sup> .....	.....	.....	X
Reservation Control Number .....	.....	.....	X
Record Sequence Number .....	.....	.....	X
Record Type .....	.....	.....	X
Passenger Update Indicator .....	.....	.....	X
Traveler Reference Number .....	.....	.....	X

**C. 72-Hour Requirement**

Under the Secure Flight program, covered aircraft operators must transmit the SFPD that is available in their system, to TSA approximately 72 hours prior to the scheduled flight departure time. For reservations created within 72 hours of flight departure, covered aircraft operators must submit SFPD as soon as it becomes available.

**D. Instructions to Covered Aircraft Operators**

TSA matches the SFPD provided by covered aircraft operators against the watch list. Based on the watch list matching results, TSA will instruct a covered aircraft operator in its boarding pass printing result to process the individual in the normal manner, to identify the individual for enhanced screening at a security checkpoint, or to deny the individual transport or authorization to enter a U.S. airport's sterile area. To ensure the integrity of the boarding pass printing results and to prevent use of fraudulent boarding

<sup>9</sup>Passport information is the following information from a passenger's passport: (1) Passport number; (2) country of issuance; (3) expiration date; (4) gender; (5) full name. See § 1560.3.

<sup>10</sup>Itinerary information is the following information about a covered flight: (1) Departure airport code; (2) aircraft operator; (3) departure date; (4) departure time; (5) arrival date; (6) scheduled arrival time; (7) arrival airport code; (8) flight number; (9) operating carrier (if available). For non-traveling individuals in the United States, the airport code for the sterile area to which the non-traveling individual seeks access. See § 1560.3.

passes, TSA will also provide instructions for placing bar codes on the boarding passes in the future. TSA may provide instructions to the covered aircraft operators through an amendment to their security programs.

**E. Summary of Requirements**

A brief summary of the requirements in this final rule is presented below. A detailed explanation of these requirements and any applicable changes from the NPRM are provided in Section III, Response to Comments, of this final rule.

**Requirements of Covered Aircraft Operators.** This final rule requires covered aircraft operators that conduct certain scheduled and public charter flights to:

- Adopt an Aircraft Operator Implementation Plan (AOIP). 49 CFR 1560.109(b).
- Conduct Operational Testing with TSA in accordance with their AOIP. 49 CFR 1560.109(a).
- Request full name, date of birth, gender, and Redress Number (if available) or Known Traveler Number (if implemented and available) from passengers and certain non-traveling individuals. 49 CFR 1560.101(a).
- Transmit full name, date of birth, and gender and any other available SFPD for passengers and non-traveling individuals seeking transport and/or authorization to enter a U.S. airport's sterile area, in accordance with the covered aircraft operator's AOIP, approximately 72 hours prior to the

scheduled flight departure time. 49 CFR 1560.101(b).

- Make a privacy notice available on public Web sites and self-serve kiosks before collecting any personally identifiable information from passengers or non-traveling individuals. 49 CFR 1560.103.
- Request a verifying identity document (VID) at the airport in either of the following situations: (1) TSA has not informed the covered aircraft operator of the results of watch list matching for an individual by the time the individual attempts to check-in; or (2) if TSA informs the covered aircraft operator that an individual must be placed on inhibited status<sup>11</sup> and may not be issued a boarding pass or authorization to enter a U.S. airport's sterile area. A verifying identity document is one that has been issued by a U.S. Federal, State, or tribal government that: (1) Contains the individual's full name, photo, and date of birth; and (2) has not expired. 49 CFR 1560.3 and 1560.105(c).
- When necessary, submit information from the VID to TSA to resolve potential watch list matches. In some cases, TSA may also request that the covered aircraft operator communicate a physical description of the individual. See 49 CFR 1560.105(c).

<sup>11</sup>"Inhibited status," as defined in this rule, means the status of a passenger or non-traveling individual to whom TSA has instructed a covered aircraft operator or a covered airport operator not to issue a boarding pass or to provide access to the sterile area. See 49 CFR 1560.3.

- Not issue a boarding pass or permit an individual to board an aircraft or enter a sterile area in a U.S. airport that serves covered flights under this regulation until that individual provides a VID when requested under the circumstances described above, unless otherwise authorized by TSA. 49 CFR 1560.105(d).

- Comply with instructions from TSA to designate identified individuals for enhanced screening before boarding a covered flight or accessing a sterile area in a U.S. airport. 49 CFR 1560.105(b)(2).

- Place codes on boarding passes in accordance with TSA instructions to be set forth in the Consolidated User Guide in the future. 49 CFR 1560.105(b)(2) and (3).

**Requirements of Individuals**

- Individuals who wish to make a reservation on a covered flight or to access a sterile area must provide their full names, date of birth, and gender to the covered aircraft operators.

- Passengers and non-traveling individuals seeking access to a U.S. airport's sterile area, for whom TSA has not provided a watch list matching result or has provided inhibited status, must present a VID to the covered aircraft operator if they wish to board their flights. After presenting the VID, an individual may receive a boarding pass to board an aircraft or enter a sterile area if the aircraft operator receives a watch list matching result from TSA that permits the issuance of a boarding pass or authorization to enter a sterile area. 49 CFR 1540.107(c).

*Government Redress Procedures Available to Individuals.* This final rule explains the redress procedures for individuals who believe they have been improperly or unfairly delayed or prohibited from boarding a flight as a result of the Secure Flight program. These individuals may seek assistance through the redress process by submitting certain personal information, as well as copies of certain identification documents, to the existing DHS Traveler Redress Inquiry Program

(DHS TRIP).<sup>12</sup> The final rule explains the process the Federal government will use to review the information submitted and to provide a timely written response. 49 CFR part 1560, subpart C.

*F. Implementation Phases of Secure Flight*

TSA will implement the Secure Flight program in two phases. The first phase includes covered flights between two domestic points in the United States. The second phase includes covered flights overflying the continental United States, covered flights to or from the United States, and all other flights (such as international point-to-point flights) operated by covered U.S. aircraft operators not covered in the first phase.

**1. Implementation of Secure Flight for Domestic Flights**

During the first phase of implementation, TSA will assume the watch list matching function for domestic flights conducted by covered U.S. aircraft operators, including those covered aircraft operators' private charter flight operations. TSA will conduct operational testing with such covered U.S. aircraft operators to ensure that the aircraft operators' systems are compatible with TSA's system. After successful operational testing with covered U.S. aircraft operators, TSA will assume the watch list matching function for domestic flights from those aircraft operators.

**2. Implementation of Secure Flight for Overflights and International Flights**

During the second phase of Secure Flight, TSA will require all covered aircraft operators to submit SFPD for covered flights that overfly the continental United States. The continental U.S. is defined as the contiguous lower 48 states and does not include Alaska or Hawaii. Flights that transit the airspace of the continental United States between two airports or locations in the same country, where that country is Canada or Mexico, are not included in this final rule. We

discuss in further detail below the reason for excluding these flights from this final rule. Covered aircraft operators that are unsure whether a particular flight overflies the continental United States may ask TSA for a determination on whether the flight is an overflight.

The second phase of Secure Flight will also include international flights. Until TSA implements the Secure Flight program for international flights by covered U.S. and foreign aircraft operators, the CBP system will conduct pre-departure watch list matching for international flights under the APIS Pre-Departure final rule. This interim approach will allow DHS to more quickly address the threat of terrorism on flights arriving in and departing from the United States.

During the second phase of Secure Flight implementation, TSA will assume the watch list matching function for covered international flights from the CBP system. There are a few differences between TSA and CBP processes. Under the Secure Flight program, covered aircraft operators will need to request passenger information at the time of reservation or prior to transmitting the passenger's SFPD; this is not the case under the APIS Pre-Departure final rule. Also, as described below, TSA requires collection of different data elements (SFPD) under the Secure Flight program than CBP collects under the APIS regulations. For its border-control functions, which CBP will continue to perform under the APIS rule, the Department (through CBP) will continue to collect APIS data. Given this, and to provide a single point of contact, covered aircraft operators can transmit both APIS data and SFPD in a single transmission to the DHS portal, which will route information to TSA and CBP accordingly.<sup>13</sup> In turn, aircraft operators will receive one boarding pass printing result from DHS. The following table lists the data elements that CBP collects under its APIS regulations and that TSA will collect under the Secure Flight<sup>14</sup> program.<sup>15</sup>

Data elements	APIS regulation (international flights) <sup>14</sup>	Secure flight regulation <sup>15</sup>
Full Name .....	X	X
Date of Birth .....	X	X
Gender .....	X	X
Redress Number or Known Traveler Number .....	.....	X*
Passport Number .....	X	X*

<sup>12</sup> Information about DHS TRIP is available at <http://www.dhs.gov/trip>.

<sup>13</sup> Covered aircraft operators may also submit Passenger Name Record information to CBP through this DHS portal.

<sup>14</sup> All APIS data elements are required, except country of residence (which is not required for departure from the U.S.) and passport information (which is required only when a passport is required for travel).

<sup>15</sup> Covered aircraft operators must provide data elements listed for Secure Flight to the extent they are available.

Data elements	APIS regulation (international flights) <sup>14</sup>	Secure flight regulation <sup>15</sup>
Passport Country of Issuance	X	X*
Passport Expiration Date	X	X*
Passenger Name Record Locator	X	
International Air Transport Association (IATA) Foreign Airport Code—place of origination	X	X
IATA Code—Port of First Arrival	X	X
IATA Code of Final Foreign Port for In-transit Passengers	X	
Airline Carrier Code	X	X
Flight Number	X	X
Date of Aircraft Departure	X	X
Time of Aircraft Departure	X	X
Date of Aircraft Arrival	X	X
Scheduled Time of Aircraft Arrival	X	X
Citizenship	X	
Country of Residence	X	
Status on Board Aircraft	X	
Travel Document Type	X	
Alien Registration Number	X	
Address While in U.S.—(except for outbound flights, U.S. citizens, lawful permanent residents, crew and in-transit passengers)	X	
Reservation Control Number		X
Record Sequence Number		X
Record Type		X
Passenger Update Indicator		X
Traveler Reference Number		X

\* If available.

If passenger information that is required under this final rule resides in covered aircraft operators' systems, covered aircraft operators must transmit the SFPD information to TSA. Covered aircraft operators must submit this information, through the same DHS portal used for APIS submissions, approximately 72 hours before departure of a covered flight, or if a passenger books after this 72 hour mark, as soon as that information becomes available. Those that elect to transmit the SFPD and all manifest information required under the APIS Pre-Departure final rule at the same time would be able to send a single transmission to DHS for the Secure Flight and APIS Pre-Departure programs and would receive a single boarding pass printing result in return.

Additionally, for reservations made within 72 hours of the scheduled flight departure time, covered aircraft operators must submit SFPD as soon as the information becomes available. If the covered aircraft operator is also required and ready to transmit APIS information at that time, the covered aircraft operator is able to send one transmission for both Secure Flight and APIS Pre-Departure and will receive one boarding pass printing result. If the covered aircraft operator does not have full and complete APIS data as required under the APIS Pre-Departure rule, the covered aircraft operator must transmit the passenger information required for Secure Flight, at a minimum.

Covered aircraft operators will use the same portal to transmit SFPD to TSA and APIS data to CBP. TSA will need to conduct operational testing with the covered U.S. aircraft operators and covered foreign air carriers to confirm that the Secure Flight process operates properly from end-to-end with these carriers.

After TSA assumes responsibility for the watch list matching function under phase two of the Secure Flight program, the CBP system will no longer be responsible for pre-departure watch list matching or the issuance of related boarding pass printing results for covered flights based on watch list matching results. Consequently, covered aircraft operators will receive, and have to comply with, one result from DHS, via TSA, regarding the issuance of boarding passes to or the boarding of passengers on covered international flights. CBP will, however, continue to require carriers to provide APIS data to carry out its border enforcement mission.

In some international airports, passengers may transit from one international flight to another, where the flights are operated by different aircraft operators and only the second flight may be covered under this final rule. TSA understands that currently, in these situations, the aircraft operator operating the first flight may issue a boarding pass for both portions of the passenger's itinerary, including the flight to the United States. Under the Secure Flight program, TSA will not

prevent the aircraft operator operating the first flight from issuing a boarding pass for the second flight. The covered aircraft operator whose flight will arrive in, or overfly the United States is responsible for preventing the boarding of passengers for whom TSA has returned an inhibited boarding pass printing result. Additionally, the covered aircraft operator should ensure that passengers for whom TSA has returned a Selectee boarding pass printing result are subjected to enhanced screening prior to boarding. Covered aircraft operators must also comply with measures in their security program to ensure that they have confirmed the boarding pass status of each passenger who receives a boarding pass for a covered flight under these circumstances. They may not rely on a lack of markings on a boarding pass issued by another aircraft operator; covered aircraft operators must take their direction from TSA.

*G. Privacy Documents*

TSA is committed to safeguarding individuals' privacy in conducting the Secure Flight program to the greatest extent possible. In conjunction with this final rule, TSA has published a Privacy Impact Assessment (PIA) and a Privacy Act System of Records Notice (SORN),<sup>16</sup> DHS/TSA 019. A final rule that explains the Privacy Act exemptions for the Secure Flight program was published in

<sup>16</sup> 72 FR 63711 (Nov. 9, 2007).

the **Federal Register**.<sup>17</sup> These three documents outline how TSA collects, uses, stores, protects, retains, and shares personally identifiable information collected and used as part of the Secure Flight program. Furthermore, TSA has identified the privacy risks and mitigation measures that will be employed to reduce or eliminate privacy risks such as false positive matches or insufficient safeguards for the information. All three documents are available at <http://www.tsa.gov>.

#### *H. The Watch List Matching Process Under Secure Flight*

This Secure Flight final rule requires all covered aircraft operators to request the information discussed above from passengers on a covered flight and certain non-traveling individuals. The final rule, however, does not require all covered aircraft operators to begin transmitting that information to TSA at the same time. TSA will bring covered aircraft operators into the Secure Flight program in phases and require all covered aircraft operators to begin providing passenger and certain non-traveler information to TSA in accordance with the deadlines set forth in their approved AOIP, discussed further below.

TSA requires covered aircraft operators to transmit information to TSA approximately 72 hours in advance of departure unless one of the following occurs: The individual makes a reservation with the covered aircraft operators within 72 hours of the scheduled flight departure time; there are changes to the name, date of birth, gender, Redress Number, Known Traveler Number, or passport information on a reservation within 72 hours of the scheduled flight departure time; there are changes to a flight within 72 hours of the scheduled flight departure time; or the individual requests to enter a sterile area upon arrival at the airport. In such cases, TSA requires covered aircraft operators to send the required information to TSA as soon as it becomes available. TSA, in coordination with the TSC where necessary, will compare the passenger and certain non-traveler information obtained from each covered aircraft operator to information contained in the watch list. TSA will also compare passenger and certain non-traveler information to a list of individuals who have previously been distinguished from persons on the watch list.

If an automated comparison using the information transmitted to TSA indicates that the passenger is not a

match to the watch list, TSA will notify the covered aircraft operator that check-in and boarding pass issuance for the individual can proceed normally. Such individuals will undergo standard passenger and baggage screening, which may include additional, random screening. If an automated comparison using the non-traveler information identifies a potential match to the watch list, the covered aircraft operator must not allow access to the sterile area for that individual unless further resolution procedures indicate otherwise or authorized by TSA.

TSA will complete the watch list matching process for, and permit covered aircraft operators to issue boarding passes to, the vast majority of passengers through this fully-automated initial comparison. If the automated comparison indicates a reasonably similar or exact match to a person on the watch list, TSA will inform the covered aircraft operator that the individual must be placed on inhibited status and consequently the covered aircraft operator may not issue a boarding pass or other authorization to enter the sterile area for that individual unless further resolution procedures indicate otherwise. If the SFPD for that individual contains sufficient data, a TSA analyst will review all available information to determine if the passenger appears to be the individual on the watch list. If necessary, the TSA analyst will check other classified and unclassified governmental terrorist, law enforcement, and intelligence databases, including databases maintained by the Department of Homeland Security, Department of Defense, National Counter Terrorism Center, and Federal Bureau of Investigation (FBI), in order to resolve the possible match between the individual and a person on the watch list.

This careful review process is intended to significantly reduce the number of false positive matches identified by the automated watch list check. If the TSA analyst determines that the individual is not a match to the watch list, TSA will inform the covered aircraft operator that the individual no longer has inhibited status, and the covered aircraft operator may issue a boarding pass or authorization to enter a sterile area to that individual. If the TSA analyst identifies a possible match between a passenger and an individual identified on the watch list, TSA will send the passenger information to TSC and request confirmation of the match.

The final rule provides that if TSA or TSC cannot determine from the information provided by the covered aircraft operator whether an individual

is a match to the watch list prior to the individual's arrival at the airport or online check-in, it will be necessary for the individual to provide additional information at the airport. Pursuant to the procedures in the security program, the covered aircraft operator must request that the individual present a VID when he or she arrives at the airport. A VID must be an unexpired form of identification that was issued by a U.S. Federal, State, or tribal government, and contains the individual's full name, photo, and date of birth, or an unexpired passport issued by a foreign government. TSA may also authorize other types of identity documents that may be used as a VID. TSA will notify the public when it authorizes another type of identity document that may be used as a VID. TSA may use one or more of the following methods to notify the public: A notice published in the **Federal Register**; a public affairs announcement; and an announcement on TSA's Web site. This requirement would not replace current requirements that covered aircraft operators request all passengers and non-traveling individuals to provide identification, such as at check-in or at the screening checkpoint.

Covered aircraft operators must follow the procedures in its security program for requesting and reviewing a VID from an individual. Examples of such procedures are that the covered aircraft operator may request that the individual present a VID: (1) To an agent at a ticket counter; and (2) at a self-serve kiosk that is capable of determining that the identification is a valid VID, authenticating the VID, and reading and transmitting passenger information from the VID. Covered aircraft operators may also submit a request to TSA for approval of other procedures for requesting and accepting a VID through the security program amendment process in § 1544.105(b).

Once the individual provides a VID to the covered aircraft operator or swipes the VID at a kiosk, the aircraft operator must update the passenger's SFPD with the additional information from the individual's VID and transmit it to TSA. There may be occasions where the aircraft operator will need to call TSA. In such cases, the aircraft operator may be asked to provide additional identifying information, such as a physical description referred to as "Passenger Resolution Information" (PRI), that TSA may need to complete the watch list matching process, in coordination with the TSC, and provide the aircraft operator with watch list matching results for that individual.

<sup>17</sup> 72 FR 63706 (Nov. 9, 2007).



Covered aircraft operators will not submit this PRI to TSA electronically. Rather, an aircraft operator will provide this information over the telephone to TSA.

Where warranted, TSA may notify another Federal agency or other public, private, or foreign government entity as appropriate to initiate an operational response to a potential watch list match.<sup>18</sup> TSA will provide the agency or entity with sufficient information about the passenger and his or her itinerary to facilitate coordination of the operational response. TSA may also notify the Federal Security Director, Federal Air Marshals, or other law enforcement personnel responsible for airport security to facilitate a timely law enforcement response to an individual identified in the watch list. Further inquiry by law enforcement may, for example, help resolve a situation of mistaken identity or confirm a determination made in the matching process that an individual should be denied boarding or entry to a sterile area.

If TSA determines that the passenger is a match to the Selectee List, TSA will notify the covered aircraft operator that the passenger and his or her baggage must be identified for enhanced screening by TSA. If TSA determines that the passenger is a match to the No Fly List, the covered aircraft operator must not issue a boarding pass to the passenger unless authorized by TSA.

In the preamble to the Secure Flight NPRM, TSA described the resolution process for the potential matches to the No Fly List but did not discuss a resolution process for potential matches to the Selectee List.<sup>19</sup> Because it is an important security measure to confirm whether a passenger is an individual on the Selectee List, TSA is applying the same resolution process for potential matches to the Selectee List as it applies to potential matches to the No Fly List. This resolution process will reduce the number of passengers who may be misidentified as a match to the Selectee List and will allow these passengers to enter the sterile area without undergoing enhanced screening for Selectees. (This does not ensure that such passengers will not always avoid enhanced screening. Random procedures employed by TSA result in enhanced screening.) TSA may also

authorize alternate resolution procedures in a covered aircraft operator's security program to address unique circumstances.

The Secure Flight NPRM also proposed that passengers with an inhibited status would present their VID to the agent at the airport ticket counter. See proposed § 1560.105(b)(1). TSA is revising the rule text to state that covered aircraft operators must request VIDs from individuals at the airport. The language change will allow a covered aircraft operator the flexibility to request and accept VID at the ticket counter, at a self-serve kiosk, or through other processes or technology that the covered aircraft operator may develop, subject to TSA approval.

#### *I. Operational Testing of Secure Flight*

As part of the implementation of the Secure Flight program, TSA will conduct operational testing of TSA's capabilities to interact with and perform watch list matching for each covered aircraft operator shortly after the effective date of this final rule and before assuming the watch list matching function from each covered aircraft operator. During the operational testing for each covered aircraft operator, the covered aircraft operator will establish data transmission connections to TSA through an established DHS portal, and TSA will test its ability to receive passenger and non-traveler information, conduct watch list matching and transmit watch list matching results back to the aircraft operator in real time. Operational testing will allow TSA to refine program operations and ensure that TSA will be able to effectively conduct watch list matching for passengers and non-traveling individuals of each covered aircraft operator before TSA assumes the watch list matching function.

Covered U.S. aircraft operators will continue to match passengers against the watch lists for domestic flights under current procedures during their operational test phase and will maintain responsibility for denying issuance of boarding passes or identifying individuals for enhanced screening as a result of their own watch list matching determinations. If, during operational testing, TSA identifies a match to the No Fly or Selectee Lists that a covered aircraft operator has not identified, TSA may identify such passengers to the TSC and the covered aircraft operator for appropriate action. Once TSA officially notifies a carrier that they have successfully completed testing and that TSA has assumed the watch list matching function from a covered aircraft operator, the aircraft operator

will discontinue conducting watch list comparisons for passengers and non-traveling individuals.

For international flights, covered U.S. aircraft operators must follow the CBP result in accordance with the APIS Pre-Departure final rule until TSA informs the covered U.S. aircraft operator that it will assume the watch list matching function. Foreign air carriers must also follow the CBP system boarding pass printing results in accordance with the APIS Pre-Departure final rule during operational testing and until TSA informs the covered foreign air carriers that TSA will assume the watch list matching function.

TSA will provide prior written notification to each covered aircraft operator of the date on which it will assume the watch list matching function from that covered aircraft operator. Because operational testing will begin with covered aircraft operators in phases, TSA will transition to implementation in phases as well and may continue operational testing with some covered aircraft operators while beginning implementation with others.

#### **III. Response to Comments**

TSA received 337 comments on the Secure Flight NPRM. These comments were submitted by a broad cross-section of parties with an interest in the function of conducting preflight comparisons of airline passenger information to Federal government watch lists for international and domestic flights. Commenters included domestic aircraft operators, foreign air carriers, privacy advocacy groups, and travel agency organizations. These comments are addressed below, and are organized by major issue.

##### *A. Scope of the Rulemaking*

*Comment:* Many commenters argued that the Secure Flight program is unconstitutional and infringes on an individual's freedom of movement, assembly, and right to travel. A commenter also argued that the Secure Flight program violates Article 12 of the International Covenant on Civil and Political Rights (ICCPR) because it restricts "liberty of movement."

*TSA Response:* TSA disagrees with the comments. The Government may place reasonable restrictions on the right to travel in order to protect compelling interests; in this case, transportation and national security. The Secure Flight program does not deny individuals their right to travel or other constitutional rights. Courts have consistently held that travelers do not have a constitutional right to travel by a single mode or the most convenient form of

<sup>18</sup> For the types of public and private entities that TSA may notify, see "Routine Uses of Records Maintained in the System, Including Categories of Users and Purpose of Such Uses" in the **Federal Register** notice entitled, "Privacy Act of 1974: System of Records; Secure Flight Records." 72 FR 63711 (Nov. 9, 2007).

<sup>19</sup> 72 FR 48356, 48365-66 (Aug. 23, 2007).

travel. The Secure Flight program would only regulate one mode of travel (aviation) and would not impose any restriction on other modes of travel. Thus, Secure Flight does not unlawfully infringe or restrict individuals' freedom of movement or assembly. Also, the Secure Flight regulations are reasonable and are not onerous or unduly burdensome to individuals.

Additionally, Article 12 of the ICCPR does not apply to laws that are necessary to protect national security. Because the purpose of the Secure Flight program is to protect national security, Article 12 would not apply even if the Secure Flight program did somehow restrict liberty of movement.

#### 1. Overflights and Foreign Air Carriers

*Comment:* Several commenters expressed concern about the Federal government collecting information in the case of overflights from individuals who have no intention of entering the United States. Several commenters argued that including overflights within the scope of Secure Flight may violate international treaties such as the Convention on International Civil Aviation (Chicago Convention).

*TSA Response:* U.S. regulations currently require aircraft touching ground in the United States to deny transportation to any passenger appearing on the U.S. No Fly List. The Secure Flight program will extend application of this rule to aircraft that only fly through U.S. airspace, without actually touching ground in the United States. The international legal bases under which a State might deny overflight to aircraft that fail to comply with the State's security-based regulations are outlined below.

Although international law recognizes the general right of overflight,<sup>20</sup> it also recognizes a State's right to regulate aircraft entering into, within or departing from its territory. Moreover, the Chicago Convention expressly recognizes that each State has sovereignty over its airspace.

The Chicago Convention, the International Air Services Transit Agreement (IASTA), and the U.S. model open skies agreement all contain provisions requiring aircraft in U.S. territory to comply with a broad array of U.S. laws and regulations. Article 11 of the Chicago Convention requires compliance with "the laws and regulations of a contracting State relating to the admission to or departure from its territory of aircraft engaged in

international air navigation, or to the operation and navigation of such aircraft while within its territory." Similarly, Article 13 requires compliance with a State's laws and regulations "as to the admission to or departure from its territory of passengers, crew or cargo of aircraft \* \* \* upon entrance into or departure from, or while within the territory of that State." These Chicago Convention obligations are incorporated by reference in Article I, Section 2, of IASTA, and are restated in Article 5 of the model open skies agreement.

The domestic laws and regulations with which compliance is mandated are defined broadly and may include security-based measures, such as Secure Flight. This is reinforced by the security provisions in most U.S. bilateral air services agreements. Those provisions generally obligate our bilateral partners to observe and assist the U.S. Government in its enforcement of U.S. security-based regulations. For instance, Article 7 of the U.S. model open skies agreement obligates each party to observe the "security provisions required by the other party for entry into, for departure from, and while within the territory of that other [p]arty, and to take adequate measures to protect aircraft and to inspect passengers \* \* \* prior to and during boarding or loading." Model Article 7 also imposes specific obligations on our bilateral partners to assist in preventing unlawful acts against the safety of aircraft, and "to address any other threat to security of civil air navigation."

Moreover, in the event that an airline fails to comply with the laws and regulations with which compliance is mandated, both IASTA and most U.S. bilateral agreements grant a State the option of revoking or denying that airline's operating authorizations or technical permissions. Under Article I, Section 5, of IASTA, each State reserves the "right to withhold or revoke a certificate or permit to an air transport enterprise of another State \* \* \* in case of failure of such air transport enterprise to comply with the laws of the State over which it operates." Similar rights exist in almost all U.S. bilateral agreements. For example, Article 4 of the U.S. model open skies agreement provides that either party may "revoke, suspend or limit the operating authorizations or technical permissions" of an airline of the other party in the event that that airline has failed to comply with the laws and regulations with which compliance is mandated.

Accordingly, TSA's Secure Flight program does not violate international treaties, such as the Chicago

Convention, and is entirely consistent with and is buttressed by international and bilateral agreements.

*Comment:* TSA received several comments opposed to including overflights in the scope of the final rule. Some commenters argued that overflights are an overextension of the Secure Flight mission. Other commenters suggested that overflights will cause costly system and operational changes for flights that did not require collection of APIS data or SFPD previously. Another commenter suggested that it would not be possible for third party agents to know if data collection was required for a particular flight since they do not have any knowledge of which flights qualify as an overflight.

*TSA Response:* Flights that overfly the United States have the potential to cause harm within the United States due their proximity to sensitive areas that may be potential terrorist targets such as major metropolitan areas and critical infrastructure. The Secure Flight program will provide TSA the ability to determine whether a passenger on an overflight poses a potential threat to national or transportation security. TSA acknowledges that there are costs associated with including overflights within the scope of Secure Flight but believes that the security benefit justifies the cost. If a covered aircraft operator is unsure whether a particular flight overflies the United States, TSA will provide assistance in determining whether that flight is an overflight. The covered aircraft operator will be responsible for informing their third party agents of the flights that are overflights.

*Comment:* Several commenters raised concerns regarding unplanned overflights. Commenters provided examples of situations such as diversions for weather, emergency, medical, or mechanical reasons when a flight may be diverted into U.S. airspace. These commenters suggested that TSA not require data collection for unplanned overflights.

