U.S. Department of Homeland Security
Customs and Border Protection (CBP)
Transportation Security Administration (TSA)

APIS Pre-Departure Final Rule
Secure Flight Final Rule
Visa Waiver Program – Electronic System for Travel Authorization Interim Final Rule

Consolidated User Guide

SF-BAP-1020 Ver 3.4

May 14, 2010

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

Note to reviewers: **COMMENTS INVITED.**

This Consolidated User Guide reflects decisions about the APIS Pre-Departure Final Rule, Secure Flight Final Rule, and the Visa Waiver Program – Electronic System for Travel Authorization Interim Final Rule.

Stakeholders are encouraged to provide their feedback, comments, and suggestions on this guidance to DHS.

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

Revision History

Date	Document ID Number	Description of Revisions	Location in Document
3/26/2010	Ver 3.4	• Included clarification on US and US Territory	• Executive Summary
		• Updated to DHS Technology Center to CBP Technology Service Desk	• Executive Summary
		• Removed the PNR option	• Section 1.1 Overview of the Consolidated User Guide
		• Set the APIS Pre-Departure final rule effective date	• Section 2.1 APIS Pre-Departure Final Rule
		• Removed Proposed AOIP and Comment Review Process	• Section 3.1 Implementation Plan Procedures
		• Updated Implementation plan procedures for the Approved AOIP	• Section 3.1 Implementation Plan Procedures
		• Updated Phase 2 – Assessment section	• Table 3 Secure Flight Deployment Phases
		• Updated Method for new passenger bookings after the initial 72-hour submission	• Table 7 Passenger Data Required Transmission Timing
		• Removed passport number and country of issuance requirement for ESTA vetting from international inbound passenger section	• Table 8 Required Transmission Events
		• Added a note to the ESTA validation section.	• Section 4.5 Message Business Rules
		• Updated the Country of Residence Data Element to not required for APIS Pre-Departure for flights leaving the US	• Table 15 APIS Data Submission Rules
		• Updated the 2Z selectee screen and travel authorization via ESTA not applicable section	• Section 4.8.3.2 Boarding Pass and Boarding Authorized
		• Added the Non-traveler (Gate Pass) Data message type to the PAXLST	• Table 38 UN/EDIFACT Messages Sets and DHS

Date	Document ID Number	Description of Revisions	Location in Document
		message set • Updated subsequent submissions example from 6 to 8 hours • Updated length of the record locator element to 6 from 10. • Removed the accepted message formats from requirement 1. • Updated Activation/Deactivation Code Required to no for option 3. • Included clarification on VID via Kiosk • Updated agency identification • Removed references to activation order codes. • Included guidance for issuance of No Fly Waiver	Message Types • Section 4.12 Alternative SFPD Submission Method • Table 39 SFPD Elements • Section 4.13 72 Hour Continuous Submission Alternative • Table 41 Secure Flight Outage Options • Section 5.3.3 Data Validation • Section 5.3.4 Passenger Handling - Airport Procedures and Resolution of Boarding Pass Printing Result • Section 5.5.4.3 Fall Back to Pre-Secure Flight Watch List Matching Processes • Section 5.14 No Fly Waiver
11/13/2009	Ver 3.3	• Included clarification for potential aircraft operator configuration changes to support message routing to Secure Flight. • Included clarification on 72 hour submissions and the requirement to submit all the directional travel operating carrier flight segments in a single submission at 72 hours. • Included guidance on the required use of high and low priority queues • Included clarification for required transmissions for passenger data	• Section 4.1 Data Interchange and Messaging Facility – Single Interface • Section 4.3 Required Submissions – Directional Travel • Section 4.3 Passenger Data Required Transmission Timing • Table 7 – Passenger Data Required Transmission Timing

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

Date	Document ID Number	Description of Revisions	Location in Document
		• Included clarification for Travel Document Type and Document Expiration Date • Included guidance for Itinerary Change submission rules • Included guidance on the contact process for unsolicited messages when a ground handling company performs check-in • Removed provision to submit full SFPD at 44 hours prior to flight departure if carriers cannot provide the Passenger Reference Number in the 72 hour PNR Pull/Push mechanism • Included guidance for the 72Hr Continuous Submission Alternative • Included guidance for approved ground handling processes • Included guidance on the DHS Lap Child policy • Included DHS clarification on the submission of duplicate messages • Removed content for Customs and Border Protection – PNR	• Table 12 SFPD Submission Rules and Table 13 SFPD Gate Pass (Non-Traveler) Submission Rules • Table 14 SFPD Submission Rules for Passenger Updates • Section 4.8.2.5 Domestic Travel – Unsolicited Messages and Section 4.8.3.6 International Travel – Unsolicited Messages • Section 4.12 Alternative SFPD Submission Method • Section 4.13 72 Hour Continuous Submission Alternative • Section 5.3.2 Passenger Check-In: TSA Check-In Statuses and Section 5.12 Ground Handling • Section 5.11 Lap Children • Section 5.13 Duplicate Message Submission • Whole document
08/24/2009	Ver 3.2	• Added clarification to the Record Locator and Passenger Reference Number values. • Included guidance for the Alternative SFPD Submission Method • Updated the TSA Privacy Notice	• Section 4.2.3 Secure Flight Rule: Table 5 • Section 4.12 Alternative SFPD Submission Method • Section 5.1 Privacy Notice

Date	Document ID Number	Description of Revisions	Location in Document
		- Included guidance on how to handle government IDs that have date of birth with year only - Updated Outage Procedures outlining available mitigation options and implementation procedures. - Included guidance for Interline Through Check-in - Included guidance for Standby Passengers - Included guidance for Ticketed Reservations - Included guidance for resubmission of passenger data to receive a new ESTA status - Included guidance for use of two documents in receiving an ESTA status response	- Section 5.3.4 Passenger Handling – Airport Procedures and Resolution of Boarding Pass Printing Results: Inhibited Resolution - Section 5.5 System Outage Procedures - Section 5.7 Interline Through Check-in - Section 5.8 Standby Passengers - Section 5.9 Ticketed Reservations - Section 5.10 ESTA Resubmission - Section 4.5 Data Submission Rules
05/29/2009	Ver 3.1	- Changed the Directional Travel requirement from 8 to 12 hours. - Inhibited Response Message Data Element List. Changed 'Guidance Message' from '11 – Call DHS Service Center' to '11 – Call Secure Flight Service Center' - Included PRL to be defined as case insensitive - Included that DHS will acknowledge an informational update from the aircraft operator. - Included codified responses: N.. for boarding pass not issued Y.. for boarding pass issued E.. for Error	- Section 4.3 Required Submissions - Section 4.8.2.3 Domestic Travel – Inhibited Response: Table 22 - Section 4.2.3 Secure Flight Rule: Table 5 - Section 4.6 Data Submission Rules - Section 4.8.2.5 Domestic Travel – Unsolicited Message: Table 24 Section 4.8.3.6 International Travel – Unsolicited Message: Table 36