*TSA Response:* As stated above, TSA will assist covered aircraft operators in determining which flights are overflights. TSA is not likely to consider flights that occasionally overfly the United States due to weather diversions or emergencies to be overflights.

*Comment:* Several commenters indicated concern that this provision may set a precedent for other countries to invoke overflight data collection requirements that would be costly to implement and present an inconvenience to U.S. passengers.

<sup>20</sup> For example, the Chicago Convention, Article 5 and the International Air Services Transit Agreement (IASTA), Article I, Section 1.

*TSA Response:* The Federal government understands that countries have a legitimate interest in protecting their territory from potential threats from overflights. DHS will work and coordinate with the governments of those countries to determine data collection requirements that would enhance security.

*Comment:* TSA received several comments about exemptions to the overflight provision. A commenter requested that any geographic exceptions to the Secure Flight final rule allow for the designation of low-risk areas to be consistent with the overall purpose of security and to take into account the risk associated with diverting air traffic to lower risk geographic areas. Another commenter expressed support for any efforts to decrease the number of flights this would apply to, based on selected geographic areas.

*TSA Response:* This final rule allows the Assistant Secretary (Transportation Security Administration) to exempt certain overflights from the Secure Flight program. In determining whether to exempt a particular flight or category of flights, TSA will take into consideration the security implications of exempting such flights, including the geographic locations of the overflights.

*Comment:* One commenter questioned why flights that are not subject to this final rule, for example those flights that overfly the U.S. with an origin and destination in Canada, pose less of a risk to U.S. aviation security than a flight originating in Canada and flying to another destination, for example the Caribbean. One commenter sought confirmation that all airlines overflying U.S. territory would be subject to the same requirements, irrespective of their nationality. The Canadian Embassy requested that all flights to, from, and within Canada that overfly the U.S. be exempt from the Secure Flight final rule in light of the security initiatives that Canada has in place and the security cooperation between Canada and the United States.

*TSA Response:* Flights between two Canadian locations or between two Mexican locations that overfly the United States are likely to merely skirt the border with the United States or enter U.S. airspace only for a brief period of time. This provision applies to all covered aircraft operators regardless of their country of nationality. All covered aircraft operators must comply with the Secure Flight rule for all other flights that overfly the continental United States, regardless of nationality.

TSA is not exempting all overflights that originate from Canada, because

most international flights originating from Canada overfly a significant portion of the United States. As stated above, TSA has determined that conducting watch list matching of passengers on these flights is an important security measure to protect national and transportation security.

However, the Assistant Secretary may exempt categories of flights that overfly the United States as provided in § 1560.3. TSA will consider requests to exempt certain categories of flights and will consider all the applicable factors, including the security risks and the benefits from doing so. For instance, TSA will consider whether the country requesting the exemption applies a no fly list system to flights that may affect the security of the United States, whether that no fly list system will provide robust protection from persons who may endanger the flights, and whether the requesting country sufficiently shares information with the United States.

*Comment:* Some commenters expressed support for the limitation of the overflight provision to the continental United States. However, the Canadian Embassy and other commenters requested clarification of the definition of “continental United States” as it applies to the overflight provision of the Secure Flight final rule.

*TSA Response:* TSA agrees that the definition should be clarified. The definition of “overflying the continental United States” in this final rule has additional language that clearly states that the continental United States includes the lower 48 states and does not include Alaska or Hawaii.

## 2. Include Other Aircraft Operators in Secure Flight Program

*Comment:* TSA received one comment from an individual who suggested that TSA include all-cargo operators within the scope of the Secure Flight rule, because many all-cargo aircraft operators also transport individuals who are not flight crew members, such as couriers and animal handlers. The commenter was concerned that these individuals may be foreign nationals, and they frequently sit immediately outside the flight deck on these all-cargo flights.

*TSA Response:* During development of the Secure Flight program, TSA determined that the scope of the initial Secure Flight implementation phases should include only those aircraft operators that are required to have a full security program under 49 CFR 1544.101(a), and foreign air carriers that are required to have a security program under 49 CFR 1546.101(a) or (b). These

aircraft operators are the passenger airlines that offer scheduled and/or public charter flights from commercial airports. TSA has decided to limit the scope of the Secure Flight final rule to these aircraft operators in order first to focus on those areas that raise the most aviation security concerns. After successful implementation of the original population of covered aircraft operators, TSA will consider broadening Secure Flight’s scope to include other categories of aircraft operators. In the interim, the all-cargo operators must conduct watch list matching for these individuals.

*Comment:* A commenter requested TSA modify the Secure Flight final rule to accommodate the processes of private charter carriers.

*TSA Response:* In the Secure Flight NPRM, TSA proposed to limit the scope of the Secure Flight program to U.S. aircraft operators that are required to have a full security program under 49 CFR 1544.101(a), and covered flights operated by foreign air carriers that are required to have a security program under 49 CFR 1546.101(a) or (b). Many U.S. aircraft operators also operate private charter operations that are subject to the requirements in 49 CFR 1544.101(f), which include requiring aircraft operators to conduct watch list matching of the passengers. TSA recognizes that it may be more efficient for the covered U.S. aircraft operators to submit the names of passengers on their private charters to Secure Flight for watch list matching. Consequently, the definition of covered flight includes private charter flights operated by covered U.S. aircraft operators. TSA intends to implement Secure Flight for other private charter flights through future rulemakings.

*Comment:* One commenter requested that TSA require foreign air carriers conducting private charter passenger operations to and from the United States to adopt and carry out a security program. Alternatively, the commenter requested that TSA include foreign operators of private charter flights within the scope of the Secure Flight program instead of the existing TSA/FAA airspace waiver procedures for flights entering, departing, or overflying U.S. airspace.

*TSA Response:* TSA appreciates the comments received concerning aircraft operators covered under this final rule. TSA did not propose, however, to require foreign air carriers not currently subject to an existing security program to adopt a security program or to apply the Secure Flight requirements on these foreign air carriers as part of this Secure Flight rulemaking.

However, foreign air carriers operating flights to and from the United States are subject to the APIS Pre-Departure final rule under which DHS will perform watch list matching of the passengers on their flights.

*Comment:* TSA received several comments from aircraft operators arguing that airlines do not have the ability to impose Secure Flight requirements on travel agents and other third parties. A commenter suggested the government should mandate travel agencies to collect full name in the reservation and place a privacy notice on associated Web sites.

*TSA Response:* TSA disagrees that covered aircraft operators are unable to require travel agents and other third parties that sell tickets for their flights to collect the necessary passenger information. Because aircraft operators control the inventory of seats on their airplanes, TSA believes that it is reasonable to expect that aircraft operators will include in their agreements with third party agents who sell tickets on the aircraft operator's behalf a requirement to collect the necessary data for the aircraft operator to comply with this rule.

Additionally, the requirement to include the Privacy Act Statement on Web sites only applies to Web sites where passenger information is collected to create the SFPD that will be sent to TSA. Third-party Web sites that provide information about their services but do not collect passenger information that create SFPD do not need to post the Privacy Act Statement.

*Comment:* A commenter agreed with TSA's definition of a non-traveling individual, which does not include employees or agents of an airport or aircraft operator.

*TSA Response:* TSA appreciates the commenter's support of Secure Flight's definition of a non-traveling individual.

*Comment:* TSA received some comments urging TSA to include watch list matching of covered aircraft operators' employees and other employees that must undergo watch list matching within the scope of Secure Flight. Similarly, a few carriers requested clarification on whether TSA plans to perform this function.

*TSA Response:* TSA agrees that comparing the names of covered aircraft operators' employees and other employees against the watch list is an important layer of security and that the Federal government should assume the responsibility for conducting the watch list matching for this population. TSA has decided to focus the Secure Flight program on watch list matching of passengers as part of this final rule. TSA

plans to assume responsibility for watch list matching of employees. TSA has begun the process by conducting watch list matching for certain persons at commercial airports.

#### *B. Coordination With CBP and Other Government Agencies*

TSA received several comments expressing support for both the Secure Flight and APIS Pre-Departure programs. Several commenters indicated their support for the shift of responsibility for passenger watch list matching from the air carriers and CBP to TSA. TSA received several comments expressing support for the "One DHS Solution" approach proposed for the Secure Flight and CBP APIS Pre-Departure programs whereby covered aircraft operators would send passenger information through one portal for both programs.

*Comment:* One commenter requested that DHS and other agencies coordinate Secure Flight's requirements with other U.S. and non-U.S. government data collection requirements.

*TSA Response:* DHS oversaw the development of the Consolidated User Guide to standardize requirements and minimize the impact to covered aircraft operators for implementation of both the Secure Flight and the APIS Pre-Departure programs. DHS will continue to work and coordinate with other Federal government agencies and other countries to develop and implement common data collection requirements to address the security concerns of the Federal government and the governments of other countries.

*Comment:* TSA received a comment expressing concern that CBP and covered aircraft operators would be required to act upon TSA's watch list matching results without a process in place for quality assurance and review.

*TSA Response:* TSA will implement a number of quality control measures as part of the Secure Flight program to ensure that the processes and procedures for watch list matching and returning results to covered aircraft operators are accurate and timely. TSA cannot provide further detail as to the control measures in place as they are Sensitive Security Information (SSI).<sup>21</sup> However, TSA is confident that these

measures will ensure the accuracy of the program.

*Comment:* TSA received several comments expressing concern and requesting clarification on the differences in requirements for the APIS Pre-Departure final rule and Secure Flight NPRM. They questioned the need to send TSA SFPD 72 hours before the flight departure while APIS Pre-Departure requires batch transmission no later than 30 minutes before the securing of the aircraft door or APIS Quick Query (AQQ) transmission up to the securing of the aircraft door.

*TSA Response:* From the perspective of covered aircraft operators, there are two major differences from APIS Pre-Departure and Secure Flight. First, TSA and CBP require different sets of data elements for their respective programs with some identical data elements. The chart above in section II of this final rule, Secure Flight Program Summary, compares the required and optional data elements for each program. Additionally, the timing of the transmission of the data elements is different for each program. As explained above in section II of this final rule, Secure Flight Program Summary, TSA will require covered aircraft operators to transmit all available SFPD 72 hours before the scheduled departure of the flight and for reservations made within 72 hours, and other SFPD as soon as they become available. Under the APIS Pre-Departure rule, CBP requires commercial air carriers to transmit APIS information 30 minutes before the securing of the aircraft door if the transmission is a batch transmission and up to the securing of the aircraft doors for AQQ transmissions.

While both rules will be used in our nation's fight against terrorism, the two rules have somewhat different purposes. The purpose of the APIS rule is to protect our nation's borders by evaluating the risk associated with passengers entering or leaving the United States. Generally, CBP conducts this analysis prior to passengers arriving in or departing the United States, to ensure more efficient and expeditious processing of legitimate travelers. By the time passengers arrive into the United States, CBP has completed its analysis and determined the appropriate operational response when the passengers present themselves to the CBP officer.

The purpose of the Secure Flight program is to protect aviation security by conducting watch list matching of the names of passengers and non-travelers. TSA must complete its watch list matching prior to the individuals' receiving a boarding pass or

<sup>21</sup> "Sensitive Security Information" or "SSI" is information obtained or developed in the conduct of security activities, the disclosure of which would constitute an unwarranted invasion of privacy, reveal trade secrets or privileged or confidential information, or be detrimental to the security of transportation. The protection of SSI is governed by 49 CFR part 1520.

authorization to enter a sterile area. Many passengers prefer to obtain their boarding passes 24 hours before departure. By receiving the SFPD 72 hours before departure, TSA will be able to allow the majority of passengers to obtain their boarding passes 24 hours in advance.

DHS' goal is to consolidate the watch list matching process into the Secure Flight program, including the timing of the transmission of passenger information for watch list matching. The watch list matching component of the APIS Pre-Departure final rule is an interim solution until such time that the Secure Flight program can assume responsibility for watch list matching for international flights. Although CBP requires that aircraft operators send batch transmission no later than 30 minutes before the securing of the aircraft doors, it allows and encourages aircraft operators to transmit the passenger information as early as 72 hours before the flight. As stated below in the excerpt from the APIS Pre-Departure final rule, CBP and DHS recognized that earlier transmission of the data benefits the aircraft operators and the passengers, including reducing the risk that passengers may miss their flights while TSA conducts further analysis.

Advance transmissions will enable earlier vetting by CBP and earlier issuance of boarding passes by carriers if warranted by vetting results, relieving the pressure that a high volume of later transmitted data could have on the carriers' operations. DHS believes that earlier transmissions, though not required, would be to the carriers' advantage and encourages carriers to adopt it as a best business practice.

\* \* \* \* \*

In addition, carriers have requested that CBP allow manifest data transmissions as early as 72 hours prior to departure. CBP agrees that such early transmissions, which DHS encourages carriers to adopt as a best business practice, would generate early vetting results, subject to later validation by the carrier (swiping of passport or other travel document or examination of document by carrier personnel), and allow early issuance of boarding passes, resulting in fewer passengers to be vetted within the 30-minute window and a reduced risk of passengers missing their flights while further vetting is conducted. APIS Pre-Departure final rule, 72 FR at 48323, 48329.

*Comment:* Some commenters suggested that TSA did not fulfill the aim of the "One DHS Solution," because Secure Flight would create a process for watch list matching that differs from the process already under implementation by the airlines for APIS Pre-Departure programs and systems. These commenters suggested that the Secure

Flight requirements would obstruct processing recently put into place and require further investments by the covered aircraft operators to update systems and processes. Several aircraft operators requested that Secure Flight further align the two programs. Specifically, aircraft operators suggested that Secure Flight require the same data elements and data transmission timeframe as APIS in order to avoid the time and cost associated with updating their systems twice. Several commenters also requested that TSA align requirements with CBP so that aircraft operators are only required to submit one data transmission to DHS and receive one response in return.

*TSA Response:* TSA has worked with CBP to align the Secure Flight and APIS Pre-Departure programs and systems. TSA and CBP jointly created the Consolidated User Guide to standardize requirements and minimize the impact to aircraft operators. In the Consolidated User Guide, TSA provided additional clarification that describes the technical and operational guidance for both programs.

Under the CBP APIS Pre-Departure final rule, aircraft operators are required to send APIS data for international flights to CBP. Secure Flight requires that covered aircraft operators provide SFPD to TSA as outlined in this final rule.

Secure Flight will not necessarily require multiple data transmissions to and responses from DHS. Covered aircraft operators may transmit both APIS data and SFPD in a single transmission to the DHS portal, which will route information to TSA and CBP as appropriate. These covered aircraft operators will receive a single boarding pass printing result in return.

CBP described the procedures for when aircraft operators submit APIS data prior to a passenger's presenting his or her travel document at the airport in its APIS Pre-Departure final rule:

[T]he CBP system has the ability to accept certain passenger data up to 72 hours in advance, including APIS data. Such very early transmissions would be more likely under either of the batch transmission options, as AQQ transmissions are more likely to occur in closer proximity to the time or day of the flight. However, as mentioned previously, any early "cleared" vetting result obtained in this process is considered provisional by CBP until the passport or other travel document is validated, either by the swiping of the travel document's machine-readable zone or through manual verification by the carrier. Successful validation by the carrier of any passenger holding a provisional boarding pass as herein described (i.e., based on early data transmission and early receipt of a "cleared"

response) requires that the APIS passenger data checked during validation be identical to the passenger data transmitted early to obtain the boarding pass. Where the data transmitted differs from data presented at validation, the carrier must transmit the new data and obtain vetting clearance on that data. Until that occurs, the carrier may not allow the passenger to board. 72 FR at 43822.

Additionally, for reservations made within 72 hours of scheduled flight departure time, covered aircraft operators must transmit SFPD as soon as possible. If the covered aircraft operator is also ready to transmit APIS information at that time, the covered aircraft operator will be able to send one transmission for both Secure Flight and APIS and will receive one boarding pass printing result. If the covered aircraft operator is not ready to transmit passenger data under the APIS Pre-Departure final rule at the same time, the covered aircraft operator must transmit the passenger information separately for Secure Flight and APIS.

Once TSA assumes responsibility under Secure Flight for the watch list matching function for the majority of passengers covered by the APIS Pre-Departure final rule, the CBP system will no longer be responsible for pre-departure watch list matching or the issuance of related boarding pass printing results for covered flights. Consequently, covered aircraft operators will receive, and will have to comply with, one result from DHS through TSA regarding the issuance of boarding passes to, or the boarding of passengers on, covered international flights. CBP will, however, continue to require carriers to provide APIS data to carry out its border enforcement mission, and the timing of that transmission will follow that of the Secure Flight program, rather than APIS.

*Comment:* TSA received several comments indicating confusion regarding how aircraft operators will determine the final boarding pass printing result and which program, APIS or Secure Flight, will provide that result throughout different phases of the program.

*TSA Response:* DHS plans to implement watch list matching in stages. Initially, the CBP system will take over watch list matching for all commercial flights into and out of the United States through the APIS Pre-Departure program, and aircraft operators will continue to conduct watch list matching for domestic flights. In the first phase of Secure Flight, TSA will conduct watch list matching for all covered U.S. aircraft operators' domestic flights under the Secure Flight Program. The CBP system will continue to

conduct watch list matching for international flights into and out of the United States.

In the second phase of Secure Flight, TSA will begin to conduct watch list matching for covered aircraft operators' flights that overfly the continental United States. Also in phase two, watch list matching for the remaining covered aircraft operator international flights will be transitioned from the CBP system to TSA under the Secure Flight program. During phase two, if an itinerary contains an international flight on a foreign-based aircraft operator covered by the APIS Pre-Departure final rule with a connecting domestic code share flight on a covered U.S.-based aircraft operator, the aircraft operator will transmit one set of data to DHS and receive one boarding pass printing result. The aircraft operator must comply with this boarding pass printing result. As discussed above, the timing of the aircraft operator's transmission of data to DHS will follow CBP's schedule under the APIS Pre-Departure final rule, until such time as Secure Flight assumes responsibility for international flights under phase two.

### C. Implementation and Compliance

*Comment:* TSA received several comments objecting to the NPRM's requirement that covered aircraft operators comply with the rule within 60 days after the Secure Flight final rule's effective date, or 120 days after publication of the final rule in the **Federal Register**. TSA also received comments that 30 days after the effective date for submission of the AOIP does not provide covered aircraft operators with sufficient time to develop the AOIP. Several commenters proposed various alternatives. Many commenters suggested that Secure Flight align its compliance schedule with CBP's APIS Pre-Departure final rule, which is 180 days from publication of the final rule in the **Federal Register**. Another commenter suggested that TSA provide an 18-month compliance schedule for covered aircraft operators.

*TSA Response:* Based on the comments received on this issue, TSA agrees that full implementation of the collection and data transmission requirements in § 1560.101 within 120 days of publication of this final rule in the **Federal Register** may be difficult, if not impossible, for several covered aircraft operators. Consequently, TSA is changing the implementation timing requirements in § 1560.101 to allow for greater flexibility in implementing the various elements of the Secure Flight program.

Also, TSA is modifying the AOIP adoption process that was originally proposed in the NPRM. Because the primary purpose of the AOIP is to set forth a schedule for compliance with elements of the Secure Flight program for each covered aircraft operator, TSA believes that it is appropriate for TSA, rather than the covered aircraft operator, to develop the AOIP. Therefore, under the final rule, TSA will assume responsibility for drafting the AOIP for each covered aircraft operator and will notify each covered aircraft operator of the proposed AOIP for the covered aircraft operator.

After receiving the proposed AOIP from TSA, the covered aircraft operator will have 30 days to submit written comments on the proposed AOIP to TSA's designated official. This designated official will review the covered aircraft operator's comments and other relevant materials. After consideration of the written submission, the designated official will notify the covered aircraft operator of the AOIP. The AOIP will be effective not less than 30 days after notice is given, unless the covered aircraft operator petitions the designated official or the Assistant Secretary for reconsideration of the AOIP. In no case will an AOIP become effective prior to the effective date of the final rule. When TSA sends the covered aircraft operator their final AOIP, the covered aircraft operator may petition the designated official or the Assistant Secretary for reconsideration of the AOIP no later than 15 days before its effective date. A timely reconsideration petition will stay the effective date of the AOIP. TSA will amend, affirm, or withdraw the AOIP within 30 days of receipt of the petition for reconsideration.

Many commenters stated that TSA did not provide sufficient time for covered aircraft operators and third party agents to make all the necessary technological and process changes to satisfy the requirements of the Secure Flight program. To address this concern, TSA is not requiring covered aircraft operators to be capable of collecting and transmitting all of the SFPD elements at the same time. Instead, TSA will allow them to implement the individual SFPD elements in phases. TSA is not specifying in the rule text the dates by which covered aircraft operators must be capable of collecting and transmitting the different data elements in the SFPD. The covered aircraft operator's AOIP will set forth these specific dates. By including the specific implementation dates in the AOIP, TSA and covered aircraft operators will have flexibility to develop a compliance schedule that

satisfies TSA's security needs to implement Secure Flight expeditiously while taking into account the covered aircraft operators' operations and technology.

The first SFPD element that covered aircraft operators will likely be able to provide is a passenger's full name. Because covered aircraft operators and third party agents currently collect the name as part of their business practice, TSA expects that they will have little difficulty collecting and transmitting full name within 120 days of publication of this final rule in the **Federal Register**. Covered aircraft operators will implement the other SFPD elements such as gender and date of birth in subsequent months in accordance with the AOIP. This approach will allow covered aircraft operators to make their technological changes gradually. However, covered aircraft operators may choose to make all their system changes for the Secure Flight program at the same time provided that the covered aircraft operators are capable of collecting and transmitting the full name within 120 days of publication of the final rule in the **Federal Register**.

TSA anticipates that covered aircraft operators will be capable of collecting and transmitting all of the SFPD elements within nine months of final rule publication in the **Federal Register**, because many covered aircraft operators have already made changes to comply with CBP's APIS Pre-Departure data submission requirements. TSA expects that these covered aircraft operators would be able to use much of the data submission and formatting system functions that they already execute. A small number of covered U.S. aircraft operators do not have international flights and, therefore, did not have to make any changes to comply with the APIS Pre-Departure final rule. TSA anticipates that the majority of the remaining covered U.S. aircraft operators that do not have international routes will use the web-based alternative data transfer mechanism. TSA will assist all covered aircraft operators in their efforts to comply with the Secure Flight requirements.

The AOIP also will set forth the implementation schedule for other aspects of the Secure Flight program such as when the covered aircraft operators will begin transmitting SFPD for covered international flights. Establishing the implementation schedule within the AOIP framework allows for some flexibility with implementation dates, taking into consideration both TSA security needs

and the covered aircraft operators' technological capabilities.

*Comment:* TSA received several comments regarding the Secure Flight implementation phases. One commenter requested clarification as to when foreign air carriers and international flights would be covered in the second phase. One aircraft operator requested a single implementation date for Secure Flight on the ground that it would be less expensive for the aircraft operators than the proposed phased implementation. Many aircraft operators offered suggested implementation timeframes and strategies, including a suggestion to "pilot" Secure Flight with one or two covered foreign air carriers in order to work out any software and operational issues.

*TSA Response:* TSA will conduct extensive testing to confirm and validate the Secure Flight watch list matching results, including benchmark testing with voluntary aircraft operators and a period of parallel testing with covered aircraft operators. TSA plans to resolve software and operational issues during the various phases of testing with participating aircraft operators and will only implement Secure Flight once these issues are resolved. TSA and covered aircraft operators will conduct the extensive testing prior to TSA assuming responsibility for watch list matching and may face operational issues in implementing Secure Flight after testing. Consequently, TSA believes that Secure Flight should be implemented in phases to ensure that the implementation process occurs as smoothly as possible and to minimize disruption of covered aircraft operators' operations and inconvenience to their passengers.

TSA will begin by implementing Secure Flight for U.S. domestic flights operated by aircraft operators required to have a full security program under 49 CFR 1544.101(a) after a period of parallel testing with all covered aircraft operators. The second implementation phase will include covered aircraft operators' flights that overfly the continental United States. TSA will determine the timing of implementing Secure Flight for covered flights that fly to and from the United States after TSA assumes the watch list matching responsibilities for covered U.S. aircraft operators' covered domestic flights. The exact implementation dates for covered aircraft operators will be in their AOIP.

*Comment:* One commenter observed that TSA developed the Secure Flight program tailored for covered U.S. aircraft operators. The commenter is concerned that TSA, in developing Secure Flight, did not take into account

the different systems that foreign air carriers use for their reservation and document control systems.

*TSA Response:* TSA is aware of the existing differences between international and domestic systems and business processes. Secure Flight is working with covered foreign carriers to determine the best way to address these differences during the implementation of the Secure Flight program.

*Comment:* TSA received one comment that stated, "Airlines should be given not less than 60 days notice of the known traveler collection requirement and that travel agents should receive no less than 55 days notice. This approach gives the airlines an ample five days to communicate the requirement to travel agents."

*TSA Response:* TSA understands the concern regarding the coordination of aircraft operator and travel agent systems to allow for entry of the Known Traveler Number. TSA believes that any programming that is required to comply with the Secure Flight implementation should be sufficient to capture Known Traveler Number when it becomes available. Thus, TSA believes that 30 days' notice should be sufficient notification for the inclusion of the Known Traveler Number.

#### D. Secure Flight Passenger Data (SFPD)

##### 1. General

*Comment:* One commenter stated that the U.S. government failed to demonstrate how the scope of the information being required is necessary to carry out the mandate of the Secure Flight program.

*TSA Response:* TSA has chosen a limited data set for use in watch list matching. Based on automated watch list matching test results, TSA has determined that it will be able to complete watch list matching for the vast majority of individuals based on full name, date of birth, and gender. As discussed below, the additional data elements may clear individuals whose names indicate that they are potential matches to individuals on the watch list. The data elements in the SFPD will help prevent passenger misidentification and will allow TSA to more effectively and consistently prevent certain known or suspected terrorists from boarding aircraft.

*Comment:* A commenter stated that the Redress Number, the Known Traveler Number, the Reservation Control Number, the Record Sequence Number, Record type, Passenger update indicator, and the Traveler Reference Number are passenger identifier codes that are used to access subsets of

individual passenger information and are most used for customer service purposes such as special needs request. The commenter questioned the need for TSA to obtain these subsets of individual passenger information.

*TSA Response:* TSA will use the Redress Number and the Known Traveler Number to attempt to distinguish a person who has been identified as a potential match to the watch list. TSA will use the other numbers listed in the comment to manage the SFPD as they are transmitted to and from TSA and are processed through Secure Flight to ensure that results are matched correctly with the appropriate SFPD and that results are transmitted to covered aircraft operators timely and accurately. Under the Secure Flight program, covered aircraft operators will transmit or "push" SFPD to TSA and TSA will not access or "pull" information from the covered aircraft operators' systems. Thus, TSA will not use the numbers to pull the subsets of individual passenger information from the covered aircraft operators' systems.

*Comment:* TSA received one comment expressing a concern that domestic passengers may be required to submit the same data that is required for international flights.

*TSA Response:* TSA will require covered aircraft operators to request a passenger's full name, gender, date of birth, and Redress or Known Traveler Number (if known). Unlike flights subject to APIS Pre-Departure, TSA will not require covered aircraft operators to request or collect passport information from individuals. However, if covered aircraft operators collect passport information for passengers, then they must transmit that information to TSA. For example, if a passenger has a flight itinerary that includes a domestic flight that connects to an international flight, the passenger may provide passport information along with his or her full name, date of birth, and gender when he or she purchases a ticket for the domestic and international flights. In this situation, the covered aircraft operator must transmit the passport information to TSA along with the other data elements in the SFPD.

*Comment:* TSA received several comments requesting clarification of the term "passenger," and whether the term includes crew members who are not on duty.

*TSA Response:* TSA is changing the definition of "passenger" as proposed in the Secure Flight NPRM to exclude employees of aircraft operators who are identified as crew members on the

manifest for that flight. TSA's Crew Vetting program conducts watch list matching of individuals who are on the manifest as crew members.<sup>22</sup> The Secure Flight program will conduct watch list matching of all other employees, including crew members traveling as passengers and not identified as crew on the manifest.

*Comment:* A commenter was concerned about Secure Flight's impact on travelers engaged in unique religious and cultural activities.

*TSA Response:* TSA appreciates and respects both religious and cultural diversity. As such, the Secure Flight program will match travelers to entries on the TSDB without prejudice, placing no specific emphasis on any particular religion. With this approach, the limited information that individuals must provide, and the ability of the Secure Flight program to respond to last minute SFPD transmissions, the Secure Flight program is not likely to impact unique religious and cultural activities.

*Comment:* Several commenters requested clarification on the requirement for an aircraft operator to validate the underlying accuracy of the collected passenger information on covered domestic flights or non-traveler information.

*TSA Response:* The Secure Flight final rule mandates that covered aircraft operators request SFPD, but that they need not validate the accuracy of that information beyond rules currently governing verifications of biographic data of international passengers. TSA would not hold a covered aircraft operator responsible or subject the aircraft operator to enforcement action if the information provided by a passenger is found to be inaccurate unless the covered aircraft operator knowingly provided the inaccurate information to TSA.