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

Date	Document ID Number	Description of Revisions	Location in Document
		• Included that Secure Flight shall accommodate passengers with only one name.	• Section 4.2.3 Secure Flight Rule: Table 5
11/04/2008	Ver 3.0	• Updated release for Secure Flight Final Rule	• Whole document
10/28/2008	Ver 2.4	• Added Phase III to the phase table • Revised introduction paragraph to distinguished between CBP and Secure Flight • Added updated phase table to beginning of section • Revised wording for APIS and SFPD submissions • Revised note for Secure Flight required data elements • Revised Required Transmission Events • Revised Reservations Data paragraph • Revised Passenger Check-in: Gate Pass • Revised Data Validation content for TSA	• Section 1 Executive Summary • Section 3.5 Readiness for Cutover • Section 4 Technical Requirements • Section 4.1 Data Interchange and Message Facility • Section 4.2.3 Table 5, Section 4.6 Table 13 & 14 • Section 4.4 Table 9 • Section 5.3.1 TSA Reservations Data • Section 5.3.2 • Section 5.3.3
10/24/2008	Ver 2.3	• Update Systems Outage procedures	• Section 5.5
10/10/2008	Ver 2.2	• Updates to Section 3.4 and 3.5 in preparation of the publication of the Secure Flight Final Rule	• Section 3.4 and 3,5
7/22/2008	Ver. 2.1	• Global change to remove references to NPRM and Proposed rule when referring to the Secure Flight • Added references to distinguish between the Secure Flight Service Center and the DHS Service Center • Updates made to reflect changes in Testing for Secure Flight • Deleted graphic 3 (Illustration of Submissions and Timing) and made changes to language	• Whole Document • Whole Document • Section 3.4 Testing • Section 4.3 Required Submission

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

Date	Document ID Number	Description of Revisions	Location in Document
		• Added footnote to table 8 • DOB and Gender now required for Secure Flight affecting table 9 and 10 • Added language for Non-travelers requesting a gate pass • Update operational procedures for resolution to include PRI as specified in Secure Flight Final Rule • Updated the DRO guidance for removing a passenger from a plane • Update to the Secure Flight Network Message Connectivity • Update for Alternative Transmission methods	• Section 4.4 Required Transmissions • Section 4.6 Data Submission Rules • Section 5.3.2 Passenger Check-in • Section 5.3.4 Inhibited Resolution • Section 5.3.4 • Section 4.10 • Section 4.11
07/21/2008	Ver 2.0	• Introduced information concerning the Visa Waiver Program and Electronic System for Travel Authorization (ESTA) Interim Final Rule.	• Whole Document
03/03/2008	Ver 1.5	• Renamed document • Identified unique identifiers for NEXUS and SENTRY cards. • Modified references to DHS Router • Included verbiage identifying future enhancements under consideration to provide means by which carriers can alert DHS of previously issued boarding pass status on 'qualified change' messages. • Included additional guidance regarding submission rules for passenger updates/cancellations. • Included 'Error' status as valid boarding pass issue status on Carrier Acknowledgements to Unsolicited Messages.	• Title page • Table 3 • Whole document • Section 4.6 • Section 4.6 • Section 4.8.2.5 & Section 4.8.3.5

Date	Document ID Number	Description of Revisions	Location in Document
		- Included Guidance regarding Itinerary reporting. - Introduced additional guidance recognizing role of 'organizations and/or individuals acting on behalf of the aircraft operator' when processing 'Selectee' or 'Inhibited' watch list results.	- Section 4.3 'Required Submissions' - Section 5.3.2 'Passenger Check-in'
08/23/2007	Ver 1.0	- Initial Document Release	

Table of Contents

Distributed in separate documents:

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

List of Tables

List of Figures

***WARNING:* This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

1 EXECUTIVE SUMMARY

The Department of Homeland Security (DHS) merges the capability to anticipate, preempt, and deter threats to the homeland whenever possible through its component agencies. Under the guidance of its Screening Coordination Office, DHS directed U.S. Customs and Border Protection (CBP) and the Transportation Security Administration (TSA) to combine the Advance Passenger Information System (APIS) Pre-Departure and Secure Flight concepts and systems to provide “One DHS Solution” to the commercial aviation industry consistent with applicable authorities and statutes. This joint approach would:

- Standardize Secure Flight and APIS Pre-Departure. TSA and CBP are coordinating their airline industry needs with the intent of providing a single DHS system to the fullest extent possible;
- Reduce unnecessary programming by aircraft operators; and
- Provide consistent treatment for passengers across all aircraft operators.

The Consolidated User Guide (CUG) provides technical and operational guidance to comply with the APIS Pre-Departure Final Rule and the technical and operational requirements to comply with the Secure Flight Final Rule.

Responsibility for watch list matching is planned for transition from aircraft operators to DHS in the following phases:

Phase I International Itineraries	From the time that an aircraft operator is compliant with APIS Pre-Departure, DHS will perform watch list matching for international itineraries to and from the United States. Until the Secure Flight Final Rule is effective, aircraft operators will perform domestic watch list matching internally for wholly domestic itineraries.
Phase II Domestic Itineraries	As specified in the Aircraft Operator Implementation Plan in the aircraft operators’ security program, DHS will assume the watch list matching responsibility for itineraries between two U.S. airports including commonwealth territories of the United States: American Samoa, Guam, Northern Mariana Islands (CNMI), U.S. Virgin Islands, Puerto Rico, Saipan (part of the Northern Mariana Islands)
Phase III Domestic, International Itineraries, Overflights and International to International U.S. Covered Flights	DHS will transition the watch list matching function for covered flights to and from the United States from APIS Pre-Departure to Secure Flight. CBP will continue the operation of Pre Departure APIS, but will cease providing a watch list matching result for covered flights. Secure Flight will assume responsibility for watch list matching for covered flights overflying the continental United States. Additionally, Secure Flight will assume responsibility for watch list matching for covered flights between two non-U.S. locations operated by U.S. aircraft operators.
Subsequent Phases	DHS will also be assuming responsibility for watch list matching for aircraft operator direct employees.

In response to aviation industry requests to ease the compliance burden, DHS developed a single portal called the DHS Router to provide network connectivity for individual aircraft operators. The router validates message formats, filters data provided, and routes messages to CBP and TSA based on their respective missions.

To describe the data elements in APIS Pre-Departure and Secure Flight, DHS will use the term "passenger data." Passenger data represents the information used to identify the passenger or non-traveler.

To clarify between data for Secure Flight and APIS Pre-Departure, DHS will refer to passenger data associated with Secure Flight as Secure Flight Passenger Data (SFPD). Passenger data for international travel associated with APIS Pre-Departure requirements will be referred to as APIS data.

DHS uses the term "Passenger Data Message" to refer to the message that aircraft operators will use to submit passenger data to DHS. The two formats accepted will be UN/EDIFACT (PAXLIST) or XML. Section 4, the Technical Requirements Guide, contains details regarding Passenger Data Messages.

The text of the applicable regulations may be found in the sources specified in Appendix 7.1.

1.1 Overview of the Consolidated User Guide

This Consolidated User Guide is published to assist aircraft operators in achieving procedural and technical compliance with the Advance Passenger Information System (APIS) Pre-Departure Final Rule and to provide the technical and operational requirements to comply with the Secure Flight Final Rule. CBP's and TSA's technical requirements and associated procedures are published together to give aircraft operators the information necessary to perform changes to their information technology systems, networks, and operations to comply with these DHS regulations.

In this guide, references to DHS should be interpreted to apply to CBP and TSA jointly, unless otherwise specified. Discrete references to CBP or TSA are specified as indicated below.

Discrete Content

CBP▸ This mark identifies implementation or operations information with respect to CBP's APIS program and the APIS Pre-Departure Final Rule (see Section 2.1).

TSA▸ This mark identifies implementation or operations information with respect to TSA's Secure Flight program and the Secure Flight Final Rule (see Section 2.2).

Throughout this guide, several terms appear that may be unfamiliar to the reader. Their definitions are as follows:

- **Aircraft operator:** aircraft operator or air carrier as defined within the respective rule documents (APIS Pre-Departure and the Secure Flight).
- **Boarding pass:** a printed document provided to each traveler by the aircraft operator. The term "boarding pass" refers to traditional seat-specific boarding entitlement documents, security

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

documents, and aircraft operator equivalents (such as "seat management cards" used to identify passengers for whom a specific seat may not be assigned until presented at the departure gate).

- **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.
- **CBP – Technology Service Desk:** the service center that will handle all APIS and ATS calls (CBP).
- **Overflight:** a flight that flies over the continental United States. TSA will conduct watch list matching for overflights to protect the United States against terrorist activity that could occur in its airspace. The continental U.S. is defined as the contiguous lower 48 states and does not include Alaska or Hawaii. Overflights do not include 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, and flights that the Assistant Secretary of Homeland Security (Transportation Security Administration) may designate in the Federal Register.
- **Secure Flight Service Center:** the service center that will handle all Secure Flight calls (TSA).

More definitions are provided in Appendix 7.3.2.

This user guide provides a comprehensive reference for aircraft operators. It is organized to meet the needs of the different organizational components responsible for implementing the technical changes necessary to comply with the APIS Pre-Departure Final Rule, Visa Waiver Program – Electronic System for Travel Authorization (ESTA) Interim Final Rule, and the Secure Flight Final Rule. Future versions of this guide will include technical guidance regarding other governmental programs and requirements, such as the Centers for Disease Control and Prevention (CDC).

The table below outlines the sections in this guide and who should read them.

CUG Section	Audience and Content
1. Executive Summary	**Primary audience:** All readers **Content:** Overview of the Consolidated User Guide and its intended usage
2. Guide to Compliance Actions	**Primary audience:** All readers **Content:** Overview of the DHS rules covered by the guide, with cross-references to the sections of the guide pertaining to each rule
3. Implementation Guide	**Primary audience:** Personnel responsible for managing the implementation activities to comply with the APIS Pre-Departure Final Rule, Visa Waiver Program – ESTA Interim Final Rule, and Secure Flight Final Rule **Content:** Technical and operational guidance to support aircraft operator activities associated with implementation and cutover
4. Technical Requirements Guide	**Primary audience:** Technical personnel responsible for system development activities **Content:** Requirements for the data format, message types, and message timing

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

CUG Section	Audience and Content
5. Operations Guide	**Primary audience:** Operations personnel responsible for ongoing post-implementation procedures **Content:** Operations scenarios and procedures
6. Other Governmental Programs and Requirements	**Primary audience:** All readers **Content:** Overview of CDC requirements.
7. Appendices	**Content:** Detailed supporting documentation Note: the appendices will be delivered under separate cover.

1.2 Updates to the Consolidated User Guide

Updates to this guide will be published as necessary, and the following resources are available to aircraft operators to assist with their compliance activities:

CBP▶

- National APIS Account Manager, Steven O'Neill, steven.oneill@dhs.gov
- UN/EDIFACT Implementation Guide
- CBP – Technology Service Desk
- APIS home page:

http://www.cbp.gov/xp/cgov/travel/inspections_carriers_facilities/apis/

TSA▶

- Secure Flight Airline Implementation Managers (to be named)
- Secure Flight FAQ (distribution method to be determined)
- XML Implementation Guide
- Secure Flight Service Center
- Secure Flight home page:

http://www.tsa.gov/what_we_do/layers/secureflight/index.shtm

2 GUIDE TO ACTIONS REQUIRED FOR COMPLIANCE

2.1 APIS Pre-Departure Final Rule

The Advance Passenger Information System (APIS) is a program within CBP that screens passengers and crewmembers traveling on international flights. Developed in 1988, APIS collects biographical data from international air passengers traveling into or departing from the United States. Aircraft operators submit passenger data at pre-determined times, allowing the data to be checked against law enforcement databases.

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Public Law 108-458) was enacted on December 17, 2004. Sections 4012 and 4071 of the IRTPA require DHS to issue regulations and procedures to allow for pre-departure watch list matching of passengers onboard aircrafts arriving in and departing from the United States, and of passengers and crew onboard vessels arriving in and departing from the United States.

The processing of passenger manifests in APIS will continue to support the existing UN/EDIFACT PAXLST passenger manifest format, as currently submitted by aircraft operators. The options discussed in this document do not supersede any of the data requirements or aircraft operator responsibilities specified within the APIS Final Rule (see Federal Register, Volume 70, No. 66 [70FR17820]).

Aircraft operators that fail to transmit APIS data in accordance with the APIS Pre-Departure Final Rule may be subject to civil and monetary penalties. Aircraft operators must validate APIS data based on what is found in the Machine Readable Zone of the provided travel document. Aircraft operators unable to utilize the technology provided with a document swipe are required to validate the data found in the Machine Readable Zone, full name, date of birth, document type, document number, document country of issuance, document expiration date, and gender. Validation may equal a visual comparison of the individual's travel document with the data submitted to DHS.

Aircraft operators are required to comply with the data collection and the timing requirements mandated in the APIS Pre-Departure Final Rule. The components below, individually or in combination with one another, will assist aircraft operators in complying with APIS regulations discussed within this document.

APIS Component	Description
APIS Pre-Departure	Under the APIS Pre-Departure final rule, which became effective February 19, 2008, aircraft operators must transmit to CBP passenger manifest information for aircraft en route to or from the United States, prior to aircraft departure. The final rule requires aircraft operators to: A. Provide complete flight information B. Provide a unique identifier for each passenger C. Accept a Response Message from DHS D. Provide a Flight Close-out Message 30 minutes after departure
APIS Batch	Aircraft operators may meet their APIS Pre-Departure

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

APIS Component	Description
	requirement with the batch submission process. Processing data received in a batch submission may take up to 30 minutes. Aircraft operators will need to allow sufficient time to process a batch submission to minimize delays in flight operations. The batch process is further discussed in this document.
APIS Quick Query	APIS is being enhanced to include a real-time component called APIS Quick Query (AQQ). AQQ is intended to prevent an inhibited passenger from boarding. AQQ allows for real-time transmission and automated screening of passenger data prior to boarding. Passengers with connecting flights may have their boarding passes issued to them for segments without a boarding pass printing result; however, they will not be granted access to their U.S.-destined flight segments until a Cleared or Selectee Response has been returned. Issuance of a boarding pass is prohibited for passengers who are attempting to check in for a direct departure to the U.S. or for flights departing from the U.S., until a boarding pass printing result is received. This eliminates the necessity for passenger removal and minimizes baggage off-loads. AQQ and the APIS batch system, when combined, are commonly referred to as APIS Pre-Departure.