*Comment:* TSA received one comment that requested clarification on how to record consumer refusals to provide optional SFPD.

*TSA Response:* TSA does not require a record of an individual's refusal to

provide optional elements of the SFPD when the covered aircraft operator initially requests the information.

*Comment:* A commenter expressed concern that TSA may change the required data elements in the SFPD after operational testing because covered aircraft operators will have already made system changes based on this final rule by the time they undergo operational testing.

*TSA Response:* TSA understands this concern based on the Secure Flight NPRM. The SFPD elements in this final rule will not change as a result of operational testing.

*Comment:* Several comments requested that TSA clarify SFPD transmission requirements and the format for full name, date of birth, and gender in the final rule. Several commenters requested that all formats be standardized to ensure ease of collection and transmission to TSA.

*TSA Response:* TSA developed transmission requirements and the standard formats for the SFPD elements in the Consolidated User Guide. TSA will provide the Consolidated User Guide to all covered aircraft operators.

## 2. SFPD Is Not Passenger Name Record (PNR)

*Comment:* TSA received comments expressing concern about the potential improper use of a Passenger Name Record (PNR). Many commenters mistakenly believed that SFPD is PNR or a subset of PNR. TSA also received a comment stating that PNR is already provided to CBP 72 hours prior to departure and should be sufficient for extraction by TSA for Secure Flight watch list matching.

*TSA Response:* TSA is not requiring covered aircraft operators to submit PNR, and TSA will not have direct access to PNR. Instead, TSA is requiring covered aircraft operators to submit SFPD which is a separate set of data elements. Covered aircraft operators may choose to extract the data elements from the PNR to create the SFPD for operational reasons. TSA, however, is not mandating that they do so nor is it mandating where covered aircraft operators store SFPD. Covered aircraft operators may choose to create a separate system to collect and store SFPD. CBP has access to PNR under a separate regulatory requirement.

*Comment:* A commenter expressed concern that TSA will require covered aircraft operators to include an individual's nationality in the PNR that would be transmitted to the Secure Flight program.

*TSA Response:* As stated above, TSA is not requiring covered aircraft

operators to include any information in the PNR or to send PNR to the Secure Flight program. Furthermore, TSA is not requiring covered aircraft operators to request or to collect an individual's nationality.

## 3. Date of Birth and Gender

*Comment:* TSA received several comments regarding the inclusion of date of birth and gender as SFPD elements. Some commenters supported date of birth and gender becoming mandatory data elements. One commenter argued that unless TSA mandates the collection of this additional information, many passengers would not be cleared by TSA. Another commenter supported making both elements mandatory, but objected to collecting this data at the time of booking. Other commenters opposed TSA requiring individuals to provide date of birth and gender. Another commenter sought clarification on whether individuals must provide any information other than full name.

*TSA Response:* Through careful consideration of the public comments and both privacy and security concerns, TSA has concluded that it will require full name, date of birth, and gender from individuals under § 1540.107(b). It is expected that these data elements in combination will be sufficient to conduct watch list matching for the vast majority of individuals and to distinguish more persons from individuals on the watch list as part of the automated process reducing instances of misidentification. Reducing misidentification is an important program goal mandated by Congress and collection of all three data elements is an important step in reaching that goal.<sup>23</sup>

*Comment:* TSA received several comments requesting that TSA require covered aircraft operators only to request date of birth and gender if a person is not cleared by submitting only their full name.

*TSA Response:* TSA believes that by requiring the airlines to ask for and passengers to provide the data elements at time of original submission, TSA can make a determination about the boarding pass printing result quickly and efficiently. There would be no need

<sup>22</sup> The Crew Vetting program vets airline crews entering, departing, or flying over U.S. airspace against terrorist-related information to determine if they are a potential threat to the aviation system. It uses computerized risk analysis and manual review of automated vetting results and matching analysis (Vetting Operations) to assess and evaluate potential threats of terrorists posing as cleared aviation or other transportation system personnel. The Crew Vetting program maintains a 24/7 operations center to receive and analyze Flight Crew Manifests (FCM) and Master Crew List (MCL) from the airlines throughout a 24-hour period. These individuals are then vetted against the various watchlists to identify potential security threats prior to an aircraft receiving authorization for departure.

<sup>23</sup> Section 518(a) of the Department of Homeland Security Appropriations Act, 2006, Pub. L. 109-90 (Oct. 18, 2005) (2006 DHS Appropriations Act), requires DHS to certify and purports to require GAO to report that TSA satisfies 10 conditions before TSA may deploy Secure Flight other than on a test basis. One of the conditions is the Secure Flight system "will not produce a large number of false positives that will result in a significant number of passengers being treated mistakenly \* \* \*." Cf. *INS v. Chadha*, 462 U.S. 919 (1983).



for a second transmission that may necessitate the individual going to the ticket counter.

*Comment:* TSA received one comment requesting that TSA eliminate the gender requirement from SFPD information and instead require passengers to submit information regarding their ethnicity, race, or national origin.

*TSA Response:* Many names are gender neutral. Additionally, names not derived from the Latin alphabet, when translated into English, do not generally denote gender. Providing information on gender will reduce the number of false positive watch list matches, because the information will distinguish persons who have the same or similar name. Consequently, TSA is including gender as a required element of the SFPD, which covered aircraft operators must request from individuals and which individuals must provide to the covered aircraft operator.

TSA disagrees that ethnicity, race, or national origin should be included in SFPD information provided by passengers of covered aircraft operators and certain non-travelers seeking access to the sterile area of a U.S. airport. Secure Flight matches names of passengers to entries on the TSDB without prejudice or regard to an individual's race, ethnicity, or national origin.

#### 4. Redress Number and Known Traveler Number

*Comment:* TSA received several comments requesting that the final rule clarify the handling of Redress Numbers and Known Traveler Numbers. Some commenters expressed opposition to the Secure Flight requirement for requesting these two numbers.

*TSA Response:* Individuals who believe they have been incorrectly delayed, identified for enhanced screening, denied boarding, or denied access to a U.S. airport's sterile area may apply for redress through DHS TRIP. DHS will assign a unique Redress Number to each individual who uses DHS TRIP. Individuals who have already undergone TSA's redress process do not need to use DHS TRIP to reapply for redress once the Secure Flight program is operational. Individuals will be less likely to be delayed by misidentification as a match to the watch list if they provide their Redress Number at the time they make a flight reservation or request access to a U.S. airport's sterile area. While TSA requires that each covered aircraft operator request a Redress Number, TSA does not require individuals to provide

a Redress Number when making a reservation for a covered flight.

TSA intends to develop and implement the Known Traveler Number as part of the Secure Flight program. Like the Redress Number, the Known Traveler Number is a unique number assigned to "known travelers" for whom the Federal government has already conducted terrorist security threat assessments and has determined do not pose a terrorist security threat. The Known Traveler Number may draw upon information from programs such as the Transportation Worker Identification Card program. Once TSA has determined the details of the Known Traveler Number program, it will inform covered aircraft operators that they must begin to request and transmit the number, if provided by the individual. The covered aircraft operators must do so in the time specified in their AOIP.

Similar to other optional information, TSA will not compel individuals to provide a Redress Number or a Known Traveler Number upon request from the aircraft operator. Without either of these numbers, the individual may be more likely to experience delays, be subjected to enhanced screening, be denied boarding, or be denied access to a U.S. airport's sterile area.

*Comment:* TSA received several comments indicating support for the development and implementation of the Known Traveler Number. TSA also received several comments against the requirement for Known Traveler Number as they claim it would be redundant. Several commenters also suggested integration of the Known Traveler Number with existing registered traveler schemes and with future plans between the U.S. and other foreign governments. They suggested that TSA relate Known Traveler Numbers for other groups of individuals, including those with national security clearances or members of the U.S. or foreign governments. Another commenter suggested that the name of the Known Traveler Number be changed to "Cleared Passenger Number" to more accurately identify those individuals who participate in the program.

*TSA Response:* TSA assures these commenters that all possible solutions for the Known Traveler Number will be considered during development efforts. At this time, however, TSA is unable to comment on whether the Known Traveler Number will be fully integrated with existing credentialing programs or future domestic or international programs. Although "Cleared Passenger Number" is a possible alternate name, TSA prefers "Known Traveler Number"

because the number is assigned to individuals "known" to the government through the credentialing program. Finally, TSA has not determined which individuals or programs will be included under the Known Traveler Number but will continue to consider the proposed inclusion of certain groups.

*Comment:* A commenter questioned whether or not TSA would continue to conduct watch list matching for known travelers. The commenter argued that if this watch list matching does occur, it would be redundant and unnecessary.

*TSA Response:* TSA intends to continue to conduct watch list matching for individuals who provide a Known Traveler Number for covered flights to ensure that the individuals' Known Travel Numbers have not expired or been revoked.

*Comment:* A covered aircraft operator stated that it will not be able to request the Known Traveler Number from passengers who made their reservation before TSA issued the 30-day written notice to them.

*TSA Response:* TSA will not require covered aircraft operators to request the Known Traveler Number for reservations made before TSA implements the Known Traveler Number program.

*Comment:* TSA received several comments regarding the requirement in proposed § 1560.101(a) prohibiting covered aircraft operators from accepting a reservation from an individual who did not provide all the required information at the time of booking. The commenters provided examples such as when an individual or a tour operator is making a reservation for a large group and does not have access to every individual's full name or passport information.

*TSA Response:* The reason for proposed § 1560.101(a) was to ensure that the Secure Flight program receives full names to conduct effective watch list matching. TSA does not intend for the Secure Flight program to impact current business practices regarding the blocking of group space without complete passenger information. TSA is changing the language in proposed § 1560.101(a) to provide that covered aircraft operators may not submit a SFPD for an individual until the individual provides his or her full name, date of birth, and gender; the regulation does not prohibit covered aircraft operators from accepting a reservation without a full name, date of birth, and gender. Once a covered aircraft operator receives the full name, date of birth, and gender associated with the blocked or group space, the aircraft

operator must transmit that SFPD to TSA in accordance with this final rule. Additionally, TSA has designed the data transmission processes to receive changes and updates to these data elements.

This change will still ensure that individuals do not receive a boarding pass or authorization to enter a sterile area without TSA's conducting watch list matching based on a full name, date of birth, and gender at a minimum. Also, the only data elements that passengers must provide are full name, date of birth, and gender; other optional information, such as passport information, does not need to be included as part of the SFPD.

#### E. Watch List Matching Process

##### 1. Transmission of SFPD

*Comment:* Numerous airlines commented that Secure Flight requires data not currently contained in the airlines' systems or incorporated in the UN-EDIFACT message standards. The UN-EDIFACT is the international electronic data interchange (EDI) standard developed under the United Nations for inter-industry electronic interchange of business transactions. Many commenters expressed concern that the requirements for collection and transmission of SFPD do not follow international standards.

*TSA Response:* TSA recognizes that programming will be required to add additional data to airline systems, but TSA has diligently limited the data requested to the minimum required to support the security processes and to provide the transactional support required for airlines to apply the boarding pass printing result provided by Secure Flight. As part of the implementation of APIS Pre-Departure, CBP has defined the additional fields for UN-EDIFACT transmissions and the Secure Flight program will use that message format. DHS has identified and harmonized the modifications to UN-EDIFACT messaging standards for these additional data with those required for APIS Pre-Departure systems. TSA will coordinate with the appropriate worldwide standards bodies, as required.

*Comment:* Several commenters expressed concern that Secure Flight would be unable to efficiently process the transactions resulting from airline passenger travel, especially during periods of irregular operations and passenger re-accommodation.

*TSA Response:* TSA understands the need for Secure Flight to efficiently process transactions, especially during periods of irregular operations and

passenger re-accommodations. In developing Secure Flight, TSA has accounted for the additional transmission volume associated with changes in passenger travel information, resolution of boarding pass printing results, and changes caused by irregular operations or passenger re-accommodation. All of these factors contributed to the design decision to require that covered aircraft operators provide available SFPD 72 hours in advance of flight departure. This advance booking information allows Secure Flight to increase real time resources available to respond to off schedule operations and passenger re-accommodation and to process SFPD for passengers who make reservations within 72 hours of the scheduled departure of the flight.

*Comment:* One aircraft operator commented that TSA should not dictate when, and from which system, the airline sends SFPD to TSA.

*TSA Response:* TSA does not specify the system from which a covered aircraft operator must transmit SFPD, and covered aircraft operators may choose the appropriate system from which to transmit SFPD. However, obtaining passenger data in advance is an integral part of the Secure Flight watch list matching process; it is designed to optimize the number of boarding pass printing results available to the covered aircraft operator prior to passenger check-in. The rule specifies that a covered aircraft operator must submit the SFPD to TSA beginning 72 hours before departure or as soon as it becomes available.

*Comment:* Several airlines expressed concern that the Secure Flight response time would adversely affect their passenger check-in processes and levels of customer service.

*TSA Response:* Secure Flight's requirement for advance transmission of SFPD is designed to provide a boarding pass printing result prior to passenger check-in. Secure Flight has made considerable investments to ensure a prompt response.

*Comment:* Several airlines and airline associations expressed concern that even a short outage of the Secure Flight system would severely impact airline operations.

*TSA Response:* TSA designed Secure Flight technical operations with geographic and component redundancy to provide for continuous, uninterrupted operations. Covered aircraft operators will receive boarding pass printing results for a majority of passengers beginning 72 hours before flight departure. TSA believes the number of individuals affected by a

significant short term outage with multiple redundancy failures would be comparatively small and likely limited to those passengers making last minute reservations or changes. The Consolidated User Guide includes a comprehensive plan to address processes and procedures for outages.

##### 2. 72-Hour Requirement

*Comment:* TSA received several comments about the requirement to submit SFPD to Secure Flight beginning 72 hours before departure and the potential impact to travelers who make last minute reservations or changes.

*TSA Response:* Secure Flight will perform watch list matching on all reservations for covered flights operated by covered aircraft operators regardless of when the reservation is made. TSA is not requiring that individuals make their reservations or purchase tickets 72 hours or more before departure. In this final rule, TSA describes two scenarios whereby a covered aircraft operator must submit SFPD to Secure Flight. The first is when a covered aircraft operator accepts a reservation with a full name, date of birth, and gender earlier than 72 hours before departure. In this situation, the covered aircraft operator must transmit the SFPD to Secure Flight 72 hours in advance of departure. The second scenario occurs when a covered aircraft operator accepts a reservation within 72 hours of departure, updates a TSA-requested SFPD within 72 hours of departure, changes a flight within 72 hours of the departure time, or seeks to authorize individuals to enter a sterile area upon arrival at the airport. For those reservations or requests, the covered aircraft operator must transmit the SFPD to Secure Flight as soon as the SFPD is available.

*Comment:* TSA received several comments from covered aircraft operators who indicated that they have two systems: A reservation system and a departure control system (DCS). These commenters, predominantly covered foreign air carriers, are concerned that Secure Flight does not take into account that their reservations system does not store all SFPD elements and that their DCS often captures SFPD elements at check-in when the individual's passport is swiped. Several comments noted that covered aircraft operators would incur costs to program their reservation systems to accept SFPD. Some covered aircraft operators indicated that they cannot transmit UN-EDIFACT messages from their reservations system; they can only be transmitted from their DCS. Many commenters also expressed concern that TSA will return a boarding pass printing result to the incorrect

system, and passengers may experience difficulties in obtaining a boarding pass.

*TSA Response:* TSA understands the concerns raised by these covered aircraft operators. The Secure Flight program is developing a solution for covered aircraft operators that have separate reservations systems and DCS as described in the comments. The solution will support the covered aircraft operators' systems as well as the transmission and boarding pass printing requirements in this final rule.

*Comment:* TSA received several comments questioning TSA's requirement that SFPD transmission begin 72 hours in advance considering that CBP is willing to accept data up to departure time.

*TSA Response:* TSA considered a number of factors in determining that covered aircraft operators should submit SFPD to TSA beginning 72 hours before departure time. The CBP system will conduct watch list matching only for covered flights that involve a flight to or from the United States. When TSA assumes watch list matching, the Secure Flight program will conduct the watch list matching for (1) all flights conducted by U.S. aircraft operators (including flights between two international points); (2) flights operated by foreign air carriers that fly to or from the United States or overfly the United States; and (3) non-travelers who are seeking authorization to enter a sterile area. While TSA believes that the automated process alone for vetting this significantly larger population of travelers may not take 72 hours, several factors that suggest a 72-hour lead time is appropriate. These include the volume of data involved, the increase in records requiring a manual review due to a potential match or an insufficient amount of information to differentiate someone from an individual on the watch list, and the time required to coordinate an operational response when necessary.

By requiring covered aircraft operators to transmit available SFPD 72 hours prior to departure, TSA will be able to prioritize SFPD by departure time. This prioritization will permit TSA to return boarding pass printing results for the vast majority of passengers in time for them to print their boarding passes 24 hours in advance of their flights while also returning boarding pass printing results for individuals who make reservations within 72 hours of the scheduled departure in time for them to obtain their boarding passes prior to the scheduled departure.

TSA understands that a certain amount of expense is involved in

making programming changes for Secure Flight. TSA believes, however, that the security benefit to covered aircraft operators and passengers is such that the 72 hour requirement is a necessity.

*Comment:* A few commenters expressed concern that there will be a number of changes to reservations within the 72 hour period that will require messaging back and forth between the covered aircraft operator and TSA. The commenters suggest that reducing the time from 72 hours to something less than 72 hours will reduce the need for such messages.

*TSA Response:* TSA believes that, on average, an overwhelming majority of reservations become stable at 72 hours before departure time. However, TSA understands that there are still some reservations that continue to change within the 72 hour period. As explained above, TSA believes that the security benefits to covered aircraft operators and passengers of providing SFPD for passengers who have made their reservations more than 72 hours before departure time are important enough to require this timeframe.

### 3. Boarding Pass Issuance

*Comment:* Several commenters argued that prohibiting covered aircraft operators from issuing a boarding pass until they receive a boarding pass printing result from TSA would unnecessarily impact the check-in of connecting passengers, specifically those inbound to the United States who are connecting/transferring through airports outside of the United States.

*TSA Response:* In the United States, the boarding pass is used to designate to personnel at the security checkpoint whether passengers are permitted to enter the sterile areas and whether passengers must first undergo enhanced screening. TSA recognizes that, outside the United States, access and enhanced screening are determined by the applicable operating authority of the airport. In some international airports, passengers may transit from one international flight to another where the flights are operated by different aircraft operators; only the second flight would be covered under this final rule. TSA understands that currently, in these situations, the aircraft operator operating the first, non-covered flight may issue a boarding pass for both legs of the passenger's itinerary, including the covered flight to the United States.

Accordingly, TSA has modified § 1560.105(b) to allow for the issuance of connecting boarding passes inbound to the United States for connecting passengers without complying with the

requirements regarding boarding pass printing result in § 1560.105(b). Under the Secure Flight program, the aircraft operator operating the first, non-covered flight is able to issue a boarding pass for the second, covered flight without obtaining a boarding pass printing result from TSA. The second aircraft operator, however, must submit SFPD or APIS data to DHS and confirm the boarding pass printing results prior to permitting the passenger to board the aircraft for the covered flight. The covered aircraft operator must comply with the measures in its security program to prevent the boarding of any individual who is identified as a No Fly match by TSA and to ensure that any passenger TSA identifies as a Selectee undergoes enhanced screening prior to boarding the aircraft. These conditions mitigate the security vulnerability associated with issuance of a boarding pass for covered flights outside of the Secure Flight program. These provisions will also apply to passengers whose connecting flight is a covered overflight.

*Comment:* One aircraft operator recommended that TSA eliminate the requirement for applying the Secure Flight requirements on subsequent connecting flights.

*TSA Response:* TSA believes that the elimination of the watch list matching requirements on subsequent connecting flights is inconsistent with the security mandate of Secure Flight. One of the benefits of the Secure Flight program is that any update to the watch list will be compared against all active SFPD. This update comparison will allow TSA and the covered aircraft operators to take appropriate action regarding any passenger whose status changes during his or her travel.

*Comment:* A commenter requested that TSA clarify the provision "that carriers can choose to designate a more restrictive boarding pass status in conjunction with other TSA or aircraft operator procedures." Secure Flight NPRM at 48374.

*TSA Response:* Covered aircraft operators must designate passengers for enhanced security screening for reasons unrelated to watch list matching pursuant to a TSA security directive such as the Computer Assisted Passenger Prescreening System (CAPPS). TSA will continue to require aircraft operators to conduct these programs once Secure Flight is implemented and a passenger may receive a more restrictive boarding pass status based on the results of these other programs. Also, TSA recognizes that covered aircraft operators may designate a more restrictive boarding pass status

based on their own policies and procedures.

*Comment:* A few commenters supported the implementation of bar codes on boarding passes to authenticate the boarding passes, because it will enhance security in the sterile area. Another commenter stated that the inability to authenticate boarding passes minimizes the benefits of the Secure Flight program. The commenter argues that Secure Flight should not be implemented until this security issue is adequately addressed.

*TSA Response:* As one commenter noted, bar codes on the boarding pass will address the security issue of altered or fraudulent boarding passes. TSA is developing the protocols and standards for placing a bar code on boarding passes and the requirement for covered aircraft operators to place the code on their boarding passes is part of this final rule in §§ 1560.105(b) and (c). When TSA updates the Consolidated User Guide with the protocols and standards for the code, covered aircraft operators must implement this requirement in accordance with their AOIP.

*Comment:* Several airlines requested additional clarification on the bar code requirements. Some commenters raised concerns that bar code requirements would be costly to implement. Many commenters suggested that TSA take advantage of existing bar code standards such as the International Air Transport Association standards and business processes. The commenters also requested more information about how TSA would intend to use the bar code in addition to any verification procedure.

*TSA Response:* TSA recognizes the importance and potential impact of requiring bar codes to be placed on boarding passes. As stated above, TSA believes that bar codes are an important security measure to authenticate boarding passes. TSA is continuing to research new and existing technologies to develop a technologically sound solution that meets the TSA mission and budgetary requirements and minimizes impacts to aircraft operators. TSA will take into consideration the IATA bar code standard in developing its protocols and standards to determine the most effective solution that meets the TSA mission.

*Comment:* Several commenters noted that the airline industry was seeking alternatives to the traditional paper boarding pass. They expressed concern that Secure Flight would hinder innovation in this respect.

*TSA Response:* Secure Flight uses "boarding pass" to refer to an entitlement for aircraft enplanement

issued by an aircraft operator. TSA will consider alternative means of conveying that boarding entitlement, subject to specific requirements like bar coded information. This final rule refers to the issuance of "a boarding pass or other authorization" thereby providing for alternatives to paper boarding passes.

*Comment:* TSA received comments suggesting that TSA should inform passengers and non-traveling individuals of their boarding status at the checkpoint, rather than send boarding pass printing results to the covered aircraft operators.

*TSA Response:* TSA believes that moving this process from the individual aircraft operators to the security checkpoint will create unacceptably long lines at the checkpoint, will cause unnecessarily lengthy delays for individuals who are not a potential match to the No Fly or Selectee lists, and will cause travelers to miss flights.

*Comment:* TSA received comments requesting that TSA not include in the Secure Flight program a provision for enhanced screening of randomly selected cleared passengers.

*TSA Response:* TSA believes that randomly selecting individuals for enhanced screening is an important layer of security and adds unpredictability to the screening process. While the current CAPPs program includes a random selection element, TSA does not anticipate that Secure Flight will initially include a random selection element. TSA may, however, include a random selection element to Secure Flight as part of its continuous efforts to review and improve its screening procedures.

*Comment:* One aircraft operator commented that the Secure Flight Service Center should be adequately and continuously staffed.

*TSA Response:* The Secure Flight Service Center will be staffed 24-hours a day, 7-days a week to receive telephone calls from covered aircraft operators' staff and assist in the clearance of inhibited passengers. If additional information such as a physical description is required, covered aircraft operators' staff would provide that information during a conversation with Secure Flight Service Center personnel.

*Comment:* Several commenters suggested that TSA expand the period in which boarding passes can be issued to a period greater than 24 hours prior to scheduled flight departure.

*TSA Response:* While TSA appreciates that covered aircraft operators and passengers would prefer greater advance boarding pass issuance, expansion of the advance time period

for boarding pass issuance increases the potential that changes to the watch list will not be correctly reflected in the traveler's boarding pass. This potential for inaccurate boarding passes may create additional security and operation exposure. Therefore, TSA does not plan to expand the authority to issue boarding passes beyond 24 hours prior to the scheduled flight departure.

*Comment:* A commenter objected to a perceived restriction to issuance of a "single boarding pass."

*TSA Response:* The Secure Flight NPRM and final rule contain no restriction on the issuance of duplicate or replacement boarding passes. The rule provides for a "single boarding pass printing result" in those cases in which a passenger itinerary would result in a watch list evaluation by both TSA and CBP.

#### 4. Passenger Resolution

*Comment:* TSA received several comments requesting further information about the provision of PRI by aircraft operators for those passengers to whom TSA has provided an inhibited boarding pass printing result. A few commenters question the need for this requirement. Some commenters suggested that TSA should not require the PRI to be transmitted electronically or it should be eliminated altogether.

*TSA Response:* TSA may require covered aircraft operators to provide PRI for individuals who have been identified as a potential match to the watch list. Without the PRI, individuals for whom TSA has returned an inhibited status result will not be able to obtain a boarding pass, because TSA would not have the means to distinguish that individual from the individual on the watch list.

In the event that it is necessary to collect additional information when there is a potential watch list match, including certain physical description information about the passenger, the covered aircraft operator will contact the Secure Flight Service Center and provide the information. Covered aircraft operators will provide PRI, including physical description information, to TSA only via a telephone call to the Secure Flight Service Center. TSA is not requiring PRI to be transmitted electronically.

*Comment:* TSA received one comment asking if a foreign passport is the only foreign document that is acceptable to TSA for VID purposes.

*TSA Response:* The definition of VID in § 1560.3 includes a valid, unexpired passport issued by a foreign government. TSA has determined that,

at this time, an unexpired foreign passport is the only document issued by a foreign government that can serve as a VID. This is because the process of issuing the passport involves procedures for verifying the identity of the individual. Also, passports universally contain required identifying information, such as full name, date of birth, and a photograph of the individual. TSA, however, may authorize covered aircraft operators to accept other foreign documents as valid VIDs.

#### 5. Use of the Terrorist Screening Database (TSDB)

*Comment:* Several commenters expressed a concern that the watch lists used by Secure Flight contain errors and inaccuracies. One of these commenters further stated that using the watch lists would not expedite the pre-boarding process or improve transportation security.

*TSA Response:* TSA seeks to ensure that data used in the watch list matching process is as thorough, accurate, and current as possible. TSA has worked with the Terrorist Screening Center (TSC) to review the No Fly list name by name, and many names have been removed; a similar process for Selectee names is ongoing. TSA continues to be committed to eliminating erroneous and out-of-date information from the watch list matching process. DHS TRIP will facilitate the redress process for Secure Flight. DHS TRIP provides the opportunity for individuals who believe that they have been delayed or prohibited from boarding or denied entry to the airport sterile area as the result of the Secure Flight program to seek redress and relief.

*Comment:* TSA has received several comments on the proposed requirement to use a larger subset list in the Terrorist Screening Database (TSDB) when the threat level changes in a particular airport, airline, and/or region in the United States. The commenters were concerned that the use of a larger list to select a particular group of travelers would be based solely on nationality.

*TSA Response:* During normal Secure Flight operations, the watch list check will consist of the No Fly and Selectee components of the TSDB. TSA will only use a larger list when warranted for security purposes, such as intelligence that terrorists are targeting a specific route. The decision to use the larger list will not be based on nationality.

*Comment:* TSA received one comment expressing concern that TSA's use of the watch list would result in

individuals with criminal records being arrested.

*TSA Response:* The watch list identifies individuals with a nexus to terrorism. We believe that the commenter's concern about those with criminal records without a nexus to terrorism is a misunderstanding of the mission of Secure Flight.

#### 6. Non-Traveling Individuals

*Comment:* TSA received several comments regarding the issuance of gate passes for non-traveling individuals and the collection of these individuals' data for Secure Flight purposes. Many international carriers expressed a concern that their systems are not capable of capturing such data and asserted that the function of collecting non-traveler data and issuing gate passes should remain in the hands of airports or other authorities. A commenter suggested that TSA provide a manual alternative for covered aircraft operators to provide the non-traveler information to Secure Flight. Furthermore, several foreign air carriers believe it is outside of the purview of TSA's authority to require such data collection and submission for airports outside of the United States. Commenters also argued that submission of information for non-travelers should be the responsibility of airport authorities.