The APIS Pre-Departure Final Rule implements these legislative requirements to further enhance national security and the security of the commercial air and vessel travel industries. APIS Pre-Departure requires transmission of, as appropriate, passenger and/or crewmember information early enough in the process to prevent a high-risk individual from boarding an aircraft.

The aircraft operator transmitting the APIS data must adhere to the APIS Pre-Departure Final Rule requirements for passengers having itineraries with an international city pair as follows:

1. The message format must be compliant with the updated UN/EDIFACT guidelines.
2. APIS data must be transmitted for the directional travel (see Section 4.3 for definition) of a passenger, and the complete itinerary for that passenger's specified flights must be provided.
3. The aircraft operator responsible for APIS data is the "aircraft operator of record." This entity operates the flight that will either arrive into or depart from the U.S.
4. In cases where aircraft operators maintain alliance partners, aircraft operators may elect to establish business practices where alliance partners collect and transfer APIS data to the aircraft operator of record transporting the passenger. These business models will be developed externally from DHS. They are the responsibility of each aircraft operator, should an aircraft operator and alliance partner choose to exchange and/or validate the APIS data.
5. The aircraft operator transporting the passenger over international boundaries is ultimately responsible for meeting APIS data requirements.
6. Aircraft operators that fail to transmit APIS data in accordance with the APIS Pre-Departure Final Rule may be subject to monetary penalties.
7. Aircraft operators must validate and transmit a complete APIS record prior to a passenger gaining access to an aircraft.
8. Aircraft operators may only transport a passenger for whom a Cleared or Selectee boarding pass printing result has been returned.

Aircraft operators may choose to submit minimum data to receive a boarding pass printing result, therefore allowing them to print a boarding pass when a passenger attempts to check in. Regardless of the timing of the watch list matching request submission, aircraft operators must comply with APIS Pre-Departure requirements prior to the passenger gaining access to the aircraft.

2.2 Secure Flight Final Rule

Secure Flight

TSA is assuming the watch list matching function from aircraft operators (currently carrying out this function under TSA security directives and emergency amendments) and CBP (for covered flights to and from the United States). To assume this function, TSA requires aircraft operators to collect information from passengers, transmit that information to TSA for watch list matching purposes, and process passengers in accordance with TSA instructions regarding boarding pass printing results.

TSA requires aircraft operators to request and collect passengers' full name, gender, date of birth, and Redress Number (if available; see Section 5.4 for details) or Known Traveler Number (if available). Aircraft operators must then transmit to TSA the Secure Flight Passenger Data (SFPD) record containing the information provided for each passenger, as well as passport information (if available), and certain non-personally identifiable information used to manage messages, including itinerary information. Itinerary information is required to support appropriate levels of regional security.

For non-travelers (who are not otherwise authorized, e.g., on-duty employees) seeking authorization to enter an airport sterile area in the U.S. (such as to escort a minor or disabled passenger), TSA is requiring aircraft operators to request the same data from these individuals as from passengers. Under the Final Rule, aircraft operators will transmit to TSA that information as well as certain non-personally identifiable information used to manage messages, including the airport code for the sterile area to which the non-traveler seeks access.

Under the Secure Flight Final Rule, TSA will match the information provided by aircraft operators against the watch list. Based on the boarding pass printing results, TSA will instruct an aircraft operator 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 the airport sterile area. To ensure the integrity of the boarding pass printing results and to prevent the use of fraudulent passes, TSA will work with the airline industry to design a solution using a bar code or optical character code on boarding passes. This concept will be developed at a future date.

This Final Rule requires passengers and non-travelers to provide full name, date of birth, and gender.

TSA recognizes that the data cannot be readily verified and requires the aircraft operator to verify information only in the event that a passenger or non-traveler appears to match a watch list entry (for further details, see Section 5.3.2).

If passenger information, as defined in Section 4.2.3 of this document, resides in a covered aircraft operator's systems and the aircraft operator auto-populates its reservation system with this information, the aircraft operator must include this information in the SFPD that are transmitted to TSA.

The goals of Secure Flight are to:

- Identify known and suspected terrorists
- Prevent individuals on the No Fly List from boarding an aircraft
- Subject individuals on the Selectee List to enhanced screening to determine if they are permitted prior to boarding an aircraft or gaining access to a sterile area
- Facilitate passenger air travel
- Protect individuals' privacy

CAPPS Obligation

As required by TSA, aircraft operators must continue running the Computer Assisted Passenger Prescreening System (CAPPS) or Domestic Selection Criteria (DSC), which is separate and different from Secure Flight. The Secure Flight program will not modify the TSA requirement for U.S. aircraft operators to operate CAPPS and identify Selectees as stipulated by the CAPPS program (including random selection) for both domestic and international flights.

As a point of clarification, the full CAPPS program refers to the behavioral evaluation/scoring that result in a Selectee designation, not the matching of passenger names to a watch list. This process is deemed to have continued benefit to the security process and requires data beyond the scope of the DHS watch list programs.

The following chart shows how a passenger or non-traveler would be handled based on the boarding pass printing results and the CAPPS evaluation.

Boarding Pass Printing Result	CAPPS Evaluation	Traveler Treatment
Clear	Not selectee	Clear
Selectee	Not selectee	Selectee
Inhibited	Not selectee	Inhibited
Clear	Selectee	Selectee
Selectee	Selectee	Selectee
Inhibited	Selectee	Inhibited

Secure Flight Rule Compliance

TSA will use a phased approach to implement Secure Flight. TSA will first conduct operational testing with aircraft operators to ensure that their systems are compatible with TSA's system. After successful operational testing with an

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

aircraft operator, TSA will assume the watch list matching function from that aircraft operator. TSA will assume responsibility for covered flights from covered U.S. aircraft operators first, followed by covered flights to, from, and overflying the United States from all covered aircraft operators. TSA will also assume responsibility for watch list matching for flights between two non-U.S. locations operated by covered U.S. aircraft operators.

The Aircraft Operator Implementation Plan in the Aircraft Operator Standard Security Plan (AOSSP) for U.S. aircraft operators and the Model Security Program (MSP) for foreign air carriers include the dates by which aircraft operators must request, collect, and transmit SFPD. TSA will inform aircraft operators of the date in which TSA will assume the watch list matching responsibility from the aircraft operator.

2.3 ESTA Interim Final Rule

Section 711 of the 9/11 Commission Act of 2007 requires that the Secretary of Department of Homeland Security (DHS), in consultation with the Secretary of the Department of State (DoS), develop and implement a fully automated ESTA to collect information from travelers seeking to visit the United States under the Visa Waiver Program (VWP) to determine whether the individual presents a security risk and is eligible to travel to the United States. An Interim Final Rule was published to satisfy this mandate on June 9, 2008.

ESTA is an internet enabled and accessible application that will allow individuals who wish to travel under the VWP to submit an application from anywhere in the world to obtain authorization to travel to the United States under the VWP. Approved travel authorization applications submitted via ESTA are granted for a period of two years, unless passport expiration dates limit validity, and are considered acceptable for multiple uses. Biographic information supplied by applicants is screened against law enforcement databases to identify those who may be ineligible for travel under the terms of the VWP as identified in Section 217 of the Immigration and Nationality Act or pose an elevated law enforcement risk.
The goals of the ESTA Interim Final Rule are:

- Enhance VWP security requirements;
- Extend visa-free travel to nationals of allied foreign countries;
- Enhance cooperation on counter-terrorism and information sharing;
- Support and expand tourism and business opportunities; and
- Strengthen bilateral relationships.