*TSA Response:* TSA is clarifying that the requirement to submit information on non-travelers seeking entry to a sterile area is limited to airports within the United States. Moreover, TSA recognizes that covered aircraft operators' systems for collecting non-traveler information vary. Thus, while covered aircraft operators may create an SFPD for the non-traveler in their systems and submit the information in the same manner that they submit SFPD for passengers, they are not required to do so. They may instead opt to submit the information in a manner that is consistent with their particular system and business practices for collecting non-traveler information. TSA also is developing an alternative method for covered aircraft operators to submit information for non-travelers through the internet.

*Comment:* A commenter expressed concern that the Secure Flight NPRM fails to adequately address the needs of non-travelers to be quickly provided access to an airport's sterile area, because it will be difficult for the covered aircraft operator to advise non-travelers that they must provide their personal information 72 hours in advance.

*TSA Response:* Covered aircraft operators may submit a non-traveler's information to TSA at any time before departure or whenever that individual wishes to access the sterile area. Furthermore, aircraft operators also have the option of using the alternative data transfer mechanism, such as a web-based alternative, for non-travelers who must be vetted and need a response quickly.

#### 7. General Comments

*Comment:* TSA received a number of comments about Secure Flight's ability to reduce false positives. TSA received a comment that suggested that the only improvement as a result of implementing Secure Flight is that a significant effort has been made to reduce false positives. Another commenter suggested that better use of a "cleared list" in the existing process alone would be sufficient to reduce false positives. One commenter questioned the capability of the Secure Flight watch list matching process to distinguish between similar sounding names, and argued that this could result in more false positives. Another commenter suggested that travelers who have been previously misidentified (false positives) would benefit from enrollment in the Registered Traveler program.

*TSA Response:* TSA agrees that a significant benefit of Secure Flight watch list matching is the expected outcome of relatively few misidentified passengers (or false positive matches). We disagree with those comments that suggest TSA retain the current system. In addition to meeting the IRPTA requirement that the government assume watch list matching from the airlines, we believe that Secure Flight brings needed consistency to the watch list matching process that does not exist currently, including more consistent application of the cleared list. With this consistency, there is the expected outcome of a low number of false positive matches.

*Comment:* A commenter expressed concern that the Secure Flight NPRM does not state that Secure Flight will supersede any current TSA security directives that require carriers to match their passengers against the watch lists. The commenter feels that this leaves carriers unable to comply with both conflicting regulations.

*TSA Response:* TSA will update security directives and programs to make them consistent with the Secure Flight regulation.

*Comment:* The commenter asks what the procedures will be for law enforcement officials to question an

individual who is a potential match to the No Fly List in a foreign country.

*TSA Response:* Today, foreign air carriers perform watch list matching and contact the TSA Office of Intelligence (OI) to resolve any potential No Fly matches. In the future, foreign air carriers will contact the Secure Flight Service Center to resolve any potential No Fly matches. Secure Flight does not change existing procedures related to law enforcement officials' involvement in questioning individuals.

*Comment:* A commenter asked what procedures will be in place to ensure other airlines are alerted when an identified No Fly passenger has attempted to purchase a ticket on an airline within a certain region.

*TSA Response:* TSA is sensitive to the commenter's concern about an identified No Fly individual attempting to purchase a ticket from one carrier after being refused by another. One of the benefits of Secure Flight is the consistency it will provide. In this scenario, TSA will send an inhibited response back to the covered aircraft operator when that operator submits the SFPD for the individual.

*Comment:* TSA received a comment requesting that the Secure Flight final rule not require repetitive requests for information for subsequent flights by the same passenger.

*TSA Response:* TSA requires covered aircraft operators to request passenger information and to submit a SFPD for each passenger on every covered flight. Covered aircraft operators may program their systems to store passenger information for future use to alleviate the burden on passengers to input the passenger information every time they make a reservation or purchase a ticket. Covered aircraft operators may also program their systems to automatically use the stored information to populate the SFPD data fields for future flights. TSA is not mandating that covered aircraft operators program their systems in this manner. If they choose, however, to use systems that automatically populate the fields in their reservation system, TSA is requiring covered aircraft operators to submit passenger information that is automatically entered into the SFPD.

## F. Privacy

### 1. General Comments

*Comment:* TSA received comments stating that U.S. carriers should not be subjected to conflicting privacy data requirements between the U.S. Government and foreign governments.

*TSA Response:* SFPD is security data provided pursuant to government

directive and typically exempted from data privacy requirements around the world.

*Comment:* Several commenters expressed a concern with the Federal government collecting any data from U.S. citizens flying domestically.

*TSA Response:* The threat to aviation security exists for both domestic and international flights and watch list matching of passengers on these flights is an important security measure. TSA has carefully selected the minimal personal information that TSA believes is necessary to conduct effective watch list matching for aviation security and is collecting it only for watch list matching purposes.

### 2. Required Privacy Notice

*Comment:* TSA received several comments objecting to providing the privacy notice outlined in this final rule.

*TSA Response:* While TSA appreciates the concerns posed by these commenters, TSA has deemed sufficient privacy notice to passengers a key element of the program in order to ensure passengers are adequately aware that their data will be shared with the government. TSA will also develop a public awareness campaign to educate the traveling public regarding information collection and TSA's use of that information.

*Comment:* TSA received several comments suggesting that TSA take into account that privacy notices are already a requirement of European law and the wording is provided by data protection agencies in European Union (EU) Member States.

*TSA Response:* This final rule requires covered aircraft operators to use specific language to provide the complete privacy notice, unless TSA approves alternative language. For instance, if a governmental entity or entities develops a common privacy notice for use for international flights, that common privacy notice may be approved for use in lieu of the privacy notice specified in this final rule. Individuals who wish further information with respect to TSA's privacy policies should refer to TSA's Web site. The proposed privacy notice requirement applies to all passengers who travel and who will be screened by Secure Flight, not just individuals traveling to/from EU member states.

The privacy notice in this final rule does not affect the covered aircraft operators' responsibilities under other countries' laws or regulations regarding notice and consent. In addition to the requirements in 49 CFR 1560.103, covered aircraft operators should

comply with any notice and consent requirements of other countries, such as Canada, in which they operate.

*Comment:* TSA received several comments expressing a concern that enforcing third parties' inclusion of a privacy notice on their Web sites or elsewhere cannot be controlled by covered aircraft operators.

*TSA Response:* TSA believes that privacy is an important component of the Secure Flight program. Because of its importance, TSA is requiring covered aircraft operators to post the privacy notice on their Web sites and on Web sites of third parties if the third party's Web site is capable of creating a reservation for the covered aircraft operator's reservation system. This comment is closely related to comments indicating that covered aircraft operators cannot require third parties to collect the required SFPD when they sell tickets for the covered aircraft operators' flights. As stated above in response to this comment, TSA believes that it is reasonable to expect that covered aircraft operators will include a requirement that the third parties post the privacy notice on their Web sites in agreements with third parties that have Web sites capable of making a reservation for covered aircraft operators' reservation systems.

*Comment:* A commenter argued that the privacy notice must be provided to individuals prior to collection of SFPD.

*TSA Response:* TSA seeks to have the privacy notice provided through a layered approach to reach the greatest number of passengers practicable. TSA is requiring covered aircraft operators to make the privacy notice available on their Web sites and to ensure that third parties that maintain Web sites capable of making a reservation for the covered aircraft operators' reservation system also make the privacy notice available on their Web sites. TSA will also post the privacy notice on its Web site. TSA believes that making the privacy notice available on Web sites is the most cost-effective and efficient method for providing notice. Requiring covered aircraft operators to provide the privacy notice for individuals who make reservations via the telephone, through a travel agent, and via other non-internet based methods would be costly and burdensome.

*Comment:* TSA received a comment requesting clarification on how covered aircraft operators should comply with the privacy notice requirement. The comment stated that the NPRM did not provide any guidance regarding how to manage the display and traveler acknowledgement of the privacy notice, when the privacy notice is required to

be shown (one time or during each subsequent reservation made by that traveler) and, where the notice must be shown.

*TSA Response:* The PIA TSA published in conjunction with the NPRM as well as this final rule explains that, prior to collecting information from an individual through a Web site or an airport kiosk, a covered aircraft operator must make the privacy notice available to the individual. The aircraft operator can achieve this by posting the privacy notice on its Web site or by providing a link to the TSA Web site.

TSA requested comments from the public on how a privacy notice could be provided during the collection of information through means not identified in section 1560.103 of the NPRM, but did not receive any.

### 3. Privacy Impact Assessment (PIA)

*Comment:* A commenter stated that DHS must address the privacy implications of the Secure Flight program and ensure that it remains within the scope of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).

*TSA Response:* In conjunction with this final rule, DHS is publishing a Privacy Impact Assessment on the DHS Web site at <http://www.dhs.gov> which assesses the privacy impacts of the final rule. TSA will also post the Privacy Impact Assessment on the TSA Web site at <http://www.tsa.gov>. TSA has designed Secure Flight to implement the Fair Information Principles and the Privacy Act<sup>24</sup> to the greatest extent possible. TSA will collect the minimum amount of personal information necessary to conduct effective watch list matching, adding more consistency and efficiency to the process by minimizing false positives and negatives while preventing known and suspected terrorists from boarding an airplane, and will provide notice and choice where possible.

*Comment:* TSA received several comments expressing concern about the requirement that covered aircraft operators submit passenger information stored in their system even though the passenger did not provide the information when he or she made the reservation. One commenter suggested that this requirement is not voluntary submission of personal data and TSA should not require SFPD to be collected in this manner.

*TSA Response:* The requirement to transmit passenger information that is stored but not provided at the time of reservation is limited to covered aircraft

operators that program their systems to automatically use the stored information to populate the SFPD data fields for future flights. TSA notes that individuals may refuse to provide covered aircraft operators with passenger information that is stored for use to populate SFPD fields when making reservations.

This requirement allows TSA to rule out individuals as a watch list match and subsequently precludes that individual from being delayed or denied boarding or access to the sterile area. Reduction of misidentification is an important program goal that can be accomplished with the addition of data passengers have already provided to aircraft operators.

*Comment:* TSA received a comment stating that TSA does not provide adequate assurance that personal information other than that listed in the SFPD will not be collected and stored. The commenter was concerned that, according to the SORN, TSA's database will include communications between TSA and covered aircraft operators and the communications may include information about individuals' belongings screened during secondary screening at the security checkpoint.

*TSA Response:* TSA will employ processes to filter out and prevent any additional personal information beyond what is identified in this final rule as SFPD from being accessible to TSA for use. As a result, the Secure Flight program will only receive the Personally Identifiable Information that would be required under the Secure Flight final rule and described in its PIA. The Secure Flight system will not collect information about an individual's belongings that are screened at the security checkpoint.

The SFPD reflects the minimal amount of personal information necessary to conduct watch list matching. This information will be transmitted, stored, used, shared, retained, and destroyed consistent with stringent privacy laws, principles, and guidance.

### 4. Privacy Act Exemptions

*Comment:* TSA received approximately 12 comments regarding the Privacy Act of 1974: Implementation of Exemption and System of Records; Secure Flight Records; final rule and notice, 72 FR 63705 (Nov. 9, 2007) (Exemption final rule).

*TSA Response:* TSA appreciates the time the commenters took to review and comment on the Exemption final rule. The Exemption final rule became effective on December 10, 2007 and is beyond the scope of this final rule. The

commenters raised many of the issues addressed in the Exemption final rule. A full discussion of these issues and the Privacy Act exemptions that TSA claimed for the Secure Flight program is in the Exemption final rule and the PIA that TSA is publishing in conjunction with this final rule.

### 5. System of Records Notice (SORN)

*Comment:* TSA received several comments expressing a concern that the Secure Flight program does not provide sufficient access to an individual's personal information under the Privacy Act. Commenters argued that individuals will not be able to access most of the information collected about them, and the program does not have a requirement to provide personal information upon request. The commenters stated that the NPRM did not provide an explanation for the restricted access and this restriction is contradictory to the Privacy Act of 1974.

*TSA Response:* Secure Flight complies with the Privacy Act access provisions, has published a SORN describing its Privacy Act system of records and providing access procedures, and also published a NPRM in connection with its exemptions as permitted under the Privacy Act. TSA fully considered public comment on the exemptions before publishing the Exemption final rule in the **Federal Register** on November 9, 2007.

*Comment:* TSA received several comments expressing concern that the public does not have sufficient information regarding the way TSA will use personal information as part of its watch list matching function. One commenter sought clarification on which databases TSA intends to use within Secure Flight.

*TSA Response:* In this final rule, TSA has determined that it will use the No Fly and Selectee components of the TSDB to perform its watch list matching function. In addition, TSA may decide to compare passenger information on some or all flights on a particular route or routes to the entire TSDB or other government databases, such as intelligence or law enforcement databases, when warranted by security considerations.

*Comment:* TSA received one comment arguing that, under the Privacy Act, an agency must collect information directly from individuals, to the extent practicable, when the agency may use the information to make a decision that adversely affects an individual's rights, benefits, and privileges under a Federal program.

*TSA Response:* TSA notes that covered aircraft operators currently

<sup>24</sup> 5 U.S.C. 552a.

collect information directly from passengers and non-travelers that is necessary for security purposes. Under this final rule, TSA requires covered aircraft operators to collect passenger and certain non-traveler information, by electronic means or verbally, at the time of reservation or when the traveler provides passenger information as part of a group or blocked space reservation, and to accurately transmit the SFPD to TSA. It is neither practical nor economically feasible for TSA to collect SFPD directly from the individual. TSA will leverage the existing practice of the aircraft operator, or a third party acting on behalf of the aircraft operator, collecting passenger and non-traveler reservation information for the purposes of conducting watch list matching comparisons. Any concern that data may be inaccurate unless collected directly from the individuals is mitigated by other factors and redress processes.

*Comment:* TSA received comments that expressed concern that the collection of SFPD “exceeds the purposes of the Secure Flight Program.” The commenters also raised concerns that Secure Flight may become a law enforcement tool that collects information that may be shared with other agencies without appropriate safeguards, legal standards, or oversight. The comment stated that the SORN and NPRM lack any explanation of the proper safeguards and protocols that TSA has put in place to protect the information that will be collected.

*TSA Response:* TSA has strictly limited the function of Secure Flight to accomplish watch list matching as mandated by Congress. Data collection has been limited to minimal identifying data elements and information used to manage the watch list matching and to notify the appropriate aircraft operator in the event of a possible match. Additional protections include the very short data retention (seven days) for the vast majority of individuals affected by the program, and integrating administrative, technical, and physical security safeguards as outlined in the PIA to place limitations on the collection of Personally Identifiable Information and to protect information against unauthorized disclosure, use, modification or destruction. Specifically, administrative safeguards will restrict the permissible uses of personal information and implement the controls for adherence to those uses. As part of the many technical safeguards employed, Secure Flight will implement role-based access controls and audit logging (the chronicling of information accesses and uses of information) as

described in section 8.0 of the PIA to control and monitor the use of personal information. Privacy risks have been mitigated by a defense-in-depth strategy, access controls, auditing, and appropriate oversight.

#### 6. Retention of Data

*Comment:* TSA received a number of comments expressing the opinion that the retention of SFPD must be consistent with European Union/United States data privacy rules as well as privacy laws of other countries. A few commenters argued that TSA should not require covered aircraft operators to comply with regulations that conflict with European Union laws and other countries’ national data privacy laws.

*TSA Response:* SFPD is security information exempt from European Union Data Protection Directives and typically from other data privacy governance around the world. It is not the same as PNR data and thus, it is not subject to the DHS–EU PNR agreement. TSA will retain Secure Flight data pursuant to published record retention schedules as specified in the final rule. The records retention schedule for this rule requires that the Secure Flight program retain records for most individuals encountered by Secure Flight for only a short period. Records for individuals who are cleared by the automated matching tool would only be retained for seven days after the completion of the individual’s directional travel. This 7-day period will be the retention period for the majority of people who travel. Records for individuals who are potential matches would be retained for seven years after the completion of the individual’s directional travel in order to expedite future screening and to enable TSA to respond to any possible legal action. Records for individuals confirmed as a positive match to an individual on the watch list will be retained for 99 years after the completion of the individual’s directional travel to support law enforcement and intelligence activities.

*Comment:* A commenter argued that the data retention schedule for overflights should be the same as the data retained for all other covered flights.

*TSA Response:* The retention schedule for Secure Flight records will be applicable to all flights, including overflights, regardless of origin or destination.

*Comment:* TSA received several comments concerned that TSA would be free to use SFPD for commercial or marketing activities.

*TSA Response:* TSA does not engage in commercial or marketing activities. It is only authorized to share information in accordance with the applicable routine uses under the governing SORN as required by the Privacy Act. In general, information may be shared with external organizations for national security, law enforcement, immigration, or intelligence purposes and as necessary to facilitate an operational response to threats to transportation or national security. Privacy risks that personal information may be disclosed to unauthorized individuals is minimized using a set of layered privacy safeguards that include physical, technical, and administrative controls to protect personal information as appropriate.

*Comment:* A commenter expressed concern that TSA will retain information for seven years about individuals who are identified as potential matches, but are in fact misidentified and will use the information to track these individuals. Although these individuals may obtain a Known Traveler Number or a Redress Number after being misidentified by Secure Flight, the commenter was also concerned that TSA will retain information about the misidentification for seven years.

*TSA Response:* The Secure Flight program will employ processes to prohibit tracking of itinerary information for those individuals not identified as a potential or confirmed match; it will permit controlled access to Personally Identifiable Information related to only those individuals identified as a potential or confirmed match. Retaining the record of potential matches for seven years provides the individual with the greatest opportunity for legal review.

*Comment:* TSA received several comments that argue TSA’s self-imposed data retention restrictions are meaningless.

*TSA Response:* TSA disagrees with the commenters. TSA is committed to the enforcement of the records retention schedule approved by the National Archives and Records Administration (NARA).

*Comment:* TSA received one comment from a foreign government that expressed an unspecified concern regarding the retention of potential watch list matches’ information for seven years, without those individuals’ consent.

*TSA Response:* While TSA is sensitive to the concerns posed by this commenter, the seven-year retention provides the individual with the maximum opportunity to seek legal



review under the law.<sup>25</sup> Consequently, TSA will retain potential matches for seven years in accordance with the approved data retention schedule for Secure Flight records.

#### 7. Sharing of Data With Other Agencies

*Comment:* Several commenters were concerned about TSA's authority to collect personal information from private citizens.

*TSA Response:* The authority for TSA to collect passenger information is section 4012 of the IRTPA, which mandates that TSA obtain passenger information in order to assume the function of conducting watch list comparisons.

*Comment:* TSA received several comments related to the sharing of data with other agencies.

*TSA Response:* External sharing will be conducted in accordance with the applicable routine uses under the governing SORN as required by the Privacy Act. Information is shared with external organizations for national security, law enforcement, immigration, or intelligence purposes and as necessary to facilitate an operational response to threats to transportation or national security. Privacy risks that personal information may be disclosed to unauthorized individuals is minimized using a set of layered privacy safeguards that include physical, technical, and administrative controls to protect personal information as appropriate. Any Federal agency receiving information is required to handle those data in accordance with the requirements of the Privacy Act and their applicable SORNs.

#### 8. Collection and Use by Private Entities

*Comment:* TSA received several comments regarding the collection and use of passenger information by private entities, such as covered aircraft operators, for marketing and sales purposes.

*TSA Response:* TSA notes that the identified entities already collect passenger information that may be used for marketing and sales purposes, including data not mandated by TSA such as address or phone number. TSA limits the use of a boarding pass printing result that TSA provides to covered aircraft operators and airport operators for any purposes other than those necessary for Secure Flight. TSA will also instruct covered aircraft

operators to appropriately safeguard the data related to Secure Flight, in terms of the SFPD it generates through the collection of information from passengers. TSA lacks the authority, however, to dictate any rules for data retention for aircraft operators. The cost associated with the storage of passenger data collected for Secure Flight purposes is beyond the scope of this final rule.

*Comment:* One association commented that some carriers might also not be allowed to collect and transmit data for these passengers according to their national data privacy laws.

*TSA Response:* SFPD is security data, which is typically exempt from privacy governance requirements around the world.

*Comment:* TSA received several comments that expressed concern that the required and "voluntary" data gathered and retained by TSA under Secure Flight could lead to traveler dossiers.

*TSA Response:* The Secure Flight program will not create "traveler dossiers." TSA has established a very short (seven day) retention period for those individuals who are not a match or potential match in the automated matching process. This is expected to be the vast majority of individuals, and the addition of gender and date of birth to the mandatory data elements is expected to reduce even further the number of individuals identified as possible matches. For those individuals whose status cannot be resolved through the initial automated comparison, TSA may be unable to rule out such individuals as a watch list match, and consequently, they may be subjected to additional screening or denied boarding or authorization to enter a sterile area. TSA will make every attempt to clear these individuals through validation of an identity document or the collection of additional information provided via telephone to the Secure Flight Service Center. The seven-year data retention period established for these individuals is to provide the greatest ability to seek review.

#### G. Redress

*Comment:* TSA received two comments expressing general support for the DHS TRIP program. The commenters expressed support for DHS TRIP as the proper mechanism for individuals who believe that they have been improperly or unfairly delayed or prohibited from boarding an aircraft or entering a sterile area as a result of Secure Flight to seek redress. A commenter noted that DHS TRIP will

minimize the number of people who will be misidentified. Other commenters noted that DHS TRIP will not be successful unless misidentified passengers who receive redress are no longer identified as potential matches to the watch list.

*TSA Response:* DHS TRIP is a robust and effective mechanism for individuals to seek redress and relief when they believe that they have been delayed or prohibited from boarding or denied entry to the airport sterile area as the result of the Secure Flight program to seek redress and relief. With the implementation of the Secure Flight program, TSA believes that it will become even more effective with uniform application by the Government rather than relying on application by individual covered aircraft operators. TSA has a continuing commitment to ensure the integrity and ease of the DHS TRIP process.

*Comment:* Various commenters objected to using DHS TRIP as the redress process for the Secure Flight program. They claim it does not meet the access and amendment criteria as required by the Privacy Act, that DHS TRIP is insufficiently transparent, and that DHS TRIP is ineffective, vague, and inadequate. Another commenter argued for the need for judicial review of TSA decisions regarding redress applications.

*TSA Response:* TSA disagrees that DHS TRIP is ineffective, vague, and inadequate. DHS TRIP is a Web-based customer service initiative developed as a voluntary program to provide a one-stop mechanism for individuals to request redress.

If TSA determines that the delay or prohibition from boarding or access to a sterile area resulted from a misidentification of the individual, TSA will retain the information provided by the individual as part of the redress process to facilitate authentication of the individual's identity during future air travel and to prevent repeated and unnecessary delays of misidentified individuals. Once the redress process is complete, an individual who has applied for redress may provide his or her Redress Number to covered aircraft operators. With this Redress Number, the Secure Flight program will have greater success in clearing this individual when it receives and processes the SFPD for the individual.

TSA is committed to minimizing misidentifications by continuously updating information as it becomes available to ensure the accuracy of the watch lists and the Cleared List.

*Comment:* One commenter stated concerns regarding the cost to airlines

<sup>25</sup> Under 28 U.S.C. 2401(a), the statute of limitation to bring suit against the U.S. Government is six years. Retaining the records for seven years ensures that the records are available should an individual file suit against the U.S. Government within the statute of limitation period.

for accommodating individuals who have been delayed or inhibited and are unable to make their scheduled flights.

*TSA Response:* TSA believes that the DHS TRIP redress process addresses the issue of individuals who have been delayed or inhibited. TSA does not require covered aircraft operators to absorb costs associated with passengers' inability to board their scheduled flights because of the Secure Flight program. Covered aircraft operators may make the appropriate customer service decisions for their operations.

*Comment:* One comment states that TSA should not require misidentified individuals to seek redress through DHS TRIP.

*TSA Response:* Individuals who believe they have been misidentified are not required to go through the redress process. DHS TRIP is designed as a voluntary program to provide a mechanism for individuals to request redress. In addition, a redress mechanism is required under the IRTPA. For individuals who choose not to seek redress through DHS TRIP, TSA does not have another mechanism to obtain the necessary information to determine whether the individual is a match to a person on the watch list.

*Comment:* Several commenters expressed concerns about the DHS TRIP redress process and offered recommendations on how to improve the DHS TRIP process.

*TSA Response:* TSA will share these commenters' concerns and recommendations with DHS TRIP.

*Comment:* One commenter stated that TSA should describe "the names on the list" and questioned the validity of the stated rationale for not disclosing the names as protecting national security.

*TSA Response:* TSA cannot respond to non-specific concerns. To the extent the commenter is referring to the watch list used by Secure Flight, it is made up of the Selectee and No Fly components of the TSDB. In certain circumstances set out in the NPRM, broader components of the TSDB might be used. Only individuals who are known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism are included in the TSDB.

As stated in the Secure Flight NPRM, TSA will not disclose the names on the watch list, because this information is derived from classified and sensitive law enforcement and intelligence information. Releasing this information would hamper the Federal government's efforts to protect national security.

#### *H. Consolidated User Guide/Aircraft Operator Implementation Plan (AOIP)*

*Comment:* TSA received several comments requesting that TSA clarify the following questions regarding the interaction between CBP's APIS Pre-Departure program and Secure Flight: (1) Whether CBP's APIS Quick Query (AQQ) message and the SFPD message can be combined; (2) whether a "result" will still be received in response to an AQQ submission; and (3) whether an AQQ result can amend a Secure Flight result. The commenters suggest that DHS should also provide a single process for submitting data sets and receiving responses, given that DHS is providing a single window for data submission. Comments also request more clarity in defining data elements terminology referenced in the rule, and that additional data feeds and varying formats (from the APIS Pre-Departure final rule) not be included in the Secure Flight final rule. One commenter felt that additional programming burdens would be placed on covered aircraft operators to program for AQQ requirements to receive two results for an international itinerary that contains both travel into and out of the United States, while Secure Flight would only require a single result for the same transaction.

*TSA Response:* The Consolidated User Guide, which is Sensitive Security Information (SSI), offers much of the guidance and requirements that covered aircraft operators designing and/or modifying their systems to interact with DHS programs, such as AQQ and Secure Flight, will need. The Consolidated User Guide also offers answers to many of the comments above. The Consolidated User Guide provides more detailed information in support of the rule by describing the data elements required to satisfy AQQ and Secure Flight requirements. Additionally, the Consolidated User Guide draws attention to those areas that are unique to either program by flagging them with a "TSA" or "CBP" marker. Data submission requirements, which are necessary to comply with AQQ and Secure Flight, have been aligned wherever possible and can be combined. The data submitted to DHS will be transmitted via the same portal. Once received, the data required by each program are extracted from the submission by the portal. A single boarding pass printing result will be returned to the submitter. There should never be an occurrence where a submitter would receive a boarding pass printing result from more than one agency.

DHS has attempted to align the data submission process for these two programs wherever possible. There will, however, be some areas where the programs are just not compatible. One example would be when submitting data for a passenger that will be flying into and out of the U.S. on the same directional itinerary. While Secure Flight's result can persist for the entire directional itinerary, APIS data are required by law for each segment of a trip into or out of the United States for the purpose of border enforcement.

*Comment:* A commenter questioned the need to re-examine a previous Secure Flight result during Irregular Flight Operations (IRROP) when APIS Pre-Departure does not.

*TSA Response:* In most IRROPS situations, Secure Flight only requires an informational update. Details are spelled out in the Consolidated User Guide that defines when an informational update is required and when a new boarding pass printing result is required.

*Comment:* Several commenters provided comments on the technical guidance and requirements in the Consolidated User Guide.

*TSA Response:* TSA appreciates the comments on the Consolidated User Guide. The comments are not within the scope of the Secure Flight NPRM. TSA will provide responses to the comments to the covered aircraft operators in conjunction with release of the updated Consolidated User Guide reflecting the Secure Flight program requirements in this final rule.

*Comment:* TSA received comments suggesting that the AOIP not be made a part of the Aircraft Operator Standard Security Program (AOSSP). Commenters believe that incorporating the implementation instructions to the program will make the AOIP subject to a lengthy process that is required for making changes to the AOSSP.

*TSA Response:* The AOIP describes how and when a covered aircraft operator or airport operator transmits passenger, flight, and non-traveler information to TSA, as well as other related matters. Because the AOIP contains requirements that covered aircraft operators must comply with, TSA has determined that it should be part of the covered aircraft operators' security programs. TSA disagrees that amending the AOSSP to incorporate the AOIP would be a lengthy process.

Although TSA is not amending 49 CFR 1560.103 to state that the AOIP is a specific element of foreign air carriers' security programs, TSA will incorporate the AOIP into covered foreign air

carriers' security programs through 49 CFR 1560.109.

*Comment:* TSA received a comment suggesting that the proposed Secure Flight program be amended to allow an airport, at its discretion, to develop its own AOIP, rather than adopt the AOIP of affected aircraft operators. This commenter indicated that aircraft operator plans do not address the particular data systems at the airport.

*TSA Response:* TSA will work with airport operators to develop an implementation plan as appropriate. TSA anticipates that the implementation plan for airport operators will be similar to the AOIP but will take into account the data systems of the airport.

#### I. Testing

*Comment:* A few commenters expressed concerns about and requested further clarification on the program's performance standards, as well as its methodology for measuring them for all testing phases, such as benchmark and parallel testing. Additionally, a commenter argued that covered aircraft operators should neither be subject to Secure Flight, nor should they incur various costs until the program is proven to work. Additionally, this commenter believes that the government should incur the cost for the test phase, not the covered aircraft operators.

*TSA Response:* TSA has separated the testing process into two different phases. First, benchmark testing will take place to test the Secure Flight watch list matching capability against the current results of a covered aircraft operator. TSA has requested voluntary participation in benchmark testing and appreciates those who have participated in this testing. From the benchmark testing, TSA will determine whether the Secure Flight program meets the standards required to successfully accomplish watch list matching.

Following benchmark testing, the second phase of Secure Flight testing will be mandatory parallel testing. During parallel testing, all covered aircraft operators will participate. It is necessary to involve each covered aircraft operator to ensure that all components—watch list matching, connectivity, etc.—successfully meet the standards established for TSA to assume the watch list matching responsibility from each covered aircraft operator. This is part of the set of regulatory requirements and must be borne by the covered aircraft operators. Therefore, TSA will not absorb the covered aircraft operators' costs for this initiative.

TSA appreciates the concerns regarding the response time standards. TSA has established a standard response of not more than four seconds for the system to process a boarding pass printing result using the interactive messages that will occur when a reservation is made or updated information is provided from 24 hours prior to and up to flight departure. One commenter stated that four seconds is not a sufficient response time. TSA believes that the 4-second standard is sufficient for the interactive period, especially when the transmission of a majority of the data will occur as early as 72 hours before departure, with the boarding pass printing results returned to the covered aircraft operator well in advance of the 24-hour period during which a boarding pass can be issued.

*Comment:* Some commenters suggested that TSA has underestimated the number of messages between TSA and the aircraft operators associated with the volume of passengers and have expressed concern that Secure Flight cannot process this volume.

*TSA Response:* TSA has taken into account the anticipated number of messages associated with the forecasted volume of passengers and will be conducting stress testing to ensure that the system is capable of handling the volume.

*Comment:* One commenter noted that DHS must certify to the Government Accountability Office (GAO) that the Secure Flight program has successfully tested the system before TSA can assume the watch list matching function from covered aircraft operators.

*TSA Response:* The 2006 DHS Appropriations Act requires DHS to certify and GAO to report to Congress that TSA meets ten conditions set forth in section 522(a) of the Department of Homeland Security Appropriations Act, 2005, Public Law 108-334 (Oct. 18, 2004), including several that relate to system testing, before it can implement Secure Flight.<sup>26</sup> As the President has instructed in his signing statement dated October 24, 2005, DHS treats this provision as advisory to the extent it purports to allow GAO to prevent implementation of the law unless GAO reports to Congress that DHS has met certain conditions. Upon due consideration, TSA does not plan to assume watch list matching from the covered aircraft operators until DHS makes the required certification and GAO reports to Congress.

<sup>26</sup> TSA may, however, implement Secure Flight on a test basis prior to the DHS certification and the GAO report.

*Comment:* One commenter believes that parallel testing should not be validated unless it has been approved by both TSA and the participating covered aircraft operator.

*TSA Response:* TSA recognizes that parallel testing must result in the successful exchange of data between covered aircraft operators and the Secure Flight program. Therefore, TSA will work with covered aircraft operators throughout parallel testing to ensure that it is successful before TSA assumes the watch list matching function from the covered aircraft operators.

*Comment:* One commenter suggested that the portal through which SFPD will be submitted may not need further testing if CBP has already performed testing on the same portal, which TSA and CBP will share.

*TSA Response:* TSA believes that complete end-to-end testing between the Secure Flight program and covered aircraft operators must be successfully completed before TSA assumes the watch list matching function from covered aircraft operators. While portal testing may have occurred with CBP, complete end-to-end testing of Secure Flight will ensure the successful exchange of data between Secure Flight and covered aircraft operators.

*Comment:* One commenter stated that it is necessary to determine by the final rule what data elements will be used.

*TSA Response:* TSA agrees with this commenter, and therefore, the Secure Flight data elements are clearly identified in this final rule.

#### J. Identification Requirements

*Comment:* A number of commenters expressed concerns that mandating travelers to present a VID to travel restricts citizens' ability and constitutional right to travel. Concerns were also raised that some individuals may not have and/or cannot afford an applicable VID.

*TSA Response:* TSA notes that VID requirements only apply to individuals who are potential matches to individuals on the Selectee or No Fly portions of the watch list. These individuals will be required to present a VID to resolve any misidentification. Individuals who are confirmed Selectee matches will be subject to enhanced screening. Individuals who are confirmed No Fly matches may not fly. Courts have consistently held that travelers do not have a constitutional right to travel by a single mode or the most convenient form of travel. The Secure Flight program would only regulate one mode of travel (aviation), and would not impose any restriction

on other modes of travel. Therefore, a restriction on an individual's ability to board an aircraft as a result of the Secure Flight program would not interfere with a constitutional right to travel.

*Comment:* One commenter states that travelers would be required to display their identification whenever TSA orders and that the order would be given to the covered aircraft operators in secret. The commenter raised the potential threat of an airline contractor committing identity theft.

*TSA Response:* Under the Secure Flight program, TSA will not arbitrarily require travelers to display identification. As detailed in the final rule, VID are required (1) when TSA is unable to distinguish a traveler from an individual on the watch list and needs additional information to help resolve the match and (2) when the covered aircraft operator has not received watch list matching results on an individual prior to check-in. This requirement does not change the other requirements currently in place requiring individuals to provide identification at the security screening checkpoint or to undergo enhanced screening. However TSA and CBP continue to work closely together to harmonize and streamline systems and procedures to maximize efficiency and benefit to the traveling public.

TSA recognizes the importance of protecting against identity theft for SFPD. As to the specific comment, TSA notes that covered aircraft operators are generally in possession of significant information that could be used for identity theft, including name, address, phone number, credit card numbers, and other information. It is the covered aircraft operators' responsibility to prevent unauthorized access to and use of personal information to commit identity theft.

*Comment:* Several commenters requested clarification on whether the requirement for covered aircraft operators to not issue a boarding pass or authorization to enter a sterile area or permit an individual to board an aircraft if the individual does not provide a VID when requested applies to cleared individuals. These commenters also requested clarification on the number of times and/or the location of security checkpoints travelers will be required to display identification.

*TSA Response:* Currently, aircraft operators must request that all passengers and non-travelers provide identification at the time of check-in. Additionally, TSA requires individuals to present appropriate identification at the screening checkpoint or to undergo enhanced screening under existing

security directives. With the implementation of Secure Flight, if an individual has an "inhibit" boarding pass printing result, covered aircraft operators will not issue a boarding pass to the individual if he or she does not provide a VID when requested at the airport. Passengers for whom Secure Flight has not inhibited boarding pass issuance will not be required to present a VID. This does not change the other requirements currently in place requiring individuals to provide identification at the security screening checkpoint or to undergo enhanced screening.

*Comment:* Several commenters agree that travelers' identification should be verified, but do not agree that TSA should specify how and where it takes place, due to different airline operating procedures, roles and responsibilities, and the possibility of delays.

*TSA Response:* TSA only requires covered aircraft operators to request a VID at the airport pursuant to procedures in its security program, when TSA has not informed the covered aircraft operator of the results for watch list matching for an individual by the time the individual attempts to check-in, or when TSA informs the covered aircraft operator that an individual must be placed on inhibited status. This procedure is required for the security of all travelers, as well as airline personnel.

*Comment:* One commenter suggests that TSA be responsible for just screening passengers and their cargo and to have Federal agencies, such as the Federal Bureau of Investigations (FBI) and the Central Intelligence Agency (CIA), assume responsibility for watch list matching activity.

*TSA Response:* The Intelligence Reform and Terrorism Prevention Act (IRPTA) requires DHS to assume the function of pre-flight watch list matching activity from aircraft operators. In accordance with IRPTA, TSA has developed the Secure Flight program to implement this congressional mandate. Under this rule, TSA will receive passenger and certain non-traveler information, conduct watch list matching against the No Fly and Selectee lists, and transmit boarding pass printing results back to covered aircraft operators.

*Comment:* TSA received several comments regarding the difficulty for passengers and non-travelers to clarify who is authorized to ask for a VID.

*TSA Response:* TSA expects to complete the watch list matching process and permit covered aircraft operators to issue boarding passes to the vast majority of passengers through the

Secure Flight fully-automated, initial comparison. However, for the instances where TSA is unable to complete the watch list matching process for an individual, covered aircraft operators must ask the individual to present a VID. This requirement is in alignment with current practices that require covered aircraft operators to request all passengers and non-travelers to provide identification at check-in or at the screening checkpoint.

*Comment:* One commenter requested clarification on how TSA would account for passengers who make reservations under a name or nickname that differs from what is listed on their VID.

*TSA Response:* Under § 1540.107(b), travelers must provide their full name at the time of reservation. The Secure Flight final rule defines "full name" as the name that matches the full name listed on the individual's VID. Therefore, individuals may not submit nicknames unless that nickname is the name on the VID.

*Comment:* TSA received several comments that addressed the fact that certain identification requirements under Secure Flight are already current practice.

*TSA Response:* TSA is aware that travelers currently present identification to check in luggage and to enter the checkpoint. Additionally, passengers who travel on international flights must present a passport or another acceptable travel document to board an aircraft. Presenting identification in these situations serves a different purpose than the requirement to present a VID under this final rule. The requirement to present a VID applies only to passengers for whom TSA has asked the covered operator to place on inhibited status. This requirement assists TSA in resolving potential matches to the watch list. While this final rule includes a separate requirement to present identification, this requirement will apply to only a limited number of individuals and serves an important step in the watch list matching process. Including the requirement in this final rule also informs the public of the process and the affected individuals will know that they need to have a VID when they go the airport.

#### K. Economic Comments

*Comment:* TSA received several comments stating that the estimated time for employees of airline reservations centers or travel agents to collect personal information data from those making flight reservations by telephone should be longer than 20 seconds, the time used in the NPRM.

These comments also suggested that 30 seconds was a more accurate estimate of the average data collection time.

*TSA Response:* Based on information received from subject matter experts and used to develop the NPRM estimates, TSA disagrees that on average this collection of personal information will take considerably longer than 20 seconds. Nonetheless, in the high estimate cost for the regulatory evaluation, TSA used 30 seconds as the cost to airline reservation centers, travel agents, and passengers themselves, who incur opportunity costs when this additional data collection requirement impinges on time that could have been used in other ways. Because of this, the regulatory evaluation contains estimates of the contribution to Secure Flight costs of a change in TSA's primary assumption on this matter. TSA recognizes that in some instances and for some reservations this data collection time could require additional time, but believes that in many if not most instances the additional data collection effort will be very modest. To balance these concerns, TSA will use a primary estimate of 25 seconds for the time required to collect personal information required by Secure Flight during the telephone reservation process.

*Comment:* TSA received a comment stating that messaging costs related to Secure Flight appear underestimated and that an average message cost of \$0.20 should be assumed. This value would be consistent with the value used by CBP in the APIS regulatory evaluation.

*TSA Response:* TSA agrees with this comment. Both in the text of the NPRM evaluation and for the final rule TSA has used a per message value of \$0.20, just as the CBP analysis in the APIS regulatory evaluation.

*Comment:* TSA received a comment that travel agencies using electronic profiles will be obliged to reprogram these profiles to accommodate the additional data fields required for reservations under Secure Flight, and that these costs should be included in the Secure Flight cost analysis. In addition, costs associated with updating agent scripts for taking passenger reservations should be included as a compliance cost.

*TSA Response:* TSA concurs with this comment and has relied on data provided by the commenter to estimate these costs in the final rule regulatory evaluation. TSA includes the updating of agent reservation scripts as part of this reprogramming activity.

*Comment:* TSA received a comment that travel agents would incur training

costs to prepare agency employees for the new data collection requirements of Secure Flight, and that these costs should be included as a cost of compliance with Secure Flight.

*TSA Response:* TSA agrees that these training costs to travel agents are among the compliance costs for Secure Flight, and has included an estimate of these costs in the final rule regulatory evaluation.

*Comment:* TSA received a comment stating that as part of the costs of Secure Flight, TSA should include the costs of holding flights that are awaiting Secure Flight clearance, and should use the estimate of these costs used by CBP in its evaluation of the APIS rule.

*TSA Response:* The Secure Flight program addresses the issuance of boarding passes to passengers, and not the clearance of flight manifests or passenger lists. Additionally, since the process of clearing passengers already exists along with delays as described above, there is a fundamental difference in the baseline between the APIS and Secure Flight rules. When implemented, the program is required to improve over the current situation and thus either the same or better than existing delays. Therefore, the cost of holding a flight is not relevant for the workings of the Secure Flight program.

*Comment:* TSA received a comment regarding reservations for international air travel and the distribution of these reservations among airline call centers, brick and mortar travel agencies and online reservation services. The comment questioned whether reservation making is distributed for international travel in the same way as it is for domestic travel, and stated that historically travel agencies have been more prominent in providing reservation services for international itineraries. Because of this the commenter requested that travel agencies should be given a greater proportion of international travel reservations. The commenter also claimed that these international reservations handled by travel agencies are typically the more difficult and time-consuming reservation assignments.

*TSA Response:* Because of the significant changes that have occurred in airline ticket distribution in the past decade, with the rise of more direct and transparent distribution of tickets to passengers via the internet and the growing use of the internet in all aspects of public life, TSA believes that forecasting the future of airline ticket distribution channels is difficult at best. Given this great uncertainty, TSA does not think changing the current

distribution used in the regulatory evaluation is justified. With respect to the greater difficulty or complexity of international reservations that are handled by travel agencies, the regulatory evaluation takes note only of the cost to reservation makers and passengers of the incremental time added to the reservation process by Secure Flight requirements, and this increment does not change with the complexity of the travel itinerary or related reservation details.

*Comment:* Numerous commenters stated that TSA had failed to consider the costs of delay to travelers and the airlines as the APIS rulemaking did.

*TSA Response:* In TSA's view, the effect of Secure Flight will be to improve the system-wide passenger clearing process, not reduce its effectiveness with increased delays. Any costs that may be imposed by Secure Flight should be measured as an increment from today's baseline, which itself already includes these types of consequential disruptions to travel plans. Numerous examples of how delays will be reduced were provided in the NPRM evaluation and there is no evidence that the centralized processing would increase the frequency or duration of associated delays. Furthermore, there are several material differences between Secure Flight and APIS implementation. The APIS rule had to consider that the screening and potential delays were being added to a baseline that did not already include those same delays. Additionally, the CBP rules were designed around giving a flight manifest a go/no-go decision for the whole flight. In this context, it is very prudent to consider the possibility of an entire flight being delayed. For Secure Flight, the screening process and delays already exist and the clearance is reservation by reservation. There is no reason to believe that air carriers would hold a flight for a single individual. TSA believes strongly, that if anything the calculation should have been a reduction and attributed as a benefit. Instead, TSA examined the federal published data on flight delays due to security causes. Using that data, TSA provided an example of what doubling those costs would look like. TSA does not believe the example is at all probable but included the information in the regulatory evaluation to assure the public TSA did not ignore the issue.

*Comment:* Numerous commenters stated that this rulemaking was an unfunded mandate.

*TSA Response:* Both the NPRM and final regulatory evaluations require application of the provisions of the Unfunded Mandates Reform Act

(UMRA). UMRA defines an unfunded mandate as one that "may result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of \$100,000,000 or more (adjusted annually for inflation) in any 1 year. \* \* \*" This final rule does not contain such a mandate on State, local, and tribal governments. The overall impact on the private sector does exceed the \$100 million threshold in the aggregate.

*Comment:* Many commenters suggested that the private sector could not afford the program.

*TSA Response:* There are legislative mandates to implement federal passenger name matching. TSA has attempted to balance very real security needs with the appropriated funds provided to it and costs imposed on the rest of the economy.

*Comment:* A private citizen said the program should be judged by a terrorist's cost to defeat the program.

*TSA Response:* TSA is uncertain how such an approach could be presented. TSA's goal is to provide a program that is difficult for the terrorist to defeat by improving the multiple levels of security TSA uses. Strengthened security does increase the costs to the terrorist but not such that a useful comparison could be made for regulatory consideration.

*Comment:* A private citizen stated that GAO should review the costs.

*TSA Response:* There is considerable review outside TSA of both program costs and the evaluation for purposes of the rulemaking. GAO is not a part of the review at this stage.

*Comment:* At least one commenter felt being denied access to travel was detrimental to professional position.

*TSA Response:* One of the requirements and goals of Secure Flight is to reduce the current number of instances where individuals are inappropriately delayed or denied access. This rulemaking should improve over the status quo.

*Comment:* Numerous comments suggested TSA had inadequately addressed various travel agent costs.

*TSA Response:* TSA used much of the suggested data and process description in completing a final estimate that included considerably more expense for programming, training, and day to day implementation. Approximately \$80 million in additional expenses was added to reflect these travel agent costs.

*Comment:* Air carrier comments generally stated that the rule cost too much and TSA had omitted some cost categories. In some cases the carrier comments speculated about what might be changed in the final rule.

*TSA Response:* TSA is not addressing the speculative comments; but where specific examples related to the final rule were provided TSA incorporated the information as appropriate. Specific examples are covered in other comment responses. TSA did identify and included slightly more than \$800 million in additional air carrier expenses based upon the public input. TSA has considered cost and security as a delicate balancing process but must achieve the security needs of the country.

*Comment:* Numerous comments suggested opportunity costs were not fully understood. Numerous comments suggested flat rates or the addition of costs already presented as opportunity costs.

*TSA Response:* TSA reviewed these comments to verify that opportunity costs had in fact been included in the Regulatory Impact Analysis. These comments included concerns with opportunity costs for passengers making reservations and compensation costs to businesses associated with collecting new passenger data from those making reservations. Based on these comments, TSA increased the average time per reservation transaction for requesting and providing this Secure Flight passenger information from the 20 seconds used for the NPRM to 25 seconds in the regulatory evaluation for the final rule. This change affected costs to travel agents taking reservations by telephone and costs to airline telephone reservation centers. The change also affected opportunity costs for passengers making telephone reservations using either of these two channels for reservation making. TSA identified opportunity costs of time that are incurred by passengers making reservations, who must spend additional increments of time providing Secure Flight required information over the telephone or internet in the course of making an airline reservation. These spans of time were valued using the average passenger value of time developed for DOT and FAA regulatory guidelines. In TSA's view, which is consistent with customary practice in this type of analysis, it is more accurate to estimate average spans of time spent, and value these using a consensus value of time, rather than assigning a flat value per passenger.

Additionally, TSA verified that it fully assessed business costs that mirror passenger opportunity costs. For increased transactions times, this involves both estimating the additional labor costs borne by these firms, and using fully-burdened compensation rates to monetize these labor costs,

because meeting the Secure Flight data collection requirements may necessitate additional staff for affected firms. In some cases, commenters indicated that Secure Flight requirements would lead to additional reaccommodation costs for travelers who were kept from boarding their intended flights. In TSA's view, the effect of Secure Flight will be to improve these matters, relative to the current baseline environment, rather than worsen them. Commenters suggested that businesses affected by Secure Flight must devote additional employee time for fulfilling Secure Flight information requirements or for assisting passengers whose travel itineraries are disrupted by factors related to Secure Flight. To assess time-related costs, such as the time associated with the solicitation and recording of additional data elements from passengers, TSA used hourly compensation rates from the Bureau of Labor Statistics. It is TSA's view that Secure Flight will improve the management of security-related passenger identity data.

*Comment:* Several air carriers stated that the estimates for the AOIP implementation were considerably low.

*TSA Response:* The rule describes the change from a carrier developed-AOIP to a TSA-developed AOIP. This substantial change could mean the cost estimate is now too high because the workload has been reduced for the carriers.

*Comment:* Numerous comments mentioned the impact and interaction of the Secure Flight and APIS rules.

*TSA Response:* TSA and CBP worked very hard to eliminate redundancies and minimize the combined impact of the rules. A Consolidated User Guide has been issued that outlined to the carriers the details showing that both agencies have adapted the process to satisfy security requirements while not causing unnecessary redundancy of work and expenses. Additionally, the costs related to that interaction were reviewed to avoid double counting in the final evaluation.

*Comment:* Several commenters provided feedback on the benefits and break-even analysis. One said that a reduction in false positives would be a benefit, but TSA needs to clean up the No Fly list. Two others noted that the benefits claimed were also claimed by CBP for the AQQ program, so they should not be double counted for Secure Flight. Several comments showed dissatisfaction with the concept of a break-even analysis.

*TSA Response:* The Federal government is constantly working to improve the quality of all matching lists.

A break-even analysis is not a traditional benefit-cost ratio. The qualitative description of benefits in both rules is appropriate as no assertion is made of an exact level. All DHS components are working hard to improve the methods of presenting security benefits in relationship to costs. The very nature of terrorism makes it impossible to assign traditional probabilities to events or to describe a risk as a specific probability. At present, the break-even analysis balances the need to present comparable methodologies among rules while not disclosing any highly sensitive intelligence.

*Comment:* Several comments addressed cost issues related to the Consolidated User Guide and that the government should pay the expenses imposed on the private sector.

*TSA Response:* TSA does not separately identify costs as Consolidated User Guide costs. Rather, TSA considers all of the known changes from the status quo and provides its best estimate of those costs in total. Status quo costs are the starting baseline for evaluating the rule, not an element TSA can add and reimburse the private sector.

*Comment:* One organization stated that the analyses required by constitutional and international law, the Airline Deregulation Act, the Privacy Act, and the Regulatory Flexibility Act must be conducted and published for additional comment before the proposed rules or any similar rules are finalized.

*TSA Response:* TSA has complied with analysis requirements for both the NPRM and final rule. The requirements of the Regulatory Flexibility Act are very clearly identified in the regulatory evaluations.

*Comment:* One public interest group stated that frequent flyer programs provide billions of dollars of benefits each year in exchange for the information they collect. Travelers will now be required to provide the information for free. This rule could have a significant impact on the frequent flyer programs—perhaps making them obsolete. The air carriers will now be able to collect the information and sell it or use it in marketing without compensation. TSA must account for those costs.

*TSA Response:* Air carriers have already begun to change their loyalty programs. TSA cannot speculate on the future of these programs, because expenses, such as fuel costs, are resulting in less end-user value. Some air carriers have stated that they did not have this information in other systems (such as frequent flyer programs) that would fully satisfy the data acquisition

requirements. If TSA calculated a marketing sales value on the data, that value would be a benefit offsetting some of the carriers' costs. Based upon carrier comments, TSA believes the carriers would not agree that such sales would be beneficial.

*Comment:* According to the Small Business Administration's Office of Advocacy (SBA Office of Advocacy), TSA's statement in the NPRM that it was withholding RFA certification implied that TSA had already predetermined that the rule would not have a significant economic impact on a significant number of small entities. The SBA Office of Advocacy believed that TSA was not making a reasonable effort to explore all effects of the rule.

*TSA Response:* TSA's intent in the Initial Regulatory Flexibility Analysis (IRFA) was to convey that TSA had not made a determination on whether there was a significant economic impact on a significant number of small entities. TSA did not intend to imply that it had predetermined that the rule would not have a significant economic impact on a significant number of small entities. Unfortunately, the word choice conveyed the opposite meaning. TSA explored all effects of the rule and used economic information from all commenters to improve the final estimates throughout the evaluation. TSA expanded a sensitivity analysis in the Final Regulatory Flexibility Analysis (FRFA) to show that we examined the various degrees of impact. TSA concluded that the rule did not have a significant economic impact on a significant number of small entities in section 2.2.2. of the final regulatory evaluation.

*Comment:* SBA Office of Advocacy stated that TSA has underestimated the cost to small business and did not consider certain costs. These costs include the impact of flights that may be delayed waiting for TSA, which is an economic cost and could lead to loss of future business. Additionally, airlines may need additional staff to deal with unhappy customers. The SBA Office of Advocacy suggested that TSA should address the cost of negative customer satisfaction.

*TSA Response:* TSA reviewed the small business analysis and has presented a FRFA that TSA believes is representative of impacts and costs. Not all air carriers are regulated under this rule. After reviewing all comments, TSA became aware that some commenters had assumed that all carriers would be regulated under this rule.

Additionally, the SBA Office of Advocacy comments fail to recognize that many of the items identified as

supposedly new impacts are actually in the existing baseline today. The evaluation presents the change, not the baseline plus change. In TSA's view, the effect of Secure Flight will be to improve the system-wide passenger clearing process, not reduce its effectiveness with increased delays. Any costs that may be imposed by Secure Flight should be measured as an increment from today's baseline, which itself already includes these types of consequential disruptions to travel plans. In the NPRM evaluation, TSA provided numerous examples of how delays will be reduced. There is no evidence that the centralized processing would increase the frequency or duration of associated delays. Additionally, the performance standards for final implementation require an improvement in overall service. TSA believes the clarification on baseline events cited as new and the strict implementation requirements provide a contrary conclusion to the SBA Office of Advocacy.

*Comment:* The SBA Office of Advocacy suggested that TSA should consider alternatives that commenters suggested.

*TSA Response:* TSA is unaware of the specific alternatives the SBA Office of Advocacy may be suggesting. TSA reviewed and considered all comments. TSA believes the final rule and evaluation reflect the viable alternatives.

*Comment:* The SBA Office of Advocacy and other commenters stated that TSA underestimated the impact on travel agents and that the impact is direct. They suggested that TSA should prepare a supplemental IRFA.

*Response:* The Regulatory Flexibility Act of 1980 (5 U.S.C. 601 *et seq.*, as amended by the Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996) requires agencies to analyze the economic impact of regulatory changes on small entities that would be directly regulated by proposed rules. An agency is not required to prepare such an analysis, however, if the agency head certifies that the rule will not "have a significant economic impact on a substantial number of small entities" and supports the certification with a statement of the factual basis for the certification. 5 U.S.C. 605(b). This final rule does not directly regulate travel agents, because the final rule requires only covered aircraft operators, not travel agents, to collect and transmit SFPD to TSA. Although TSA proposed in the Secure Flight NPRM to require covered aircraft operators to collect passenger information at the time an individual makes a reservation for a flight, TSA has decided not to include

this requirement in this final rule. Instead, covered aircraft operators cannot transmit a SFPD to TSA for processing unless they have the individual's full name, date of birth, and gender. Thus, it is up to the covered aircraft operators to decide how and when it will collect passenger information, provided that the covered operator collects full name, date of birth, and gender for all reservations 72 hours prior to the scheduled time of flight departure.

TSA used much of the information from the comments to increase the costs that travel agents will incur by approximately \$80 million. Even in the NPRM, TSA did not dismiss the costs to the travel agents; rather, as stated in the legal citations above, TSA believes it has made the appropriate presentation in the FRFA.

*Comment:* A commenter stated that TSA's count of small airlines is wrong particularly in the case of Alaska.

*TSA Response:* TSA worked from an exact list of regulated entities. TSA believes that many commenters assumed that TSA, through this rule, would regulate all air carriers.

*Comment:* A commenter argued that setting the threshold for determining whether an entity experienced an impact at 2 percent or higher of their revenue is too high.

*TSA Response:* TSA included a sensitivity table with different thresholds but TSA's intent was to convey no decision on the Regulatory Flexibility Act determination. TSA revised the analysis in the FRFA in section 2.2.2. of the final regulatory evaluation.

*Comment:* A commenter stated that the use of an internet portal is not practical for any operator other than the very smallest.

*TSA Response:* TSA is developing a software application to enable Secure Flight connectivity for the very smallest carriers. The use of the term "internet portal" was merely a way to label this alternative. TSA is developing this alternative system specifically with the small carriers' needs in mind. TSA also developed a system whereby air carriers may communicate directly with DHS and will be able to send SFPD to TSA and receive results through this system. TSA adjusted both the cost levels and distribution among the air carriers to better reflect costs.

*Comment:* A commenter stated that some small airlines do not participate in APIS and therefore will have first time programming costs to connect with Secure Flight.

*TSA Response:* TSA adjusted both the cost levels and distribution among the

air carriers to better reflect costs that are reflected in the FRFA. TSA is unable to differentiate or provide relief separately to non-APIS carriers. TSA calculations did attempt to estimate the number in APIS versus original programming. This information, however, is not air carrier specific.

*Comment:* A commenter stated that this rule would affect small businesses in instances where individuals representing the small businesses would attempt to travel without proper documents.

*TSA Response:* Except under the limited circumstance in which a passenger must present a verifying identity document at the airport, the rule does not change the current requirements for presenting documents at the airport and does not impact passengers who do not need to present a verifying identity document. Section 1.6.6 of the final regulatory evaluation includes an analysis of the impact of passengers who must present a verifying identity document.

*Comment:* A commenter stated that there are several sections in the rule where Secure Flight appears to be in conflict with international law, specifically, article 12 of the International Covenant on Civil and Political Rights (ICCPR).