ESTA was developed and implemented under an aggressive schedule. Significant dates are as follows:

- June 9, 2008 – Interim Final Rule was published
- August 1, 2008 – ESTA web site will be operational and accessible to VWP travelers
- November 13, 2008 – A notice will be published in the Federal Register by the Secretary of Homeland Security indicating that ESTA will be implemented as a mandatory program
- January 12, 2009 – All VWP travelers will be required to have an electronic travel authorization via ESTA

- March 21, 2010-Carriers are subject to penalty for transporting non-compliant VWP travelers.

In order to ensure compliance with the 9/11 Act, aircraft operators must verify that VWP travelers have approved travel authorizations obtained via ESTA prior to authorizing their boarding of international flights en route to the United States. It was determined that this requirement can be best accomplished by leveraging the APIS Pre-Departure interactive messaging process. The submission of passenger manifest data compliant with the APIS Pre-Departure Rule automatically results in an ESTA status query, when applicable. In these cases, submission of data in compliance with the Secure Flight Final Rule that includes the passport number and country of issuance is sufficient to obtain an ESTA status message. It is returned to carriers upon submission of passenger data via APIS Batch Interactive and APIS Quick Query. CBP describes the messages and their operational implications in Section 4.5 of this document. **Submission of manifest data via eAPIS will result in an ESTA status message being returned through the eAPIS process. Carriers relying on receipt of ESTA status responses via the eAPIS mechanism should coordinate this function through the ESTA office and their APIS Account Manager.** CBP has and will continue to engage in an outreach effort to aircraft operators, travel industry professionals, other government agencies, and the traveling public to communicate this requirement.

The ESTA Interim Final Rule states that once carriers are capable of receiving and validating ESTA status messages, the CBP Form I-94W may be eliminated. System modifications to fully support this initiative have been completed, initial testing at selected sites has been successful, and CBP anticipates large-scale implementation of automated capabilities this year provided ongoing assessments stay positive and remaining carriers complete the requisite system modifications to accommodate ESTA.

3 IMPLEMENTATION GUIDE

The implementation guide explains the processes and procedures for aircraft operators to follow to comply with the APIS Pre-Departure Final Rule and the Secure Flight Final Rule. Compliance dates are specified in each rule (see Appendix 7.1).

DHS is committed to support all aircraft operators in their transition and integration process. To meet this need, DHS will use the knowledge and background of CBP and TSA officers in developing teams assigned to multiple aircraft operators that will coordinate testing, system integration, and process transition. DHS will also provide training to help aircraft operators meet their individual training needs.

DHS account managers will also work in monitoring aircraft operators' system rollout. Monitoring system rollout should aid in identifying an aircraft operator's process development. As additional needs arise, the account managers will work with aircraft operators individually or in groups.

3.1 Implementation Plan Procedures

TSA▶ TSA has modified the Aircraft Operator Standard Security Program and the Model Security Program to incorporate the Aircraft Operator Implementation Plan (AOIP).

CBP▶An implementation plan will not be necessary for aircraft operators attempting to comply with the APIS Pre-Departure requirements; APIS account managers will work individually with aircraft operators to establish testing and implementation timetables. Therefore, the remainder of this section contains instructions pertinent only to the Secure Flight Final Rule.

Registration

TSA▶ Each Secure Flight covered carrier are encouraged to register online at a URL which will be provided in the transmittal letter accompanying the proposed AOIP not later than the date by which comments on the proposed AOIP are due. Registered aircraft operators will receive the Aircraft Operator Deployment Guide, which includes test cases.

Approved AOIP

TSA▶ TSA issued a change to the AOSSP and the MSP incorporating the approved AOIP to aircraft operators. The AOIP establishes dates for compliance with the Secure Flight Final Rule.

AOIP Reconsideration

TSA▶ An aircraft operator may petition for reconsideration of the approved AOIP as specified in the Secure Flight Final Rule.

3.2 Implementation Coordination

Overall Coordination DHS recommends that aircraft operators' project organizations designate a point of contact for the implementation effort. DHS will establish a point of contact for each aircraft operator and establish an Implementation and Operations Team to support their implementation. The team will include network and system technical specialists to assist in implementing networking, messaging, system interfaces, and testing.

CBP▸ Aircraft operators may choose to submit APIS data through either the interactive batch manifest transmission or the AQQ transmission function, or through a combination of the interactive batch and AQQ transmission functions. Aircraft operators are encouraged to determine if it would be possible to use both transmission functions, as it is believed this will reduce a number of functions associated with APIS.

Aircraft operators may initially submit APIS data using the interactive batch process as they develop their AQQ capabilities. DHS is committed to working with the operators in every way possible to ensure that they can meet the function or functions best suited to their operations.

DHS understands that deploying functions in a phased approach may best suit an aircraft operator. Aircraft operators may submit AQQ transmissions from their U.S. locations prior to their foreign locations. This is acceptable as long as the aircraft operator is not in direct violation of current DHS submission requirements.

Project Communications

Correspondence from aircraft operators regarding the implementation plan should be sent to the following email addresses:

CBP▸ apisquickquery@dhs.gov

TSA▸ secureflight@dhs.gov

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

3.3 Training Support

To facilitate effective implementation, DHS will offer orientation training and informational materials to aircraft operator personnel responsible for establishing operational procedures that comply with DHS regulations. The DHS training support will assist the aircraft operators in making necessary adjustments to internal procedures in the following areas:

- Customer service
- Central reservations
- Technical operations

The following training support materials will be available from a secure website and the DHS implementation team:

- Job aids
- Technical FAQs
- User manuals
- Training modules
- Other DHS information

DHS will develop training modules that align with implementation milestones for APIS Pre-Departure and Secure Flight. Training will be provided to support the aircraft operators in implementing operational changes due to the publication of the rules. Figure 1 illustrates the planned training modules in relationship to key milestones for APIS Pre-Departure and Secure Flight. The timeline below is not drawn to scale and is subject to change.

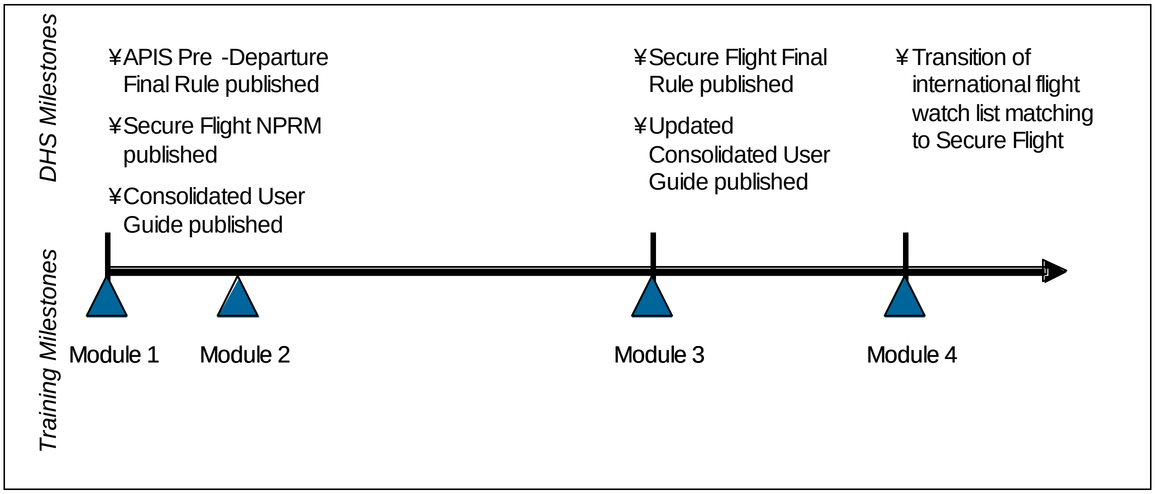
DHS Milestones
Training Milestones
¥APIS Pre -Departure Final Rule published
¥Secure Flight NPRM published
¥Consolidated User Guide published
¥Secure Flight Final Rule published
¥Updated Consolidated User Guide published
¥Transition of international flight watch list matching to Secure Flight
Module 1
Module 2
Module 3
Module 4