*TSA Response:* The commenter mischaracterized this issue as a small business issue. The relationship between Secure Flight and various international agreements has been discussed, as appropriate, in section III.A of this preamble. TSA does not consider this a comment on the IRFA or appropriate to address in the FRFA.

#### L. General Comments

TSA received numerous general comments on the Secure Flight NPRM as a whole without comment on any specific provision of the NPRM. TSA received several comments expressing general support for the Secure Flight program and its mission to enhance the security of commercial air travel through preflight comparisons of airline passenger information to Federal government watch lists for international and domestic flights. TSA also received several comments expressing general opposition to the Secure Flight NPRM without noting specific objections.

*Comment:* TSA received several comments stating that the Secure Flight NPRM fails to improve on the current process and/or flight safety. Other commenters similarly claim the increased bureaucracy and costs of Secure Flight are not warranted by the benefits of the program.

*TSA Response:* TSA disagrees that Secure Flight will fail to improve on current processes and/or flight safety. IRTPA requires DHS to assume from aircraft operators the function of conducting pre-flight comparisons of airline passenger information to Federal government watch lists for international and domestic flights. TSA has designed Secure Flight to implement this congressional mandate.

The Secure Flight program will streamline and simplify the watch list matching process by moving watch list matching responsibilities currently performed by dozens of air carriers to TSA. There are many benefits of the Secure Flight program. The program will create consistency for the traveler and help prevent passenger misidentification and will allow airlines to focus on other aspects of their operations. TSA will be able to prevent more effectively and consistently certain known or suspected terrorists from boarding aircraft where they may jeopardize the lives of passengers and others. Furthermore, TSA will be able to identify individuals who must undergo enhanced screening because they pose a threat to civil aviation. TSA will also be able to facilitate the secure and efficient travel of the vast majority of the traveling public by distinguishing them from individuals on the watch list, thereby minimizing the likelihood of a passenger being incorrectly identified as an individual on the watch list.

*Comment:* TSA received requests for an extension of the comment period due to the complexity and scope of the NPRM. There were requests to extend the comment period from October 22, 2007, to both December 21, 2007, and January 21, 2008.

*TSA Response:* TSA appreciates the concern and desire for additional time to provide substantive comments on the rule. TSA extended the comment period an additional 30 days (to November 21, 2007) in a notice published in the **Federal Register** on October 24, 2007.<sup>27</sup> TSA believes this provided a sufficient amount of time for commenters to fully understand and comment on the impacts and implications of the Secure Flight NPRM.

*Comment:* TSA received several comments expressing a concern that the Secure Flight program would increase the likelihood and length of delays at airports for passengers.

*TSA Response:* The covered aircraft operators will provide the majority of the requested passenger information and will receive boarding pass printing results in advance of a passenger's

<sup>27</sup> 72 FR 60307 (Oct. 24, 2007).



arrival at the airport. This process will reduce the need for passengers to go to the ticket counter to provide passenger information. For the majority of passengers, Secure Flight will not impact their ability to obtain a boarding pass in the manner that they currently do so. Additionally, DHS must certify that Secure Flight will not produce a significant number of misidentified passengers.<sup>28</sup> For many passengers who currently need to go to the ticket counter to obtain a boarding pass, Secure Flight will allow them to obtain their boarding passes in advance or at the airport kiosks. Therefore, TSA believes that the Secure Flight program will not cause additional airport delays.

*Comment:* A commenter requests that TSA coordinate with the aircraft operators during Secure Flight development.

*TSA Response:* TSA has been coordinating, and will continue to coordinate, with covered aircraft operators, as well as other affected parties, during development and implementation of Secure Flight.

*Comment:* One aircraft operator questions what TSA has done to address the issue of following a disciplined life cycle development approach outlined in the August 4, 2006, GAO Report on Secure Flight.

*TSA Response:* TSA has implemented processes and a program management organization to address the concerns identified in the GAO report on Secure Flight. These include the development of program goals and requirements, a detailed program schedule, cost estimates and tracking mechanisms, and system and data security programs. GAO continues to review Secure Flight progress in these areas. DHS will certify that TSA has followed a disciplined life cycle program for the Secure Flight program before TSA assumes responsibility for watch list matching.

*Comment:* TSA received several comments asking if TSA or DHS plans to launch a public awareness campaign to ensure that the traveling public understands the new requirements for providing additional personal information such as full name, date of birth and gender. Several of these commenters indicated they would support such a program. One commenter suggested that the definition of full name should simply be explained as matching the identity document of the individual and should become a focal point of the campaign.

*TSA Response:* TSA agrees that the full name provided by a passenger or non-traveler must match that which appears on their VID. Under §§ 1640.107(a) and 1560.3, passengers and non-travelers must provide their full name as it appears in their VID.

Additionally, TSA plans to launch a public awareness campaign to ensure the traveling public understands the new requirements for providing additional personal information such as full name and gender. The campaign is still being developed and will be described in further detail in the future.

#### *M. Comments Beyond the Scope of the Rulemaking*

*Comment:* TSA received one comment that expressed support for Secure Flight, but also requested that TSA mandate “no movement between cabins out of the U.S., as well as into the U.S.” In order to achieve this, the commenter proposes that a “chain mesh curtain must be mandated.”

*TSA Response:* Restrictions on movement between cabins on flights into and out of the United States is outside of the scope of this final rule.

*Comment:* Several comments indicated support for the APIS Pre-Departure final rule and resulting changes in the definition of “departure.” Other commenters suggested changes to the APIS Pre-Departure final rule, including recommendations that CBP use the Cleared List in watch list matching.

*TSA Response:* The APIS Pre-Departure final rule and resulting changes, such as the change in the definition of “departure,” are outside of the scope of the Secure Flight final rule.

*Comment:* Several commenters suggested that DHS address other threats to our nation’s security, for example, threats involving port security and border security.

*TSA Response:* Comments on other actions taken by DHS to ensure our nation’s security, by means other than Secure Flight, are beyond the scope of this final rule.

*Comment:* TSA received several comments expressing concern that covered aircraft operators operating the first flight of a connecting flight would not be able to issue a boarding pass for the second flight until the covered aircraft operator received an appropriate boarding pass printing result from TSA. Some commenters requested that Secure Flight develop a standard for transmission and sharing of messages between covered aircraft operators to enhance the security process, with respect to connecting passengers.

*TSA Response:* The decision to share data between covered aircraft operators is beyond the purview of TSA’s authority and outside of the scope of this final rule. While data sharing agreements between covered aircraft operators are decisions unique to the business of each carrier or carrier alliance, TSA acknowledges that such agreements would enhance the Secure Flight data transmission/security clearance process, particularly with respect to connecting passengers.

*Comment:* A commenter suggested that DHS “sunset” the 2007 APIS Pre-Departure final rule once Secure Flight takes over watch list matching for international flights. The commenter believes that the 2007 APIS Pre-Departure final rule is unnecessary once Secure Flight is in place for watch list matching.

*TSA Response:* TSA appreciates the commenters concerns related to “One DHS Solution,” however, any changes to the APIS Pre-Departure final rule are outside of the scope of this rulemaking.

*Comment:* TSA received one comment requesting information on what TSA’s contingency plans are for accommodating passengers on another carrier in the event of a Secure Flight outage.

*TSA Response:* TSA will provide outage information to covered aircraft operators in the Consolidated User Guide. Rebooking airline passengers is outside the scope of the Secure Flight program.

*Comment:* A commenter suggested that TSA indemnify covered aircraft operators for any and all claims related to that information collection.

*Response:* While TSA understands the concern expressed in this comment, indemnification of covered aircraft operators is beyond the scope of this rulemaking and TSA’s authority to implement.

## **IV. Rulemaking Analyses and Notices**

### *A. Paperwork Reduction Act*

The Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501 *et seq.*) requires that TSA consider the impact of paperwork and other information collection burdens imposed on the public and, under the provisions of section 3507(d), obtain approval from the Office of Management and Budget (OMB) for each collection of information it conducts, sponsors, or requires through regulations.

This final rule contains new information collection activities subject to the PRA. Accordingly, TSA has submitted the following information requirements to OMB for its review.

<sup>28</sup> Section 522(a)(2) of the 2005 DHS Appropriations Act (Pub. L. 108–334, 118 Stat. 1298, Oct. 18, 2004).

TSA is establishing this information collection in accordance with 49 U.S.C. 44903(j)(2)(C), which requires TSA to assume the passenger matching function of comparing passenger information to Federal watch lists. In order to carry out effective watch list matching, TSA has determined that it must receive each individual's full name, gender, date of birth, and, to the extent available, Redress Number, Known Traveler Number (in the future), and passport information. Therefore, TSA is requiring covered aircraft operators to request this information from passengers or non-travelers seeking sterile area access on covered flights. The covered aircraft operator must then communicate this information, as well as message management information and itinerary information to TSA. The covered aircraft operator must also transmit relevant updates to the passengers' or non-travelers' information. Additionally, TSA may need the covered aircraft operators to obtain and communicate information from an individual's form of identification or a physical description (e.g., height, weight, hair color, or eye color) of the individual. TSA would use all of this information during watch list matching.

After the final rule is published, TSA will provide an Aircraft Operator Implementation Plan (AOIP) to each covered aircraft operator, outlining each covered aircraft operator's specific requirements for implementing Secure Flight. These requirements include the specific compliance dates on which each covered aircraft operator must begin testing and providing SFPD to TSA. Although the AOIP was described in the preamble of the NPRM as a reporting burden, under the final rule, TSA will provide the AOIP to covered aircraft operators. Therefore, the AOIP is now a recordkeeping requirement, and, as such, the covered aircraft operators must adopt the AOIP into their Aircraft Operator Standard Security Plan (AOSSP) upon finalization of the AOIP.

Under this final rule, TSA will provide authorization for non-travelers to enter a sterile area to accompany a traveling passenger (such as to escort a minor or assist a passenger with a disability). In the future, TSA plans to authorize non-travelers seeking authorization to enter a sterile area for other purposes, and TSA will collect information about those non-travelers. TSA is not able to estimate the information collection burden for this future aspect of the Secure Flight program and therefore has not included them in the burden estimates.

TSA is requiring covered aircraft operators to submit passenger

information for covered flights and certain non-traveling individuals to TSA for the purpose of watch list matching. This information includes data elements that are already a part of the routine collection by the covered aircraft operators (e.g., name, itinerary info), as well as the additional information required in the Secure Flight final rule.

TSA assumes that the great majority of covered aircraft operators will use an automated transmission process to submit passenger information and information for non-traveling individuals. The transmission time for an automated system is instantaneous and, as such, TSA believes the additional time-related burden of transmission is too small to be significant. TSA has determined that the information that covered aircraft operators must collect or request from passengers (e.g., date of birth, gender, Redress Number (if available)) will take no more than 25 seconds per transaction to collect. TSA estimates that the annual hour burden for this activity is 548,843 hours. For the remaining 16 covered aircraft operators (see table 1.4.1.e of the Regulatory Analysis) who will potentially leverage the Web-based alternative data transfer mechanism, TSA has estimated the time required to build and transmit initial messages and updated messages to TSA at 4,013 total annual hours. Thus, TSA estimates the total annual hour burden for an annual 163 respondents to be 552,856 hours [548,843 + 4,013].

As a protection provided by the Paperwork Reduction Act, as amended, an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number.

TSA received several comments generally on the information collection burden. Below is a summary of the comments and TSA responses to the comments.

*Comment:* One commenter noted that the additional passenger information that TSA is requiring covered aircraft operators to submit to TSA is already available to the aircraft operator. This additional information, however, still represents an additional transmission burden than that already required for APIS.

*TSA Response:* As part of its PRA analysis, TSA has recognized a transmission burden, but because for most aircraft operators the transmission is automated and therefore instantaneous, as stated above, TSA believes the additional time-related burden is too small to be significant. Also above, TSA has calculated an hour

burden for the remaining 16 covered aircraft operators who will potentially leverage a Web-based alternative data transfer mechanism to transmit data to TSA.

*Comment:* With regard to specific data elements, a commenter expressed the view that with the exception of name and some flight information, no SFPD is routinely collected or contained within a passenger's reservation booking.

*TSA Response:* TSA recognizes that aircraft operators have different systems in which they maintain passenger information. TSA does not require that aircraft operators submit SFPD from their reservation systems. Aircraft operators may use any system in which the data resides to transmit the passenger information.

*Comment:* A commenter held the view that TSA did not consider costs other than transmission of the passenger data in its annual burden estimate, such as costs of collecting the SFPD, resource costs to meet new requirements, training costs, costs of responding to inhibited vetting responses, and the cost of delay to aircraft where TSA is unable to provide a vetting response in a timely manner.

*TSA Response:* Within the PRA analysis, TSA has not calculated a cost burden on aircraft operators for collecting SFPD from passengers that is separate from the cost of the hour burden to collect these data. The other additional costs are not part of the PRA cost analysis, but are considered in the regulatory evaluation. In its Information Collection Request (ICR) submitted to OMB as part of the NPRM, TSA did consider the costs to respondent covered aircraft operators to modify and maintain systems in order to accommodate the new communication requirements.

*Comment:* Another commenter asked how TSA derived its annual cost estimate to respondents of \$129.2 million in the first three years to modify and maintain systems to accommodate the new communication requirements.

*TSA Response:* In the NPRM, TSA estimated that covered aircraft operators will incur \$125,200,000 in capital startup costs in the first two years and \$4,000,000 for operations and maintenance costs in the second and third years. The estimate of \$129.2 million was the combination of these two cost amounts and represents the total cost for three years, not an annual cost. TSA estimated that the annual average costs will be approximately \$43 million. For this final rule, TSA revised its estimates. TSA estimates that covered aircraft operators will incur \$285,400,000 in capital startup costs in

the first two years and \$9,400,000 for operations and maintenance costs in the second and third years. The estimate of \$294.8 million is the combination of these two cost amounts and represents the total cost for three years, not an annual cost. TSA estimates that the annual average costs for the first three years will be approximately \$98.3 million.

*Comment:* A commenter questioned TSA's time-related burden estimate for transmission of the information covered aircraft operators must collect or request from passengers, which TSA had estimated will take no more than 20 seconds per transaction to collect.

*TSA Response:* After considering this comment and reviewing the information concerning the collection of information, TSA is revising its estimate. TSA now estimates that it will take covered aircraft operators no more than 25 seconds per transaction to collect the information.

## B. Regulatory Impact Analysis

### 1. Regulatory Evaluation Summary

Changes to Federal regulations must undergo several economic analyses. TSA has prepared a separate detailed analysis document, which is available to the public in the docket. Although the regulatory evaluation attempts to mirror the terms and wording of the regulation, no attempt is made to precisely replicate the regulatory language and readers are cautioned that the actual regulatory text, not the text of the evaluation, is binding. With respect to these analyses, TSA provides the following conclusions and summary information. Each of these findings is explained in the corresponding sections which follow:

- *Executive Order 12866 and Significance.* This rulemaking is an economically significant rule within the definition of E.O. 12866, as estimated annual costs or benefits exceed \$100 million in any year. The mandatory OMB Circular A-4, Regulatory Analysis, accounting statement is included in the separate complete analysis and is not repeated here.

- *Final Regulatory Flexibility Analysis (FRFA).* TSA believes that it is unlikely the final rule has a significant economic impact on a substantial number of the small entities subject to this rulemaking. A detailed FRFA is provided in the separate full regulatory analysis.

- *International Trade Assessment.* TSA has assessed the potential effect of this final rule and has determined this rule would not have an adverse impact on international trade.

- *Unfunded Mandates.* This final rule does not contain such a mandate on State, local, and tribal governments. The overall impact on the private sector does not exceed the \$100 million threshold in the aggregate.

### 2. E.O. 12866 Assessment

#### a. Benefits

Benefits of the rule will occur in two phases: the first during operational testing and the second post-implementation. During operational testing, Secure Flight will screen passengers in parallel with the airlines. Primary responsibility for watch list matching will remain with covered aircraft operators during this period, but Secure Flight may notify aircraft operators if its watch list matching technology enables it to detect a potential match the aircraft operator may have missed. Therefore, during the operational testing phase, benefits may include increased aviation security resulting from the detection of threats not identified by covered carriers participating in the testing.

Most of the rule's benefits occur post-implementation. Secure Flight standardizes the watch list matching process across domestic and foreign commercial airlines. Resulting benefits will include more accurate, timely, and comprehensive screening, and a reduction in false positives. This occurs because Secure Flight has access to more initial data with which to distinguish passengers from records in the watch lists than is currently available to airlines. Further, the airlines will be relieved of watch list matching responsibilities, and TSA will be relieved of distributing the watch lists. Together, these factors contribute to the overall objective of focusing resources on passengers identified as potential threats to aviation security.

This benefit is further augmented by the requirement that covered airlines must print on boarding passes a code generated by the Secure Flight system that is unique for each watch list result returned. Depending on the final implementation method, this requirement will, at a minimum, allow checkpoint personnel to verify that a boarding or gate pass has been processed by the Secure Flight system. This will prevent individuals from passing through the checkpoint with a boarding or gate pass that has not originated in an airline system.

By transferring responsibility for watch list matching of international passengers from the CBP system to TSA, the final rule consolidates passenger prescreening operations within DHS,

thereby reducing redundancies between similar programs and facilitating better governance. The rule enables CBP to focus its resources on its mission of protecting U.S. borders while permitting TSA to apply its expertise in watch list matching consistently across all commercial air traffic within and overflying the United States. DHS expects that reducing overlap between these agencies' missions will improve national security through more efficient and targeted use of national resources.

Other benefits include increased security due to the watch list matching of non-traveling individuals who request access to a sterile area. Also, TSA anticipates it may allow airports to authorize non-traveling individuals to enter the airport sterile area. As a result, the final rule establishes requirements related to airports' transmission of data from non-traveling individuals to Secure Flight for watch list matching. These requirements only apply to airports that request and receive authorization from TSA to grant non-traveling individuals access to the airport sterile area.

Once TSA assumes primary responsibility for watch list matching, airlines will be relieved of their passenger watch list matching responsibilities. For the purpose of the estimates in this analysis, TSA assumed that domestic implementation will be completed in the first year of the rule and international implementation will be completed in the second year. However, the actual date the carriers will be completely relieved is unknown and is contingent on several factors, such as the impact of budgetary constraints and the results of operational testing. Prior to full implementation, operational testing will have to demonstrate that Secure Flight does not produce a large number of false positives, processes all matching requests in an efficient and accurate manner, and interfaces with a redress system for passengers who believe they have been incorrectly delayed or denied boarding as a result of Secure Flight matching. Elimination of their watch list matching responsibilities enables airlines to reallocate to other tasks some of their operational resources currently dedicated to comparing passenger information to the watch lists and will offset some costs imposed by the regulation. Due to the difference in resources used by each airline for watch list matching and uncertainty regarding the actual date each will be relieved of watch list duties, TSA was unable to quantify these cost savings.

Further, while TSA conducted significant testing using previously

collected passenger name record (PNR) data, no testing has been completed in a live environment using all of the passenger information requested by this proposed rule. The operational testing phase provides TSA the opportunity to work with the airlines and other stakeholders to refine Secure Flight to achieve optimal results while the airlines continue to have primary responsibility for watch list matching.

TSA has included a rough break-even analysis which indicates the tradeoffs between program cost and program benefits (in the form of impact on baseline risk of a significant aviation-related terror attack) that would be

required for Secure Flight to be a cost beneficial undertaking.

#### b. Costs

All costs in the following summary are discounted present value costs using a 7 percent discount rate over ten years unless noted otherwise. The table below provides totals in constant 2005 dollars as well as totals discounted at 7 percent and 3 percent. Cost tables in section 1.6 of the full regulatory evaluation present year-by-year costs in constant 2005 dollars. Both in this summary and the economic evaluation, descriptive language conveys the consequences of the regulation.

Given the global nature of commercial aviation and the prevalence of airline partnerships, TSA was unable to divide the incidence of the estimated costs between the domestic and foreign economies. Thus, the table below presents the aggregate costs attributable to the Secure Flight final rule. TSA has divided its discussion within each of the cost sections in the regulatory evaluation between domestic and international operations, reflecting the scope and phasing of the rule. However, this distinction between costs accruing to domestic and international operations should not be confused with costs to the domestic and foreign economies.

TABLE B-1—TOTAL AND AVERAGE COSTS  
[Millions]

Cost category	Average annual costs, undiscounted (Low-High)	Average annual costs, discounted 3% (Low-High)	Average annual costs, discounted 7% (Low-High)	10 Year total costs, discounted 3% (Low-High)	10 Year total costs, discounted 7% (Low-High)
Air Carrier Reprogramming Costs .....	\$36.2–\$63.5	\$38.6–\$66.3	\$41.8–\$70.0	\$329.5–\$565.3	\$293.8–\$491.8
Airline Collection Costs .....	10.5–15.7	10.4–15.5	10.3–15.3	88.6–132.4	72.2–107.8
Travel Agency Costs .....	26.1–39.4	26.0–39.3	26.0–39.3	221.9–278.8	182.4–276.1
Federal Costs .....	137.0–167.5	135.9–166.2	134.4–164.5	1,159.3–1418	943.9–1,155.7
Outlay Subtotal Costs .....	209.8–286.1	210.9–287.3	212.5–289.2	1,799.3–2,451.0	1,492.4–2,031.3
Passenger Opportunity Costs .....	79.4–96.2	78.7–95.3	77.8–94.3	671.3–813.1	546.5–662.0
Total Costs .....	289.2–382.2	289.6–382.7	290.3–383.5	2,470.5–3,264.1	2,038.9–2,693.3

TSA estimated a range of possible costs to reflect uncertainty in TSA's assumptions about the additional time the rule adds to the airline reservation process. The summary table above presents the minimum and maximum of this range. TSA did not have sufficient information from industry, however, to determine a likely cost distribution; therefore, the minimum and maximum should be taken as extremes, with the actual cost falling somewhere in between.

TSA estimated the cost impacts of this rulemaking will total from \$2.039 billion to \$2.693 billion over ten years, discounted at 7 percent. At the 7 percent discount rate, air carriers will incur total costs of \$366.0 million to \$599.6 million, and travel agents will incur costs of \$182.4 to \$276.1 million. TSA projected Federal government costs will be from \$943.9 million to \$1.156 billion. The total cost of outlays by all parties, discounted at 7 percent, will be from \$1.492 billion to \$2.031 billion. Additionally, the opportunity costs to individuals (value of time), discounted at 7 percent, will be between \$546.5 and \$662.0 million. The following paragraphs discuss these costs.

Air carriers will incur costs to comply with requirements of this rulemaking.

Over the 10-year period from 2008 to 2017, TSA estimated air carriers will incur average annual costs of \$41.8 to \$70.0 million, discounted at 7 percent, to reprogram their computer systems to accommodate the additional data fields required by the rule and achieve two-way connectivity with TSA and the recurring costs to operate and maintain system modifications. Because the rule requires air carriers to request additional information from passengers, additional time will be required for airline call centers to complete reservations. TSA estimated these costs will be between \$10.3 and \$15.3 million per year. Together, the air carriers' discounted average annual costs will range from \$52.1 to \$85.3 million.

The rule does not directly regulate travel agents. However, the rule requires aircraft operators to ensure that travel agencies request the additional passenger information. Therefore, travel agents, like covered aircraft operators, must spend additional time to complete airline reservations. TSA estimated the average annual cost to travel agents, discounted at 7 percent, will range from \$26.0 to \$39.3 million.

The Federal government incurs several costs as a result of the rule. These costs include network

infrastructure to enable communication between TSA and covered aircraft operator data systems, hardware and software procurement, operations and maintenance, and general support for implementation. The government further incurs costs to complete adjudication of name similarities or watch list matches and also for redress activities. Finally, the government incurs costs to implement a system at checkpoints to verify the codes that the Secure Flight system will issue and the covered aircraft operators will print on boarding and gate passes. The government's estimated average annual cost, discounted at 7 percent, will be from \$134.4 million (\$137.0 million, undiscounted) to \$164.5 million (\$167.5 million, undiscounted).

The final rule also impacts individuals. Time is a valuable economic resource, like labor, capital, and other factors of production, which may be used for work or relaxation. The loss of time imposes an opportunity cost on individuals. TSA attempted to quantify opportunity costs to individuals based on the incremental additional time required to make a reservation. TSA estimated the average annual cost to individuals, discounted at 7 percent, will range from \$77.8

(\$79.4 million, undiscounted) to \$94.3 million (\$96.2 million, undiscounted). Due to program refinements and information gleaned from public

comments, these cost estimates differ in some respects from those reported in the Secure Flight NPRM. The table below

identifies these cost differences and their origins, by the entity bearing the cost.

CHANGES IN SECURE FLIGHT COST ESTIMATES FROM NPRM COST ESTIMATES

Cost component	Undiscounted 10 year total costs (\$millions)			Notes
	NPRM	Final rule	Difference	
Reprogramming Costs to Carriers .....	\$318.5	\$498.8	\$180.3	In response to public comments, carrier reprogramming costs for Secure Flight were increased.
Airline Data Collection Costs .....	104.8	130.7	25.9	In response to public comments, average data collection time for obtaining Secure Flight data elements during telephone reservations was increased from 20 seconds to 25 seconds.
Travel Agency Reprog/Training Costs ..	n/a	16.7	16.7	In response to public comments, first year costs for travel agent training and reprogramming costs for larger travel agencies were included.
Travel Agency Data Collection Costs ...	249.0	310.7	61.7	In response to public comments, average data collection time for obtaining Secure Flight data elements during telephone reservations was increased from 20 seconds to 25 seconds.
Federal Costs .....	1,670.3	1,427.5	(242.8)	Program costs revised based on recent Congressional appropriations; costs change principally in Implementation, Operations Planning and Service Center cost areas.
<b>Total Cash Outlay .....</b>	<b>2,342.6</b>	<b>2,384.4</b>	<b>41.8</b>	
Passenger Opportunity Costs .....	787.3	877.9	90.5	In response to public comments, average time to provide Secure Flight data elements during telephone reservations was increased from 20 seconds to 25 seconds; added complexity risk.
<b>Total Program Costs .....</b>	<b>3,129.9</b>	<b>3,262.3</b>	<b>132.4</b>	

3. Final Regulatory Flexibility Analysis (FRFA)

The Regulatory Flexibility Act of 1980 (RFA) establishes "as a principle of regulatory issuance that agencies shall endeavor, consistent with the objective of the rule and of applicable statutes, to fit regulatory and informational requirements to the scale of the business, organizations, and governmental jurisdictions subject to regulation." To achieve that principle, the RFA requires agencies to solicit and consider flexible regulatory proposals and to explain the rationale for their actions. The Act covers a wide range of small entities, including small businesses, not-for-profit organizations, and small governmental jurisdictions. Agencies must perform a review to determine whether a proposed or final rule will have a significant economic impact on a substantial number of small entities. If the determination is that it will, the agency must prepare a regulatory flexibility analysis as described in the Act.

However, if an agency determines that a proposed or final rule is not expected to have a significant economic impact on a substantial number of small entities, section 605(b) of the RFA

provides that the head of the agency may so certify and a regulatory flexibility analysis is not required. The certification must include a statement providing the factual basis for this determination, and the reasoning should be clear. Although TSA does not believe the final rule will have a significant impact on a substantial number of small entities, the agency has prepared a Final Regulatory Flexibility Analysis (FRFA).

Section 1: Reasons for and Objectives of the Final Rule

2.1.1 Reason for the Final Rule

Section 4012(a) of the Intelligence Reform and Terrorism Prevention Act requires the Transportation Security Administration (TSA) to assume from aircraft operators the function of conducting pre-flight comparisons of airline passenger information to Federal Government watch lists.

2.1.2 Objective of the Final Rule

This rule allows TSA to begin implementation of the Secure Flight program, under which TSA will receive passenger and non-traveler information, conduct watch list matching, and transmit gate and boarding pass printing instructions back to aircraft operators indicating whether individuals should

be cleared to enter the sterile area, marked as selectees, or prohibited from receiving a boarding or gate pass.

Section 2: Affected Small Business Population and Estimated Impact of Compliance

2.2.1 Aircraft Operator Small Business Population

The final Secure Flight rule affects all aircraft operators conducting flight operations under a full security program per 49 CFR 1544.101(a). In general, these aircraft operators are the major passenger airlines that offer scheduled and public charter flights from commercial airports. Specifically, the covered carriers are those performing scheduled service or public charter passenger operations either with an aircraft having a passenger seating configuration of 61 or more seats or having 60 or fewer seats if the aircraft enplanes from or deplanes into a sterile area.

Of the 66 aircraft operators that are covered by the final rule, TSA estimated that 24 of these can be identified as small business entities. This is based on the Small Business Administration (SBA) Office of Size Standards' size standard of "fewer than 1,500

employees” for small businesses within NAICS Code 481111, Scheduled Passenger Air Transportation, and those within NAICS Code 481211, Nonscheduled Chartered Passenger Air Transportation.<sup>29</sup> For this analysis, air carrier employee counts were developed from publicly available information and from carrier filings with the U.S. Department of Transportation’s Bureau of Transportation Statistics (BTS) and Federal Aviation Administration (FAA).