Figure 1 DHS Training Module

Module 1 One DHS Solution (APIS Pre-Departure and Secure Flight)

- One DHS Solution overview
- APIS Pre-Departure overview
- Secure Flight briefing

***WARNING:* This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

- DHS TRIP briefing

Module 2 DHS Pre-Departure Aircraft Operator Compliance Requirements

- Initial steps for APIS Pre-Departure aircraft operator compliance
  - APIS Pre-Departure contacts
  - Network connectivity options
- Technical compliance requirements
  - UN/EDIFACT messaging
  - Batch and interactive message submission
  - DHS Response Messages
  - Flight Close-out Messages
  - Passenger unique identifier
  - Changes to current internal watch list queries
  - Identifying and coordinating system outages (aircraft operator, DHS, or other components)
  - Identifying system or network problems
  - Troubleshooting tips
  - Procedures for obtaining guidance and assistance
- Operations compliance requirements
  - Standard operating procedures for handling DHS decisions
  - Anticipated public questions and recommended responses
  - Flight Close-out Messages
  - Irregular flight operations (IRROPS)
  - Procedures for obtaining guidance and assistance
- Final steps for APIS Pre-Departure aircraft operator compliance
  - System testing
  - APIS Pre-Departure authorization
  - Phased production deployment

Module 3 Secure Flight Implementation

- Technical compliance requirements
  - Identifying and coordinating system outages (aircraft operator, DHS, or other components)
  - Identifying system or network problems
  - Overall program-level coordination
  - Procedures for obtaining guidance and assistance
- Operations compliance requirements
  - Updated Secure Flight overview
  - Secure Flight privacy notice
  - Overview of the watch list matching process
  - Standard operating procedures for handling DHS decisions
  - Anticipated public questions and recommended responses

Module 4 Transition of International Watch List Matching

- Transition of covered flights to/from Secure Flight
- Secure Flight updates

DHS training materials will be posted on the TSA Web Board or available through the DHS implementation teams.

3.4 Testing

Successful implementation is dependent on the ability to conduct a full range of system and operational testing between DHS and aircraft operators prior to cutover. Cutover is defined as the time when the aircraft operator and DHS initiate production operations for APIS Pre-Departure and/or the Secure Flight requirements. Testing will be performed based on a series of test cases, specific to each testing phase and type of component being tested. Each test case will include defined success criteria. Movement to the next phase of testing and eventual production cutover will not occur until all exit criteria have been met.

The aircraft operator and DHS will jointly validate all testing. Additional testing requested by the aircraft operator will be scheduled to the extent possible. Each aircraft operator is expected to conduct their own internal system and unit testing prior to testing with DHS. During the aircraft operator's internal system testing phase, CBP or TSA (as applicable) will be available for questions and clarifications, but will not participate in the test execution.

The objective of testing is to validate automated system processes from the transmission of data from aircraft operators, completion of the watch list matching, and issuance of boarding pass printing results.

CBP▶ CBP will work with each aircraft operator directly to develop and execute testing. It is anticipated that non-U.S. and U.S. aircraft operators, with both domestic and international flights, will conduct functionality testing prior to implementing CBP requirements. In doing so, DHS anticipates that any eventual Secure Flight system-related testing would be less extensive for these aircraft operators. TSA has designed the Secure Flight requirements in such a way that the CBP-required functionality testing should be very similar to any eventual Secure Flight testing. DHS is interested in comments that would help DHS ensure this is the case.

Aircraft operators that have already completed AQQ testing will coordinate through their assigned AQQ tester to determine any additional testing needed to verify their ability to receive and manage returned ESTA responses. Aircraft operators that have not completed testing can coordinate with their assigned AQQ tester to conduct ESTA testing.

TSA▶ The operational test readiness date for Secure Flight testing will be provided to each aircraft operator in their AOIP.

3.4.1 Testing Phases

Table 1 Testing Phases and Affected Aircraft Operators

Aircraft Operator Type	APIS – Test Phases	Secure Flight – Test Phases
U.S. – domestic-only operations		1, 2, 3, and 4
U.S. – domestic and international operations	2 & 3	Limited validation of 2 and 3; full set of 1 and 4
Non-U.S. (international)	2 & 3	1, 2, 3, and 4

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

Table 2 below illustrates the testing phases.

Table 2 Test Phases

Test Phase 1	Aircraft Operator Internal System Testing	Each aircraft operator is expected to conduct internal system testing prior to testing with DHS. During this internal system testing phase, the TSA or CBP point of contact (as applicable) will be available for questions and clarifications, but will not participate in the test execution.
Test Phase 2	Connectivity Testing	This test phase covers the testing of communication link(s) between aircraft operators and the DHS Router, and the communication link(s) between the DHS Router and Secure Flight. It also includes message configuration and transmission testing.
Test Phase 3	System-to-System Interface Testing	The focus of this testing phase is to ensure full integration of system components between the aircraft operator and DHS. This testing will validate that each passenger transaction and matching result can be generated, transmitted, received in the correct message and data formats, and processed successfully. System testing will be conducted in a test environment using simulated data. At the successful conclusion of this phase, DHS will certify the aircraft operator for follow-on development and cutover testing.
Testing Phase 4	Development and Cutover Testing	This test phase will include any follow-on testing to validate that the aircraft operator system and associated processes will function as intended in an operational production environment.

TSA▶ Aircraft operators covered by the APIS Final Rule who have completed Test Phase 2 Connectivity Testing during testing for APIS Pre-Departure do not need to complete this testing phase unless their network or message configuration is modified for Secure Flight. Aircraft operators who are APIS Pre-Departure certified and utilize the APIS Interactive (Batch and/or Quick Query) method for transmission of APIS data will perform a subset of the Test Phase 3 test cases normally required for aircraft operators. Additional test documentation will be provided to aircraft operators.

3.5 Readiness for Cutover; Cutover Certification

Production cutover indicates when the aircraft operator and DHS initiate production operations for APIS Pre-Departure and/or Secure Flight. The timing of the issuance of CBP and TSA regulations will specify separate cutover activities for each of these programs. Aircraft operators may choose to phase implementation for APIS Pre-Departure by routes, airports, or any other basis agreed upon by CBP. Aircraft operators may also choose a phased implementation for Secure Flight if permitted by TSA. However, aircraft operators must have initiated full cutover prior to the established date required for regulatory compliance. In the case of APIS Pre-Departure, aircraft operators who fail to meet the date mandated for implementation must provide their APIS manifests in the APIS batch format, pre-departure.

TSA▶ The required date for submission of data for Secure Flight watch list matching will be included in the AOIP issued to each aircraft operator.

Aircraft Operator Readiness

Prior to cutover to full production, the aircraft operator should assess internal readiness to support the technology and business process changes. The readiness assessment should include confirmation of the following:

- Standard operating procedures and policies are established

- All internal aircraft operator testing was successful
- All phases of testing with TSA and/or CBP, as applicable, were successful including full volume and response time tests
- Cutover and go-live plan is developed and ready for execution
- Roll-back plan is ready to be executed, if necessary
- Operational and Service Center staffs are operational

TSA or CBP Readiness

Prior to cutover to full production, TSA and CBP shall assess internal readiness to support the volume of production activity from an aircraft operator. The readiness assessment should include, but is not limited to, confirmation of the following:

- DHS Operations Team(s) are staffed and prepared for production volume
- Network communication is satisfactory
- Internal testing was successful
- Testing with the aircraft operator was successful
- System vulnerabilities are identified and corrected/mitigated
- Cutover and go-live plan is ready to be executed
- Roll-back plan is ready to be executed, if necessary

Post-cutover Transition

During the post-cutover period, TSA and CBP aircraft operator implementation and operations teams will phase out certain responsibilities to operational and Service Center (DHS or Secure Flight as applicable) staffs established to provide ongoing support. These responsibilities include answering aircraft operator questions and addressing their concerns. Formal communication with an aircraft operator will occur when the initial post implementation support has concluded. At this point, DHS will consider the aircraft operator to be fully transitioned to production operation.

Compliance with Dates

All cutovers must be completed in compliance with deadlines mandated in the applicable regulations (see Appendix 7.1) and standard security programs.

TSA▶ Deployment Plan

The deployment plan for Secure Flight will incorporate the above test phases, certification, system and operational readiness and cutover to production. The plan has four phases as described in Table 3:

Table 3 Secure Flight Deployment Phases

Phase 1	Aircraft Operator Interface Testing	Consists of the testing associated with the Connectivity and System-to-System Interface test phases described above,
Phase 2	Assessment	Includes assessment of Aircraft Operator Interface testing and validation that testing has successfully completed.
Phase 3	On-boarding	During this phase the aircraft operator will submit passenger data but will not apply boarding pass printing results returned by Secure Flight. It will also include a readiness review to ensure that all requirements for effective Secure Flight operations have been implemented. The final step of this phase will be a pre-production cutover assessment that provides a final opportunity to mutually verify expected and acceptable performance prior to initiation of production cutover.

Table 3 Secure Flight Deployment Phases

Phase 4	Production Cutover	Production cutover will occur beginning at 72 hours prior to the cutover date and time." Cutover" is the date and time of the first flight that will be applying Secure Flight matching results. At that time, the aircraft operator system will be connected to the Secure Flight production environment and begin submitting passenger data. It will conclude when the aircraft operator is using Secure Flight boarding pass printing results for all passengers and non-travelers.

4 TECHNICAL REQUIREMENTS GUIDE

4.1 Data Interchange and Messaging Facility

Single Interface

DHS will provide all aircraft operators with a single point of transmission when submitting data in either a batch or interactive mode. The single point of transmission will identify the data content, route data elements, and return the matching result to the original message sender. A consolidated set of data elements and the events that trigger submissions will enable aircraft operators to fulfill data submission requirements for APIS Pre-Departure and requirements for the Secure Flight Final Rule. This is illustrated in Figure 2 below. For details of the Passenger Data Message formatting, see Section 4.9. Technology providers who deliver shared services for multiple aircraft operators over this single interface will, in some cases, need to deploy additional capability to route messages to the appropriate queue / workflow, corresponding with the watch list matching method utilized by a specific aircraft operator; namely: 1) CBP only, 2) a combination of CBP / Secure Flight, or 3) Secure Flight only.

CBP▸ APIS data submissions will be formatted in UN/EDIFACT (PAXLST and Customs Response Message [CUSRES]) only; this is in accordance with the APIS Pre-Departure Final Rule.

TSA▸ SFPD submissions may be formatted using either UN/EDIFACT or XML. An aircraft operator can only use one format of transmission. For example, if an aircraft operator is using UN/EDIFACT, then all submissions must be in UN/EDIFACT.

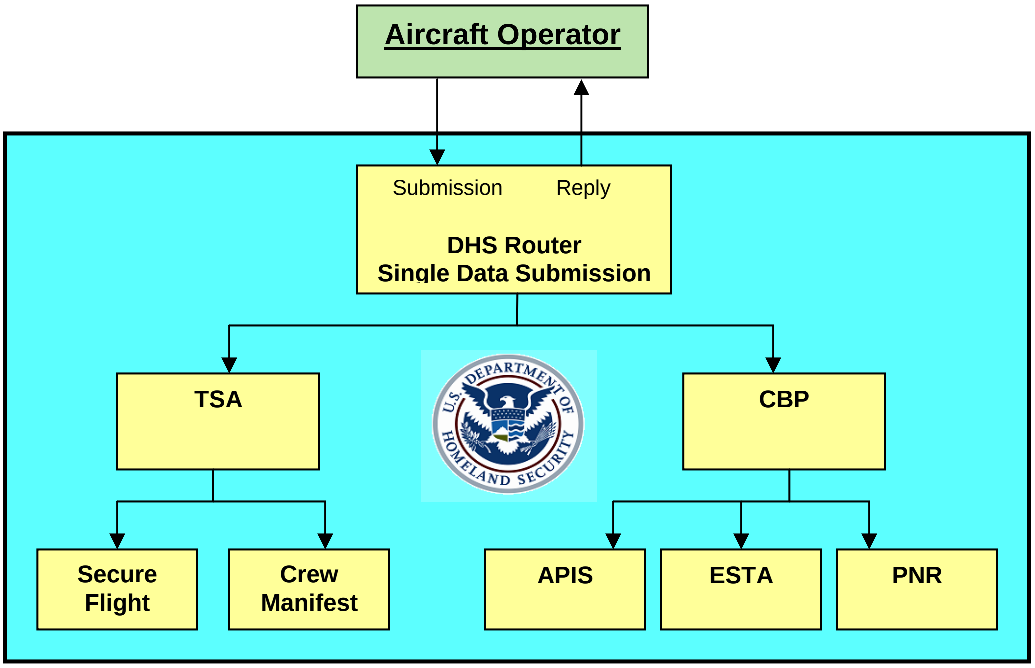

Figure 2 Single Communications Interface and Single Submission

4.2 Data Requirements

The subsections below list the data requirements for each rule.

4.2.1 APIS Pre-Departure Final Rule Data Requirements

The data elements listed in Table 4 identify those data elements required to meet the APIS Pre-Departure Final Rule. Submission requirements may differ from those necessary to receive a boarding pass printing result. Submission of data compliant with the APIS Pre-Departure Final Rule will be sufficient to obtain an ESTA status verification.