In the Secure Flight regulatory evaluation, TSA divided covered carriers into four “cost groups” based on the nature of their reservations systems and BTS size classification (i.e., major, national, large regional, etc.).<sup>30</sup> These groupings correspond to the estimated costliness of reprogramming airline reservation systems to comply with the Secure Flight requirements.

Implementation Group 1 represents all legacy marketing carriers and their affiliates utilizing an older Global Distribution System (GDS) or host Airline Reservation System (ARS). Legacy airlines, those flying prior to the Airline Deregulation Act of 1978, are all major airlines and have the oldest computer systems. Accordingly, TSA assumed this group incurs the highest compliance costs. Implementation Group 2 includes marketing carriers utilizing a newer GDS or host ARS, as well as national carriers subscribing to an older GDS. Implementation Group 3 represents carriers with independently

maintained reservation systems TSA determined were capable of receiving a direct connection to Secure Flight, as well as regional, commuter, and small airlines subscribing to an older GDS or host ARS. Airlines with very simple or no computerized reservation systems form Group 4. Rather than requiring Group 4 carriers to establish complex systems capable of connecting directly with Secure Flight, TSA allows them to transmit passenger information through a secure Internet portal.

In Groups 1 and 2, smaller airlines often use the reservation systems of larger airlines. For example, a passenger may book a reservation with a large, marketing airline, but the flight may be operated by a smaller airline owned by or contracting with the marketing airline (an affiliate). In such cases, TSA assumed in its regulatory evaluation that the marketing airline bears the cost of changes to the reservation system and designated those carriers as “points of implementation.” Section 1.4.1 of the regulatory evaluation describes this distinction in greater detail.

In the discussion below, TSA relaxes this assumption and treats affiliate carriers as if they are marketing carriers. Since no Group 1 affiliate carriers are major airlines, they were re-categorized as Group 3 carriers (regional, commuter, or small carriers using an older GDS). Specifically, these are Carriers 3, 4, 8, and 9 in the tables.<sup>31</sup> Although this method ensures a potential cost is

estimated for all small business carriers, TSA notes that it likely overstates the actual cost that will be incurred. Thus, for this small business analysis, TSA considers ten carriers under Implementation Groups 2 and 3. The remaining 14 carriers belong to Group 4.

Table 2.2.1.a reports annual 2005 employment and operating revenues or sales<sup>32</sup> TSA gathered for these 24 airlines (in one case the financial data are from 2002). These small air carriers are active in different areas of the passenger air transportation marketplace. Some provide scheduled passenger service in small niche markets, often as part of the larger route system of an established hub and spoke carrier; others provide charter transportation services to tour groups or organizations such as professional sports teams. Some of those that provide scheduled passenger services use reservation systems hosted by one of the existing ARS providers, while others handle phone reservations or receive reservations from travel agents. All of these small airlines are subject to the rule, however, due to the size of aircraft they use and/or because of the airport environments in which they operate. Thus, these airlines will collect more information from passengers, but TSA will take over their current requirement to compare passenger manifests to the watch lists.

TABLE 2.2.1.A—SECURE FLIGHT SMALL BUSINESS AIR CARRIERS  
[2005 Data]

Small business carrier ID No.	Employees (total full- and part-time)	Annual operating revenues	Enplanements	Share of total covered carrier enplanements (percent)
<b>Aircraft Operators in Implementation Groups 2 and 3</b>				
1 .....	914	\$204,000,000	1,266,293	0.199
2 .....	893	80,300,000	1,132,207	0.178
3 .....	546	78,100,000	838,959	0.051
4 .....	545	60,000,000	440,865	0.069
5 .....	400	45,100,000	636,768	0.100
6 .....	380	42,800,000	570,291	0.090
7 .....	255	18,600,000	49,242	0.008
8 .....	230	39,600,000	355,607	0.056
9 .....	220	24,000,000	141,252	0.022
10 .....	50	5,000,000	48,221	0.008
<b>Aircraft Operators in Implementation Group 4</b>				
11 .....	964	\$74,300,000	208,120	0.033
12 .....	826	76,392,000	344,741	0.054
13 .....	739	137,900,000	506,292	0.080
14 .....	600	68,600,000	91,571	0.014

<sup>29</sup> Small Business Administration. Table: “Small Business Size Standards matched to North American Industry Classification System.” Available at <http://www.sba.gov/size/sizetable2002.html>. Accessed May 4, 2006.

<sup>30</sup> For more information, please see section 1.4.1.

<sup>31</sup> Since in some cases the reported revenue data are proprietary, TSA substituted an ID number in place of company names.

<sup>32</sup> In cases for which annual revenues were not available, carrier filings of total annual sales were used as a proxy for revenue.

TABLE 2.2.1.A—SECURE FLIGHT SMALL BUSINESS AIR CARRIERS—Continued  
[2005 Data]

Small business carrier ID No.	Employees (total full- and part-time)	Annual operating revenues	Enplanements	Share of total covered carrier enplanements (percent)
15 .....	593	132,500,000	836,409	0.132
16 .....	549	33,400,000	329,418	0.052
17 .....	411	105,266,000	82,529	0.013
18 .....	220	6,330,000	18,707	0.003
19 .....	212	35,649,000	329,083	0.052
20 .....	159	12,000,000	35,788	0.006
21 .....	75	14,230,000	22,511	0.004
22 .....	19	930,000	(a)	(a)
23 .....	(a)	(a)	38,471	0.006
24 .....	(a)	(a)	17,521	0.003

<sup>a</sup> Unavailable.

### 2.2.2 Estimated Impact to Aircraft Operator Small Businesses

TSA determined that the rule does not cause a significant economic impact for a substantial number of these small business entities based on several considerations. First, under the current procedures, these small airlines must devote effort to matching passenger identification information to TSA watch lists but are not able to establish staff and back office activities that are dedicated to these security functions due to the small scale of their operations. Instead, the existing security responsibilities are fulfilled by airline personnel who may have other unrelated duties. These scale considerations suggest that the benefits of changing the current responsibilities by implementing the rule may be weighted toward these smaller airlines, when considered on a per enplanement basis.

In addition, given the variety of business activities pursued by the small carriers under consideration—scheduled passenger operations or charter operations, operations that collaborate with a larger hub and spoke carrier or that are independent of larger carriers, and operations that do or do not make use of an existing ARS host for processing reservations—it is difficult to estimate the costs that are incurred by these small carriers when the rule is implemented. In order to evaluate the possible economic impact of the rule on small aircraft operators, TSA utilized two calculation methods: one for

carriers in Groups 2 and 3 and a second for carriers in Group 4.

Since reprogramming and data collection costs have already been presented in the aggregate for Groups 2 and 3 in sections 1.6.2 and 1.6.3 of the regulatory evaluation, TSA used the same techniques to calculate the potential impact to small business carriers in these two groups. Table 2.2.2.a below shows the outcome of these calculations.

TSA first assigned an estimated initial reprogramming cost to each small business carrier based on whether it belonged to Group 2 or 3 (column B). The initial reprogramming cost was used since this is the highest expenditure in any one year. Each carrier will also experience an increase in the time required to collect passenger data during reservations, as discussed in section 1.6.3. To arrive at the maximum annual collection cost (column D), TSA annualized the total High Scenario Airline Collection Costs from Table 1.6.3.a. These airline collection costs are a function of reservations and TSA assumed an airline's share of reservations is proportional to its share of enplanements. Thus, TSA multiplied the total annual collection cost by each carrier's share of enplanements (column C) to arrive at its proportion of the annual collection cost (column E). Adding the collection cost to the initial reprogramming cost yielded a per-carrier estimated cost of compliance (column F). TSA divided these estimated compliance costs by each

carrier's reported revenue to determine the percent of revenue that will be expended on Secure Flight (column G).

Although there is no hard and fast definition for "significant economic impact," agencies frequently use 2 percent of an entity's revenue as a threshold. As can be seen in the table, in one case the estimated compliance cost exceeds 2 percent of the carriers' reported 2005 revenues and in one case it exceeds 8 percent. After reviewing the relevant information, however, TSA determined the threshold may not be applicable in this particular case. This is because the percentage is extremely sensitive to the estimated reprogramming cost (column B). TSA's estimated reprogramming costs for these carriers are based on assumptions about limited data and may overstate the costs to smaller carriers. This consideration is especially true of carrier ten. This carrier maintained its own reservation system until August 2005, when it began subscribing to a GDS. Consequently, its reprogramming costs may be significantly lower than projected here. Further, these carriers have the option to use the Secure Flight Web interface rather than reprogram their reservation systems if they determine reprogramming to be too costly.

Based on these considerations, TSA determined the estimated compliance cost likely does not meet the requirements of a significant economic impact under the RFA.

TABLE 2.2.2.A—ESTIMATED SMALL BUSINESS IMPACT, CARRIER GROUPS 2 AND 3

Small business carrier ID No.	2005 annual operating revenues (000)	Estimated carrier re-program costs (000)	Share of total covered carrier enp (percent)	Annualized airline collection costs* (000)	Share of airline collection costs* (000)	Estimated total compliance cost* (000)	Compliance cost as % of revenues*
	(A)	(B)	(C)	(D)	(E) = C*D	(F) = B+E	(G) = F/A
1 .....	\$204,000	\$850	0.20	\$11,690	\$23	\$873	0.43
2 .....	80,300	425	0.18	11,690	21	446	0.56
3 .....	78,100	425	0.13	11,690	15	440	0.56
4 .....	60,000	425	0.07	11,690	8	433	0.72
5 .....	45,100	425	0.10	11,690	12	437	0.97
6 .....	42,800	425	0.09	11,690	11	436	1.02
7 .....	18,600	425	0.01	11,690	1	426	2.29
8 .....	39,600	425	0.06	11,690	7	432	1.09
9 .....	24,000	425	0.02	11,690	2	427	1.78
10 .....	5,000	425	0.01	11,690	1	426	8.52

\* Reflect totals from the high case scenario presented in the regulatory evaluation.

As discussed in section 1.6.2 of the regulatory evaluation, TSA assumed Group 4 carriers will not have any reprogramming costs associated with implementation of Secure Flight but that 13 of the 16 Group 4 carriers will spend \$100,000 in the first year of the program on staff retraining and customer outreach. TSA did not have sufficient information, however, to reliably estimate costs incurred by these carriers due to changes in their reservation process. For the purpose of discussion, TSA here calculates a unit compliance cost per enplanement in order to illustrate the average impact of the rule. The results of this calculation are shown in Table 2.2.2.b.

TSA chose to use a broad assumption in developing its unit cost and therefore included the annual costs related to the entire reservations process for air transportation providers. As reported in Tables 1.6.3.a and 1.6.4.a, costs

associated with the reservations process include airline and travel agency costs to make available privacy notices and request additional passenger information. In TSA's high scenario, these two categories total to approximately \$34.2 million in fiscal year 2008. This value can be normalized to a per enplanement basis using the reservations forecast reported in Table 1.4.1.a, which totals 672.1 million in 2008. This normalized cost per enplanement equals  $\$34.2/672.1$ , or about \$0.05 per enplanement (column B).

Multiplying this normalized value by each carrier's 2005 annual enplanements total (column B) and adding in the implementation expenditure where applicable (column A), TSA estimated the cost to each of the small business entities identified (column D). As column F of Table 2.2.2.b indicates, this estimate for costs

never exceeds 2 percent of 2005 annual revenues for these small carriers. Note further that the annual enplanements value is unadjusted for round trip itineraries or for reservations that may have been generated as part of a marketing carrier's reservations process. Thus, the estimated values in Table 2.2.2.b are very likely to be overstatements of the impact of the rule on these small carriers.

Finally, as noted previously, DHS will make available a Secure Flight Internet portal for the transmittal of passenger and other itinerary data from Group 4 small airlines to TSA. The availability of this interface simplifies the transition to the environment that will prevail once the rule is implemented, while providing greater assurance regarding the provision of the relevant security data to TSA for comparison to the watch lists.

TABLE 2.2.2.B—ILLUSTRATIVE SMALL BUSINESS IMPACT, CARRIER GROUP 4

Small business carrier ID No.	Assumed start-up outlay	FY 2005 enplanements	Maximum unit compliance cost per enplanement	Compliance cost	2005 Annual operating revenues	Compliance cost as % of 2005 revenues
	(A)	(B)	(C)	(D) = A+B*C	(E)	(F) = D/E
11 .....	\$100,000	208,120	\$0.05	\$110,400	\$74,300,000	0.15
12 .....	100,000	344,741	0.05	117,200	76,392,000	0.15
13 .....	100,000	506,292	0.05	125,300	137,900,000	0.09
14 .....	100,000	91,571	0.05	104,600	68,600,000	0.15
15 .....	100,000	836,409	0.05	141,800	132,500,000	0.11
16 .....	100,000	329,418	0.05	116,500	33,400,000	0.35
17 .....	100,000	82,529	0.05	104,100	105,265,872	0.10
18 .....	100,000	18,707	0.05	100,900	6,330,280	1.59
19 .....	100,000	329,083	0.05	116,500	35,649,201	0.33
20 .....	100,000	35,788	0.05	101,800	12,000,000	0.85
21 .....	100,000	22,511	0.05	101,100	14,229,510	0.71
22 .....	0	0*	0.05	0	930,000	(**)
23 .....	0	38,471	0.05	1,900	0	(**)
24 .....	0	17,521	0.05	900	0	(**)

\* Carrier had not yet begun reporting enplanements to BTS.

\*\* Data not available.



The estimates provided in Table 2.2.2.b show how Group 4 small businesses would be impacted by Secure Flight were their operations comparable to those of airlines in Groups 1 through 3. As has been noted above, however, this is not the case. Consequently, the costs Group 4 airlines actually incur to comply with Secure Flight may diverge significantly from the estimates presented. Nevertheless, the table illustrates that these costs

would have to increase dramatically before they would constitute a significant economic impact.

2.2.3 Travel Agency Small Business Population

The Small Business Administration (SBA) classifies any travel agency as a small business if it has revenues of less than \$3.5 million annually.<sup>33</sup> The SBA data provided in Table 2.2.3.a indicate that in 2003 more than 98 percent of travel agencies had annual revenues less

than \$5 million. Although the division of the SBA revenue categories do not allow for a precise count of the number of small businesses, the average revenue per firm of \$1.9 million for the \$1 million to \$5 million category indicates that many of the firms in this category have revenues below the \$3.5 million threshold. Consequently, the discussion of small businesses in the travel agency industry will be a discussion about the vast number of firms.

TABLE 2.2.3.A—DISTRIBUTION OF TRAVEL AGENCIES (NAICS 561510) BY REVENUE, 2003<sup>34</sup>

	Total	\$0– \$99,999	\$100,000– \$499,999	\$500,000– \$999,999	\$1,000,000– \$4,999,999	Total <\$5,000,000	Total >\$5,000,000
Number of Firms .....	14,838	6,125	6,627	1,098	714	14,564	274
Percent of Total .....	100.00	41.28	44.66	7.40	4.81	98.15	1.85

Tables 2.2.3.b through 2.2.3.d below reflect the recent story of the travel agent industry. The first two tables are based on 2002 data provided by the Airlines Reporting Corporation (ARC) to the National Commission to Ensure Consumer Information and Choice in the Airline Industry (the Commission).

When the Commission prepared its report “Upheaval in Travel Distribution: Impact on Consumers and Travel Agents, Report to Congress and the

President” (Commission Report), the SBA had just increased the small business revenue threshold from \$1 million to \$3 million for travel agents. Consequently, the Commission used \$5 million in total revenue (approximately \$2.5 million in commission and fee revenue) as a proxy threshold for small businesses when creating Tables 2.2.3.b and 2.2.3.c below. Although these tables do not capture the full universe of travel agency small businesses, they

nevertheless illustrate general trends affecting these entities.

As can be seen in Tables 2.2.3.b and 2.2.3.c, the number of travel agencies whose sales are less than \$5 million per year declined steadily through 2001. Correspondingly, the share of industry sales by these smaller firms also fell. At the same time, however, the largest firms increased both their share of industry sales and the dollar value of their sales.

TABLE 2.2.3.B—NUMBER OF TRAVEL AGENCIES BY SIZE CATEGORY<sup>35</sup>

Agency size	1995	1997	1999	2001
\$2M or Less .....	19,851	19,226	17,855	15,253
\$2M–\$5M .....	2,356	2,803	2,482	1,770
\$5M–\$50M .....	1,059	1,277	1,236	1,015
Greater than \$50M .....	77	107	117	117
Total .....	23,343	23,413	21,690	18,425

TABLE 2.2.3.C—SHARE OF TRAVEL AGENT SALES BY SIZE CATEGORY<sup>36</sup>  
[Percent]

Agency size	1995	1997	1999	2001
\$2M or Less .....	25.3	20.6	16.9	14.2
\$2M–\$5M .....	13.5	12.8	10.7	8.4
\$5M–\$50M .....	24.8	24.5	22.5	20.1
Greater than \$50M .....	36.4	42.1	49.9	57.2

Table 2.2.3.d shows aggregate monthly statistics released by the Airlines Reporting Corporation

indicating that the travel agent industry continued to contract and consolidate

through 2005. Corresponding revenue data, however, were not available.

<sup>33</sup> Small Business Administration. Table: “Small Business Size Standards matched to North American Industry Classification System.” Available at <http://www.sba.gov/size/size2002.html>. Note: The SBA size standard for travel agencies is based on “total revenues,

excluding funds received in trust for an unaffiliated third party, such as bookings or sales subject to commissions. The commissions received are included as revenue.”

<sup>34</sup> Small Business Administration. Table: “All Industries by NAICS codes, 2003.” See TXT file

“2003” available at <http://www.sba.gov/advo/research/data.html>.

<sup>35</sup> Commission Report, p. 114.

<sup>36</sup> Ibid.

TABLE 2.2.3.D—TRAVEL AGENCIES ACCREDITED BY THE AIRLINES REPORTING CORPORATION<sup>37</sup>

	2001	2002	2003	2004	2005
Retail Locations .....	27,633	24,679	22,244	20,729	19,871
Home Offices .....	1,651	1,368	1,203	1,118	1,041
Independent/Single Entities .....	15,057	13,206	11,670	10,578	9,874
Branch .....	6,696	6,171	5,695	5,474	5,451
Restricted Access .....	862	950	1,039	1,120	1,205
On-site branch .....	3,367	2,984	2,637	2,439	2,300
Satellite Ticket Providers .....	6,347	4,693	3,204	2,413	1,975
Corporate Travel Departments .....	108	150	172	182	197
<b>TOTAL LOCATIONS</b> .....	<b>34,088</b>	<b>29,522</b>	<b>25,620</b>	<b>23,324</b>	<b>22,043</b>
Change over previous year (percent) .....	N/A	-13.39	-13.22	-8.96	-5.49
<b>TOTAL ENTITIES*</b> .....	<b>17,678</b>	<b>15,674</b>	<b>14,084</b>	<b>12,998</b>	<b>12,317</b>
Change over previous year (percent) .....	N/A	-11.34	-10.14	-7.71	-5.24

\*Sum of Home Offices, Independent/Single Entities, Restricted Access, and Corporate Travel Departments.

#### 2.2.4 Estimated Impact to Travel Agency Small Businesses

While not directly regulated, small travel agencies will certainly be affected by the implementation of Secure Flight. TSA anticipated the most significant burden on these entities results from the increased time to collect additional passenger information. Small travel agencies may also incur incremental costs due to retraining of staff and reaching out to clients in order to update customer profiles prior to their next trip.

In section 1.6.4 of the regulatory evaluation, TSA estimated a cost that is borne by non-Internet (brick-and-mortar) travel agencies as a result of the requirements. Detailed industry data did not exist, however, that would allow TSA to determine the portion of that cost that is borne by small travel agencies. In lieu of such information, TSA chose to calculate a minimum number of airline reservations the smallest travel agency size category would have to process in order for the requirements of the rule to result in a "significant economic impact." This calculation corresponds to the high

estimate scenario and depends on a number of assumptions:

1. The average hourly wage of small business travel agents is \$20.69 (including benefits).
2. In TSA's highest cost scenario, an additional 30 seconds per airline reservation is needed to collect additional passenger information.
3. The additional time to collect passenger information will be incurred for every airline reservation booked through a travel agency.

4. The average revenue of the smallest travel agency firms (revenues between \$0 and \$99,999) is \$47,204.<sup>38</sup>

5. Two percent of a small travel agency's revenue constitutes a "significant economic impact." Accepting these assumptions, 2 percent of the smallest firm revenue would constitute an impact of \$942 ( $\$47,204 \times 0.02$ ). Reversing the calculations used in section 1.6.4, this total must be converted into the additional reservation time it represents. This is accomplished by dividing \$942 by the travel agent hourly wage, which yields 45.5 hours ( $\$942 \div \$20.69/\text{hour}$ ). This cumulative 45.5 hours can then be broken down into individual

reservations by dividing by the total incremental time per reservation, which is 0.008 hours (30 incremental seconds  $\div$  3600 seconds/hour). Thus, 45.5 hours represent approximately 5,690 airline reservations (45.5 hours  $\div$  0.008 hours/reservation). Under the most burdensome scenario, then, on average the smallest travel agencies would need to book 5,690 airline reservations in a year in order to potentially incur a significant economic impact as a result of the final rule.

Table 2.2.4.a presents this threshold number of reservations for the range of data collection times presented in the Secure Flight regulatory evaluation. Alternatively, the table also presents the number of airline reservations a travel agency would have to process to meet 2 percent of the SBA small business threshold for travel agencies.

These estimates below should be considered as a range of "worst case scenarios." For example, reservations made for clients for whom a travel agency already has the requested Secure Flight information saved in a profile will not incur the additional data collection time.

TABLE 2.2.4.A—AIRLINE RESERVATIONS THRESHOLD FOR SMALL BUSINESS TRAVEL AGENCIES

	Revenue class \$0-\$99,999			SBA small business threshold		
	High	Primary	Low	High	Primary	Low
Firm Revenue (A) .....	\$47,120			\$3,500,000		
2% of Revenue (B) .....	\$942			\$70,000		
Average Agent Hourly Wage (C) .....	\$20.69			\$20.69		
Total Incremental Hours (D) = B/C .....	45.5			3,383.5		
<b>Estimate Scenario</b>	<b>High</b>	<b>Primary</b>	<b>Low</b>	<b>High</b>	<b>Primary</b>	<b>Low</b>
Additional Hours per Reservation (E) .....	0.008 (30 sec.)	0.006 (20 sec.)	0.003 (10 sec.)	0.008 (30 sec.)	0.006 (20 sec.)	0.003 (10 sec.)

<sup>37</sup> "End of Year Reporting and Settlement Results," Airlines Reporting Corporation press release, December 2002, December 2003, December

2004, December 2005. Available at [http://www.arccorp.com/regist/news\\_sales\\_doc\\_stats.jsp](http://www.arccorp.com/regist/news_sales_doc_stats.jsp).

<sup>38</sup> Small Business Administration. Table: "All Industries by NAICS codes, 2003." See TXT file

"2003" available at <http://www.sba.gov/advo/research/data.html>. Estimated receipts divided by number of firms, revenue class 0-99,999.

Estimate Scenario	High	Primary	Low	High	Primary	Low
Reservations (F) = D/E .....	5,690	7,580	15,170	422,900	563,900	1,127,800

**Section 3: Significant Alternatives Considered**

The final rule provides small business carriers the flexibility of either reprogramming their reservation systems to interface directly with the Secure Flight system or to transmit passenger and non-traveler information to Secure Flight through a secure Internet interface. Thus, small business carriers identified in Groups 2 and 3 have the option of joining Group 4 and using the Internet portal if they determine reprogramming their systems to communicate directly with Secure Flight is too costly. Similarly, small business carriers TSA has identified in this analysis as scheduled to use the Secure Flight Internet portal have the option to reprogram their systems to communicate directly with Secure Flight if they determine using the portal is too burdensome on their business processes.

While either method imposes some costs on small businesses, TSA determined that exempting these carriers from the requirements of the rule would fail to meet the mandate within the IRTPA that TSA assume the watch list matching function. Taking this into consideration, TSA determined the options described above would effectively minimize the impact to small businesses.

**Section 4: Identification of Duplicative or Overlapping Federal Rules**

TSA is aware that other Federal agencies, such as the Centers for Disease Control and Prevention (CDC) and Customs and Border Protection (CBP), collect data concerning aviation passengers and may conduct or will conduct watch list matching for these passengers. TSA is working with other agencies, including the CDC and CBP, to develop ways to eliminate unnecessary duplication of comparable screening efforts and thereby reduce governmental and private sector costs. Therefore, the rule allows TSA to relieve covered aircraft operators of the requirement to transmit passenger information if TSA determines that the U.S. government is conducting watch list matching for a passenger on a particular flight that is comparable to the screening conducted pursuant to part 1560. TSA will work with each covered aircraft operator to establish the specific procedures and times for these transmissions as it

**develops its Aircraft Operator Implementation Plan.**

**Section 5: Final Determination of No Significant Impact**

Based on the considerations above, TSA believes that it is unlikely the final rule has a significant economic impact on a substantial number of the small entities subject to this rulemaking. In conducting this analysis, TSA acknowledges that the ability of carriers to share the incidence of security costs with their customers has been limited.

While not required by the RFA, TSA has also considered the potential impact to small business travel agencies, as these entities are likely to be indirectly impacted by the rule given their role in the airline reservation process. TSA does not believe the final rule will have a significant economic impact on a substantial number of these small business travel agencies.

**C. International Trade Impact Assessment**

The Trade Agreement Act of 1979 prohibits Federal agencies from engaging in any standards or related activities that create unnecessary obstacles to the foreign commerce of the United States. Legitimate domestic objectives, such as security, are not considered unnecessary obstacles. The statute also requires consideration of international standards and, where appropriate, that they be the basis for U.S. standards. In addition, consistent with the Administration's belief in the general benefits and desirability of free trade, it is the policy of TSA to remove or diminish, to the extent feasible, barriers to international trade, including both barriers affecting the export of American goods and services to foreign countries and barriers affecting the import of foreign goods and services into the United States. TSA has assessed the potential effect of this rulemaking and has determined that it does not create barriers to international trade.

**D. Unfunded Mandates Assessment**

The Unfunded Mandates Reform Act of 1995 is intended, among other things, to curb the practice of imposing unfunded Federal mandates on State, local, and tribal governments. Title II of this Act requires each Federal agency to prepare a written statement assessing the effects of any Federal mandate in a proposed or final agency rule that may result in an expenditure of \$100 million

or more (adjusted annually for inflation) in any one year by State, local, and tribal governments, in the aggregate, or by the private sector. Such a mandate is deemed to be a "significant regulatory action." This final rule does not contain such a mandate on State, local, and tribal governments. The overall impact on the private sector does exceed the \$100 million threshold in the aggregate. The full regulatory evaluation documents the costs, alternatives, and TSA accommodation of the public comments.

**E. Executive Order 13132, Federalism**

TSA has analyzed this final rule under the principles and criteria of Executive Order 13132, Federalism. We determined that this action will not have a substantial direct effect on the States, on the relationship between the Federal government and the States, or on the distribution of power and responsibilities among the various levels of government, and therefore, does not have federalism implications.

**F. Environmental Analysis**

TSA has analyzed this final rule under the Department of Homeland Security (DHS) Management Directive 5100.1, "Environmental Planning Program" (see also 71 FR 16790, April 4, 2006), which guides TSA compliance with the National Environmental Policy Act of 1969 (NEPA) (42 U.S.C. 4321-4370f). TSA has determined that this final rule is categorically excluded from further NEPA analysis under the following categorical exclusions (CATEXs) listed in MD 5100.1, Appendix A, Table 1:

- Administrative and Regulatory Activities:
  - CATEX A3 (Promulgation of rules, issuance of rulings or interpretations and the development and publication of policies that implement, without substantive change, statutory or regulatory requirements);
  - CATEX A4 (Information gathering, data analysis and processing, information dissemination, review, interpretation and development of documents).
    - Operational Activities:
      - CATEX B3 (Proposed activities and operations conducted in an existing structure that would be compatible with and similar in scope to ongoing functional uses).
      - Unique Categorical exclusions for TSA:

• CATEX H1 (Approval or disapproval of security plans required under legislative or regulatory mandates unless such plans would have a significant effect on the environment).

Additionally, TSA has determined that no extraordinary circumstances exist (see MD 5100.1, Appendix A, paragraph 3.B.(1)–(3)) which would limit the application of a CATEX with regard to these activities.

#### G. Energy Impact

The energy impact of this action has been assessed in accordance with the Energy Policy and Conservation Act (EPCA) Public Law 94–163, as amended (42 U.S.C. 6362). We have determined that this rulemaking is not a major regulatory action under the provisions of the EPCA.

#### H. International Compatibility

In keeping with U.S. obligations under the Convention on International Civil Aviation, it is TSA's policy to comply with International Civil Aviation Organization (ICAO) Standards and Recommended Practices to the maximum extent practicable. TSA has determined that there are no ICAO Standards and Recommended Practices that correspond to the regulatory standards established by this final rule. TSA has assessed the potential effect of this rulemaking and has determined that it does not create barriers to international trade.

However, when TSA reviewed the impact of foreign carrier overflights, the conclusion is not clear. The right of airlines from one country to overfly another country in the course of traveling to the destination country is the first of the well known "freedoms of the air." This technical freedom has been engrained in international aviation since the Chicago Convention of 1944, qualified, however, by the right of countries to regulate the airspace over their territory. How countries might react to the new conditions being placed on the fulfillment of this freedom is uncertain. International trade in travel and international shipping may be negatively impacted should foreign countries choose to respond in a retaliatory manner. One response by foreign carriers might be to avoid overflying the U.S. entirely, thereby lengthening flight routes and the costs of operation to those carriers. These re-routings would change airline costs and thus contribute to fare increases, which would affect trade between the departure and arrival countries, even though it would not directly affect trade involving the U.S. If the foreign carrier response is to reroute, it is not clear that

such a change would eliminate all risks, since aircraft skirting the boundaries of U.S. airspace could be redirected into U.S. airspace by hijackers or terrorists.

#### List of Subjects

##### 49 CFR Part 1540

Air carriers, Aircraft, Airports, Civil aviation security, Law enforcement officers, Reporting and recordkeeping requirements, Security measures.

##### 49 CFR Part 1544

Air carriers, Aircraft, Aviation safety, Freight forwarders, Incorporation by reference, Reporting and recordkeeping requirements, Security measures.

##### 49 CFR Part 1560

Air carriers, Aircraft, Reporting and recordkeeping requirements, Security measures.

#### The Amendments

■ For the reasons set forth in the preamble, the Transportation Security Administration amends Chapter XII, of Title 49, Code of Federal Regulations to read as follows:

#### Subchapter C—Civil Aviation Security

##### PART 1540—CIVIL AVIATION SECURITY: GENERAL RULES

■ 1. The authority citation for part 1540 continues to read as follows:

**Authority:** 49 U.S.C. 114, 5103, 40113, 44901–44907, 44913–44914, 44916–44918, 44935–44936, 44942, 46105.

■ 2. Revise § 1540.107 to read as follows:

##### Subpart B—Responsibilities of Passengers and Other Individuals and Persons

##### § 1540.107 Submission to screening and inspection.

(a) No individual may enter a sterile area or board an aircraft without submitting to the screening and inspection of his or her person and accessible property in accordance with the procedures being applied to control access to that area or aircraft under this subchapter.

(b) An individual must provide his or her full name, as defined in § 1560.3 of this chapter, date of birth, and gender when—

(1) The individual, or a person on the individual's behalf, makes a reservation for a covered flight, as defined in § 1560.3 of this chapter, or

(2) The individual makes a request for authorization to enter a sterile area.

(c) An individual may not enter a sterile area or board an aircraft if the

individual does not present a verifying identity document as defined in § 1560.3 of this chapter, when requested for purposes of watch list matching under § 1560.105(c), unless otherwise authorized by TSA on a case-by-case basis.

##### PART 1544—AIRCRAFT OPERATOR SECURITY: AIR CARRIERS AND COMMERCIAL OPERATORS

■ 3. The authority citation for part 1544 continues to read as follows:

**Authority:** 49 U.S.C. 114, 5103, 40113, 44901–44905, 44907, 44913–44914, 44916–44918, 44932, 44935–44936, 44942, 46105.

■ 4. Amend § 1544.103 by adding new paragraph (c)(22) to read as follows:

##### Subpart B—Security Program

##### § 1544.103 Form, content, and availability.

\* \* \* \* \*

(c) \* \* \*

(22) The Aircraft Operator Implementation Plan (AOIP) as required under 49 CFR 1560.109.

■ 5. Add a new part 1560, to read as follows:

##### PART 1560—SECURE FLIGHT PROGRAM

##### Subpart A—General

Sec.

1560.1 Scope, purpose, and implementation.

1560.3 Terms used in this part.

##### Subpart B—Collection and Transmission of Secure Flight Passenger Data for Watch List Matching

1560.101 Request for and transmission of information to TSA.

1560.103 Privacy notice.

1560.105 Denial of transport or sterile area access; Designation for enhanced screening.

1560.107 Use of watch list matching results by covered aircraft operators.

1560.109 Aircraft Operator Implementation Plan.

1560.111 Covered airport operators.

##### Subpart C—Passenger Redress

1560.201 Applicability.

1560.203 Representation by counsel.

1560.205 Redress process.

1560.207 Oversight of process.

**Authority:** 49 U.S.C. 114, 40113, 44901, 44902, 44903.

##### Subpart A—General

##### § 1560.1 Scope, purpose, and implementation.

(a) *Scope.* This part applies to the following:

(1) Aircraft operators required to adopt a full program under 49 CFR 1544.101(a).

(2) Foreign air carriers required to adopt a security program under 49 CFR 1546.101(a) or (b).

(3) Airport operators that seek to authorize individuals to enter a sterile area for purposes approved by TSA.

(4) Individuals who seek redress in accordance with subpart C of this part.

(b) *Purpose.* The purpose of this part is to enhance the security of air travel within the United States and support the Federal government's counterterrorism efforts by assisting in the detection of individuals identified on Federal government watch lists who seek to travel by air, and to facilitate the secure travel of the public. This part enables TSA to operate a watch list matching program known as Secure Flight, which involves the comparison of passenger and non-traveler information with the identifying information of individuals on Federal government watch lists.

(c) *Implementation.* Each covered aircraft operator must begin requesting the information described in § 1560.101(a)(1) and have the capability to transmit SFPD to TSA in accordance with its Aircraft Operator Implementation Plan (AOIP) as approved by TSA. Each covered aircraft operator must begin transmitting information to TSA as required in § 1560.101(b) on the date specified in, and in accordance with, its AOIP as approved by TSA. TSA will inform each covered aircraft operator 60 days prior to the date on which TSA will assume the watch list matching function from that aircraft operator.

### § 1560.3 Terms used in this part.

In addition to the terms in §§ 1500.3 and 1540.5 of this chapter, the following terms apply to this part:

*Aircraft Operator Implementation Plan* or *AOIP* means a written procedure describing how and when a covered aircraft operator or airport operator transmits passenger and flight information and non-traveler information to TSA, as well as other related matters.

*Airport code* means the official code, designated by the International Air Transport Association (IATA), for an airport.

*Consolidated User Guide* means a document developed by the Department of Homeland Security (DHS) to provide guidance to aircraft operators that must transmit passenger information to one or more components of DHS on operational processing and transmission of passenger information to all required components in a unified manner. The Consolidated User Guide is part of the

covered aircraft operator's security program.

*Covered aircraft operator* means each aircraft operator required to carry out a full program under 49 CFR 1544.101(a) or a security program under 49 CFR 1546.101(a) or (b).

*Covered airport operator* means each airport operator that seeks to authorize non-traveling individuals to enter a sterile area for a purpose permitted by TSA.

*Covered flight* means any operation of an aircraft that is subject to or operates under a full program under 49 CFR 1544.101(a). *Covered flight* also means any operation of an aircraft that is subject to or operates under a security program under 49 CFR 1546.101(a) or (b) arriving in or departing from the United States, or overflying the continental United States. *Covered flight* does not include any flight for which TSA has determined that the Federal government is conducting passenger matching comparable to the matching conducted pursuant to this part.

*Date of birth* means the day, month, and year of an individual's birth.

*Department of Homeland Security Traveler Redress Inquiry Program* or *DHS TRIP* means the voluntary program through which individuals may request redress if they believe they have been:

- (1) Denied or delayed boarding transportation due to DHS screening programs;
- (2) Denied or delayed entry into or departure from the United States at a port of entry; or
- (3) Identified for additional (secondary) screening at U.S. transportation facilities, including airports, and seaports.

*Full name* means an individual's full name as it appears on a verifying identity document held by the individual.

*Inhibited status* means the status of a passenger or non-traveling individual to whom TSA has instructed a covered aircraft operator or a covered airport operator not to issue a boarding pass or to provide access to the sterile area.

*Itinerary information* means information reflecting a passenger's or non-traveling individual's itinerary specified in the covered aircraft operator's AOIP. For non-traveling individuals, itinerary information is the airport code for the sterile area to which the non-traveler seeks access. For passengers, itinerary information includes the following:

- (1) Departure airport code.
- (2) Aircraft operator.
- (3) Scheduled departure date.
- (4) Scheduled departure time.
- (5) Scheduled arrival date.

(6) Scheduled arrival time.

(7) Arrival airport code.

(8) Flight number.

(9) Operating carrier (if available).

*Known Traveler Number* means a unique number assigned to an individual for whom the Federal government has conducted a security threat assessment and determined does not pose a security threat.

*Non-traveling individual* or *non-traveler* means an individual to whom a covered aircraft operator or covered airport operator seeks to issue an authorization to enter the sterile area of an airport in order to escort a minor or a passenger with disabilities or for some other purpose permitted by TSA. The term *non-traveling individual* or *non-traveler* does not include employees or agents of airport or aircraft operators or other individuals whose access to a sterile area is governed by another TSA requirement.

*Overflying the continental United States* means departing from an airport or location outside the United States and transiting the airspace of the continental United States en route to another airport or location outside the United States. Airspace of the continental United States includes the airspace over the lower 48 states of the United States, not including Alaska or Hawaii, and the airspace overlying the territorial waters between the U.S. coast of the lower 48 states and 12 nautical miles from the continental U.S. coast. *Overflying the continental United States* does not apply to:

(1) Flights that transit the airspace of the continental United States between two airports or locations in the same country, where that country is Canada or Mexico; or

(2) Any other category of flights that the Assistant Secretary of Homeland Security (Transportation Security Administration) designates in a notice in the **Federal Register**.

*Passenger* means an individual who is traveling on a covered flight. The term *passenger* does not include:

- (1) A crew member who is listed as a crew member on the flight manifest; or
- (2) An individual with flight deck privileges under 49 CFR 1544.237 traveling on the flight deck.

*Passenger Resolution Information* or *PRI* means the information that a covered aircraft operator or covered airport operator transmits to TSA for an individual who TSA places in an inhibited status and from whom the covered aircraft operator or covered airport operator is required to request additional information and a Verifying Identity Document. *Passenger*

*Resolution Information* includes, but is not limited to, the following:

- (1) Covered aircraft operator's agent identification number or agent sine.
- (2) Type of Verifying Identity Document presented by the passenger.
- (3) The identification number on the Verifying Identity Document.
- (4) Issue date of the Verifying Identity Document.
- (5) Name of the governmental authority that issued the Verifying Identity Document.

(6) Physical attributes of the passenger such as height, eye color, or scars, if requested by TSA.

*Passport information* means the following information from an individual's passport:

- (1) Passport number.
- (2) Country of issuance.
- (3) Expiration date.
- (4) Gender.
- (5) Full name.

*Redress Number* means the number assigned by DHS to an individual processed through the redress procedures described in 49 CFR part 1560, subpart C.

*Secure Flight Passenger Data* or (*SFPD*) means information regarding a passenger or non-traveling individual that a covered aircraft operator or covered airport operator transmits to TSA, to the extent available, pursuant to § 1560.101. *SFPD* is the following information regarding a passenger or non-traveling individual:

- (1) Full name.
- (2) Date of birth.
- (3) Gender.
- (4) Redress number or Known Traveler Number (once implemented).
- (5) Passport information.
- (6) Reservation control number.
- (7) Record sequence number.
- (8) Record type.
- (9) Passenger update indicator.
- (10) Traveler reference number.
- (11) Itinerary information.

*Self-service kiosk* means a kiosk operated by a covered aircraft operator that is capable of accepting a passenger reservation or a request for authorization to enter a sterile area from a non-traveling individual.

*Sterile area* means "sterile area" as defined in 49 CFR 1540.5.

*Terrorist Screening Center* or *TSC* means the entity established by the Attorney General to carry out Homeland Security Presidential Directive 6 (HSPD-6), dated September 16, 2003, to consolidate the Federal government's approach to terrorism screening and provide for the appropriate and lawful use of terrorist information in screening processes.

*Verifying Identity Document* means one of the following documents:

(1) An unexpired passport issued by a foreign government.

(2) An unexpired document issued by a U.S. Federal, State, or tribal government that includes the following information for the individual:

- (i) Full name.
- (ii) Date of birth.
- (iii) Photograph.

(3) Such other documents that TSA may designate as valid verifying identity documents.

*Watch list* refers to the No Fly and Selectee List components of the Terrorist Screening Database maintained by the Terrorist Screening Center. For certain flights, the "watch list" may include the larger set of watch lists maintained by the Federal government as warranted by security considerations.

### Subpart B—Collection and Transmission of Secure Flight Passenger Data for Watch List Matching

#### § 1560.101 Request for and transmission of information to TSA.

(a) *Request for information.* (1) Each covered aircraft operator must request the full name, gender, date of birth, and Redress Number for passengers on a covered flight and non-traveling individuals seeking access to an airport sterile area. For reservations made 72 hours prior to the scheduled time of departure for each covered flight, the covered aircraft operator must collect full name, gender, and date of birth for each passenger when the reservation is made or at a time no later than 72 hours prior to the scheduled time of departure of the covered flight. For an individual that makes a reservation for a covered flight within 72 hours of the scheduled time of departure for the covered flight, the covered aircraft operator must collect the individual's full name, date of birth, and gender at the time of reservation. The covered aircraft operator must include the information provided by the individual in response to this request in the SFPD.

(i) Except as provided in paragraph (a)(1)(ii) of this section, each covered aircraft operator must begin requesting the information described in paragraph (a)(1) of this section in accordance with its AOIP as approved by TSA.

(ii) An aircraft operator that becomes a covered aircraft operator after the effective date of this part must begin requesting the information on the date it becomes a covered aircraft operator.

(2) Beginning on a date no later than 30 days after being notified in writing by TSA, each covered aircraft operator must additionally request the Known Traveler Number for passengers on a

covered flight and non-traveling individuals seeking access to an airport sterile area. The covered aircraft operator must include the Known Traveler Number provided by the passenger in response to this request in the SFPD.

(3) Each covered aircraft operator may not submit SFPD for any passenger on a covered flight who does not provide a full name, date of birth and gender. Each covered aircraft operator may not accept a request for authorization to enter a sterile area from a non-traveling individual who does not provide a full name, date of birth and gender.

(4) Each covered aircraft operator must ensure that each third party that accepts a reservation, or accepts a request for authorization to enter a sterile area, on the covered aircraft operator's behalf complies with the requirements of this section.

(5) If the covered aircraft operator also has an operation of an aircraft that is subject to 49 CFR 1544.101(b) through (i), the covered aircraft operator may submit SFPD for passengers on these operations for watch list matching under this part, provided that the covered aircraft operator—

(i) Collects and transmits the SFPD for the passengers in accordance with this section;

(ii) Provides the privacy notice to the passengers in accordance with 49 CFR 1560.103; and

(iii) Complies with the requirements of 49 CFR 1560.105 and 1560.107.

(b) *Transmission of Secure Flight Passenger Data to TSA.* Beginning on the date provided in a covered aircraft operator's AOIP, the covered aircraft operator must electronically transmit SFPD to TSA, prior to the scheduled departure of each covered flight, in accordance with its AOIP as approved by TSA.

(1) To the extent available, each covered aircraft operator must electronically transmit SFPD to TSA for each passenger on a covered flight.

(2) Each covered aircraft operator must transmit SFPD to TSA prior to the scheduled flight departure time, in accordance with its AOIP as approved by TSA.

(c) *Transmission of non-traveler information to TSA.* Beginning on the date provided in a covered aircraft operator's AOIP, the covered aircraft operator must electronically transmit SFPD to TSA for each non-traveling individual, prior to authorizing access to an airport sterile area.

(d) *Retransmission of information.* Each covered aircraft operator must retransmit to TSA updates to the information listed in paragraphs (b) and

(c) of this section to reflect most recent changes to that information, as specified in its AOIP as approved by TSA.

**§ 1560.103 Privacy notice.**

(a) *Electronic collection of information*—(1) *Current electronic collection of information.* Prior to collecting information through a Web site or self-service kiosk from a passenger or non-traveling individual in order to comply with § 1560.101(a), a covered aircraft operator must make available the complete privacy notice set forth in paragraph (b) of this section.

(2) *Other electronic collection of information.* If a covered aircraft operator collects information directly from a passenger or non-traveling individual in order to comply with § 1560.101(a) through an electronic means not described in paragraph (a)(1) of this section, the covered aircraft operator must make available the complete privacy notice set forth in paragraph (b) of this section.

(3) *Third party Web site.* Each covered aircraft operator must ensure that each third party that maintains a Web site capable of making a reservation for the covered aircraft operator's reservation system, make available on its Web site the complete privacy notice set forth in paragraph (b) of this section prior to collecting information through the Web site.

(b) *Privacy notice.* The covered aircraft operator may substitute its name for the word "us," but the complete privacy notice otherwise must be identical to the following paragraph unless TSA has approved alternative language:

The Transportation Security Administration of the U.S. Department of Homeland Security requires us to collect information from you for purposes of watch list screening, under the authority of 49 U.S.C. section 114, and the Intelligence Reform and Terrorism Prevention Act of 2004. Providing this information is voluntary; however, if it is not provided, you may be subject to additional screening or denied transport or authorization to enter a sterile area. TSA may share information you provide with law enforcement or intelligence agencies or others under its published system of records notice. For more on TSA Privacy policies, or to view the system of records notice and the privacy impact assessment, please see TSA's Web site at [www.tsa.gov](http://www.tsa.gov).

**§ 1560.105 Denial of transport or sterile area access; Designation for enhanced screening.**

(a) *Applicability.* (1) This section applies to each covered aircraft operator beginning on the date that TSA assumes the watch list matching function for the passengers and non-traveling individuals to whom that covered

aircraft operator issues a boarding pass or other authorization to enter a sterile area. TSA will provide prior written notification to the covered aircraft operator no later than 60 days before the date on which it will assume the watch list matching function from that covered aircraft operator.

(2) Prior to the date that TSA assumes the watch list matching function from a covered aircraft operator, the covered aircraft operator must comply with existing watch list matching procedures for passengers and non-traveling individuals, including denial of transport or sterile area access or designation for enhanced screening for individuals identified by the covered aircraft operator or TSA.

(b) *Watch list matching results.* Except as provided in paragraph (b) of this section, a covered aircraft operator must not issue a boarding pass or other authorization to enter a sterile area to a passenger or a non-traveling individual, and must not allow that individual to board an aircraft or enter a sterile area, until TSA informs the covered aircraft operator of the results of watch list matching for that passenger or non-traveling individual, in response to the covered aircraft operator's most recent SFPD submission for that passenger or non-traveling individual.

(1) *Denial of boarding pass.* If TSA sends a covered aircraft operator a boarding pass printing result that says the passenger or non-traveling individual must be placed on inhibited status, the covered aircraft operator must not issue a boarding pass or other authorization to enter a sterile area to that individual and must not allow that individual to board an aircraft or enter a sterile area.

(2) *Selection for enhanced screening.* If TSA sends a covered aircraft operator a boarding pass printing result that says the passenger has been selected for enhanced screening at a security checkpoint, the covered aircraft operator may issue a boarding pass to that individual and must identify the individual for enhanced screening, in accordance with procedures approved by TSA. The covered aircraft operator must place a code on the boarding pass that meets the requirements described in the Consolidated User Guide. If TSA sends a covered aircraft operator a boarding pass printing result that says the non-traveling individual has been selected for enhanced screening at a security checkpoint, the covered aircraft operator must not issue an authorization to enter a sterile area to that individual.

(3) *Cleared for boarding or entry into a sterile area.* If TSA sends a covered aircraft operator a boarding pass

printing result that instructs a covered aircraft operator that a passenger or non-traveling individual is cleared, the covered aircraft operator may issue a boarding pass or other authorization to enter a sterile area to that individual, unless required under another TSA requirement to identify the passenger or non-traveling individual for enhanced screening or to deny entry into the sterile area. The covered aircraft operator must place a code on the boarding pass or authorization to enter the sterile area that meets the requirements described in the Consolidated User Guide.

(4) *Override by a covered aircraft operator.* No covered aircraft operator may override a TSA boarding pass printing result that instructs a covered aircraft operator to place a passenger or non-traveling individual in an inhibited status or to identify a passenger or non-traveling individual for enhanced screening, unless explicitly authorized by TSA to do so.

(5) *Updated SFPD from covered aircraft operator.* When a covered aircraft operator sends updated SFPD to TSA under § 1560.101(d) for a passenger or non-traveling individual for whom TSA has already issued a boarding pass printing result, all previous TSA results concerning the passenger or non-traveling individual are voided. The covered aircraft operator may not issue a boarding pass or grant authorization to enter a sterile area until it receives an updated result from TSA authorizing the issuance of a boarding pass or authorization to enter a sterile area. Upon receiving an updated result from TSA, the covered aircraft operator must acknowledge receipt of the updated result, comply with the updated result, and disregard all previous boarding pass printing results.

(6) *Updated boarding pass printing results from TSA.* After TSA sends a covered aircraft operator a result under paragraph (b)(1), (b)(2), or (b)(3) of this section, TSA may receive additional information concerning the passenger or non-traveling individual and may send an updated boarding pass printing result concerning that passenger or non-traveling individual to the covered aircraft operator. Upon receiving an updated boarding pass printing result from TSA, the covered aircraft operator must acknowledge receipt of the updated result, comply with the updated result, and disregard all previous results.

(7) *Boarding pass issuance for covered flights to or overflying the United States.* Covered aircraft operators may permit another aircraft operator to issue a boarding pass for a covered flight

departing from a foreign location to the United States or overflying the United States without regard to the requirements in paragraphs (b)(1) through (b)(6) of this section provided that—

(i) Before allowing the individual to board the aircraft for a covered flight, the covered aircraft operator confirms that it has received a boarding pass printing result from DHS for individuals who are issued boarding passes under paragraph (b)(7) of this section;

(ii) Before allowing the individual to board an aircraft for a covered flight, the covered aircraft operator applies the measures in its security program to prevent an individual for whom DHS has returned an inhibited status boarding pass printing result under paragraph (b)(1) of this section from boarding the aircraft; and

(iii) The covered aircraft operator applies the measures in its security program, as provided in 49 CFR part 1544, subpart B or 49 CFR part 1546, subpart B, to ensure that an individual for whom DHS returns a Selectee result under paragraph (b)(2) of this section undergoes enhanced screening pursuant to the covered aircraft operator's security program prior to that individual boarding the aircraft.

(c) *Request for identification*—(1) *In general.* If TSA has not informed the covered aircraft operator of the results of watch list matching for an individual by the time the individual attempts to check in, or informs the covered aircraft operator that an individual has been placed in inhibited status, the aircraft operator must request from the individual a verifying identity document pursuant to procedures in its security program, as provided in 49 CFR part 1544, subpart B or 49 CFR part 1546, subpart B. The individual must present a verifying identity document to the covered aircraft operator at the airport.

(2) *Transmission of Updated Secure Flight Passenger Data.* Upon reviewing a passenger's verifying identity document, the covered aircraft operator must transmit the SFPD elements from the individual's verifying identity document to TSA.

(3) *Provision of Passenger Resolution Information.* If requested by TSA, the covered aircraft operator must also provide to TSA the individual's Passenger Resolution Information as specified by TSA.

(4) *Exception for minors.* If a covered aircraft operator is required to obtain information from an individual's verifying identity document under this paragraph (c), and the individual is younger than 18 years of age and does

not have a verifying identity document, TSA may, on a case-by-case basis, authorize the minor or an adult accompanying the minor to state the individual's full name and date of birth in lieu of providing a verifying identity document.

(d) *Failure to obtain identification.* If a passenger or non-traveling individual does not present a verifying identity document when requested by the covered aircraft operator, in order to comply with paragraph (c) of this section, the covered aircraft operator must not issue a boarding pass or give authorization to enter a sterile area to that individual and must not allow that individual to board an aircraft or enter a sterile area, unless otherwise authorized by TSA.

#### **§ 1560.107 Use of watch list matching results by covered aircraft operators.**

A covered aircraft operator must not use any watch list matching results provided by TSA for purposes other than those provided in § 1560.105 and other security purposes.

#### **§ 1560.109 Aircraft Operator Implementation Plan.**

(a) *Content of the Aircraft Operator Implementation Plan (AOIP).* Each covered aircraft operator must adopt and carry out an AOIP that sets forth the following:

(1) The covered aircraft operator's test plan with TSA.

(2) When the covered operator will begin to collect and transmit to TSA each data element of the SFPD for each covered flight.

(3) The specific means by which the covered aircraft operator will request and transmit information under § 1560.101, the timing and frequency of transmission, and any other related matters, in accordance with the Consolidated User Guide.

(b) *Adoption of Aircraft Operator Implementation Plan (AOIP).* Each covered aircraft operator must adopt an AOIP pursuant to the procedures set forth in this paragraph (b).

(1) TSA notifies each covered aircraft operator in writing of a proposed AOIP, fixing a period of not less than 30 days within which the covered aircraft operator may submit written information, views, and arguments on the proposed AOIP.

(2) After considering all relevant material, TSA's designated official notifies each covered aircraft operator of its AOIP. The AOIP becomes effective not less than 30 days after the covered aircraft operator receives the notice of its AOIP, unless the covered aircraft operator petitions the Assistant

Secretary or designated official to reconsider no later than 15 days before the effective date of the AOIP. The covered aircraft operator must send the petition for reconsideration to the designated official. A timely petition for reconsideration stays the effective date of the AOIP.

(3) Upon receipt of a petition for reconsideration, the designated official either amends the AOIP or transmits the petition, together with any pertinent information, to the Assistant Secretary or designee for reconsideration. The Assistant Secretary or designee disposes of the petition within 30 days of receipt by either directing the designated official to withdraw or amend the AOIP, or by affirming the AOIP.

(4) TSA may, at its discretion, grant extensions to any schedule deadlines, on its own initiative or upon the request of a covered aircraft operator.

(c) *Incorporation into Security Program.* Once an AOIP is approved, the AOIP becomes part of the covered aircraft operator's security program as described in 49 CFR part 1544, subpart B, or 49 CFR part 1546, subpart B, as appropriate, and any amendments will be made in accordance with the procedures in those subparts.

(d) *Handling of Aircraft Operator Implementation Plan (AOIP).* An AOIP contains sensitive security information (SSI) and must be handled and protected in accordance with 49 CFR part 1520.

#### **§ 1560.111 Covered airport operators.**

(a) *Applicability.* This section applies to a covered airport operator that has a program approved by TSA through which the covered airport operator may authorize non-traveling individuals to enter a sterile area.

(b) *Requirements.* A covered airport operator must adopt and carry out an AOIP in accordance with § 1560.109. Each covered airport operator must comply with the procedures required of covered aircraft operators in §§ 1560.101(a), (c), and (d), 1560.103, and 1560.107 of this part and any other applicable TSA requirements when authorizing non-traveling individuals to enter a sterile area.

### **Subpart C—Passenger Redress**

#### **§ 1560.201 Applicability.**

This subpart applies to individuals who believe they have been improperly or unfairly delayed or prohibited from boarding an aircraft or entering a sterile area as a result of the Secure Flight program.



**§ 1560.203 Representation by counsel.**

A person may be represented by counsel at his or her own expense during the redress process.

**§ 1560.205 Redress process.**

(a) If an individual believes he or she has been improperly or unfairly delayed or prohibited from boarding an aircraft or entering a sterile area as a result of the Secure Flight program, the individual may seek assistance through the redress process established under this section.

(b) An individual may obtain the forms and information necessary to initiate the redress process on the DHS TRIP Web site at <http://www.dhs.gov/trip> or by contacting the DHS TRIP office by mail. Individuals should send written requests for forms to the DHS TRIP office and include their name and

address in the request. DHS will provide the necessary forms and information to individuals through its Web site or by mail.

(c) The individual must send to the DHS TRIP office the personal information and copies of the specified identification documents. If TSA needs additional information in order to continue the redress process, TSA will so notify the individual in writing and request that additional information. The DHS TRIP Office will assign the passenger a unique identifier, which TSA will recognize as the Redress Number, and the passenger may use that Redress Number in future correspondence with TSA and when making future travel reservations.

(d) TSA, in coordination with the TSC and other appropriate Federal law

enforcement or intelligence agencies, if necessary, will review all the documentation and information requested from the individual, correct any erroneous information, and provide the individual with a timely written response.

**§ 1560.207 Oversight of process.**

The redress process and its implementation are subject to review by the TSA and DHS Privacy Offices and the TSA and DHS Offices for Civil Rights and Civil Liberties.

Issued in Arlington, Virginia, on October 20, 2008.

**Kip Hawley,**

*Assistant Secretary.*

[FR Doc. E8-25432 Filed 10-27-08; 8:45 am]

**BILLING CODE 9110-05-P**