Table 4 APIS Pre-Departure Final Rule Data Elements – International Passengers

Data element	Definition	Mandatory	Comment
Last name	Passenger last name	Y	Complete last name
First name	Passenger first name	Y	Complete first name. First names submitted with a single character are allowable; however, may result in a higher occurrence of Inhibited responses.
Middle name	Passenger middle name	Mandatory if available	If available

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

Table 4 APIS Pre-Departure Final Rule Data Elements – International Passengers

Data element	Definition	Mandatory	Comment
Date of birth	Passenger date of birth	Y	Must be valid month, valid day within month, and valid year. Format for date of birth is yymmdd, as found in the Machine Readable Zone of an acceptable travel document.
Gender	Passenger gender	Y	Only M (male) or F (female) allowed.
Redress number	DHS-assigned redress number	Mandatory if available	
Citizenship	Passenger citizenship	Y	Validated against the ICAO country code list (ISO 3166).
Country of residence	Country where passenger resides	Y	Country of residence is required for arriving passengers only. Validated against the ICAO country code list (ISO 3166).
Status on board the aircraft	Passenger is either passenger or crew member	Y	Status code is further described in UN/EDIFACT PAXLST Guide.
Travel document type **	1-2 character code that represents the accepted government travel document	Y	CBP-accepted document type codes: P – passport C – permanent resident card A – resident alien card G – U.S. Merchant Mariner Card M – U.S. military identification T – re-entry permit or refugee permit F – facilitation document IN – NEXUS IS – SENTRY
Document number	Document number	Y	
Document country of issuance	Country issuing document	Y	Validated against the ICAO country code list (ISO 3166).
Document expiration date **	The expiration date for the document	Mandatory for passport only	Expiration date is required for passports only. Must be valid month, valid day within month, and valid year. Format for expiration date is yymmdd, as found in the Machine Readable Zone of an acceptable travel document.
Address while in the United States	Passenger address while in the U.S.	Y	Mandatory for visiting foreign nationals, only on a flight inbound to the United States.
Record Locator (PNR) *	Record Locator identifier	Y (If available)	The Record Locator shall be used by DHS in the response message and any required acknowledgements from the aircraft operator. Carriers using an established reservation system are required to provide the Record Locator Identifier.
Passenger Reference Number	Unique passenger identifier	Y	The Passenger Reference Number is used in combination with the record locator to uniquely describe a passenger to DHS as well as from DHS for responses and acknowledgements. Carriers sending interactive data are required to provide, at a minimum, a Unique passenger identifier.
Passenger itinerary: airport where transportation began (embarkation)	Airport of known embarkation	Y	Validated against the International Air Transport Association (IATA) airport code list.
Passenger itinerary: airport of first (arrival)	For U.S. arrivals, the airport where CBP processing occurs	Y	Validated against the IATA airport code list. APIS Pre-Departure Final Rule requirement for U.S. arrivals.

***WARNING:* This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

Table 4 APIS Pre-Departure Final Rule Data Elements – International Passengers

Data element	Definition	Mandatory	Comment
Passenger itinerary: final airport of destination (debarkation)	Airport of known debarkation	Y	Validated against the IATA airport code list.
Aircraft operator code	IATA or ICAO carrier code, as commonly used by aircraft operator for APIS transmissions	Y	Validated against the IATA or ICAO aircraft operator code list.
Flight number	Flight number assigned by aircraft operator	Y	Alphanumeric
Flight itinerary: last foreign port/place of call (departure port code)	Flight departure airport	Y	Validated against the IATA airport code list.
Scheduled date/time of aircraft departure	Flight departure time	Y	Valid month, valid day within the month, and valid year.
Flight itinerary: port/place of first arrival (CBP clearance port code for U.S. arrivals)	Flight arrival airport	Y	Validated against the IATA airport code list.
Scheduled date/time of aircraft arrival	Flight arrival time	Y	Valid month, valid day within the month, and valid year.

* Generally, a Passenger Name Record locator remains unchanged for the life of a booking record (except from split or divided records which are covered elsewhere). In the unlikely event that a Passenger Name Record Locator changes, the aircraft operator may choose to generate a new submission or may elect to submit a qualified change.

** The Travel Document Type and Document Expiration Date should be considered qualified changes as they are changes to the passenger's information resulting in the submission of a Change Passenger type message. Secure Flight only accepts a Document Type = Passport (P) for SFPD. Other document types required for APIS will not be passed to Secure Flight if provided by the carrier to meet APIS requirements.

4.2.2 Secure Flight Rule

The data elements listed in Table 5 identify those data elements that TSA requires aircraft operators to transmit to TSA under the Secure Flight Final Rule.

Table 5 Secure Flight Passenger Data Elements

Data Element	Definition	Mandatory	Comment
Last name	Passenger last name	Y	Complete last name.
First name	Passenger first name	Y	Complete first name. First names submitted with a single character are allowable; however, may result in a higher occurrence of Inhibited responses. In cases where the passenger has a single name, record that as the last name and insert FNU (first name unknown) in the first name field.

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

Table 5 Secure Flight Passenger Data Elements

Data Element	Definition	Mandatory	Comment
Middle name	Passenger middle name	Mandatory if available	If available If no middle name field, the middle name can be submitted in the first name field so long as it is space delimited.
Date of birth *	Passenger date of birth	Y	Must be valid month, valid day within month, and valid year. Format for date of birth is yymmdd, as found in the Machine Readable Zone of an acceptable travel document.
Gender *	Passenger gender	Y	Only M (male) or F (female) allowed.
Redress number	DHS-assigned redress number	Mandatory if available	DHS-issued redress number
Known Traveler number	Identification number assigned to a person who participates in the Known Traveler program	Mandatory if available	Unique number assigned to a person after the Federal Government has conducted a threat assessment.
Passport type	Type limited to passport	Mandatory if available	Passport document indicator
Passport number	Passport number	Mandatory if available	Alphanumeric, no special characters
Passport country of issuance	Country issuing document	Mandatory if available	Validated against the ICAO country code list (ISO 3166).
Passport expiration date	Expiration date of document	Mandatory if available	Must be valid month, valid day within month, and valid year. Format for date of expiration is yymmdd, as found in the Machine Readable Zone of an acceptable travel document.
Record Locator **	Record Locator Identifier	Y	The Record Locator shall be used by DHS in the response message and any required acknowledgements from the aircraft operator. This field is case insensitive.
Passenger Reference Number ***	Unique Passenger identifier	Y	The Passenger Reference Number is used in combination with the Record Locator to uniquely describe a passenger to DHS as well as from DHS for responses and acknowledgements.
Aircraft operator code	Aircraft operator code	Y	Validated against the IATA or ICAO aircraft operator code list.
Flight number	Flight number	Y	Up to 4 digits in length
Flight itinerary: departure airport	Flight departure airport	Y	Validated against the IATA airport code list.
Scheduled date/time of aircraft departure	Flight departure time	Y	Valid month, valid day within the month, and valid year
Arrival airport	Flight arrival airport	Y	Validated against the IATA airport code list.
Scheduled date/time of aircraft arrival	Flight arrival time	Y	Valid month, valid day within the month, and valid year
Schema Version	XML schema version	N	Version of the schema used to generate the current message. Applies only to XML submissions.
Time Stamp	Message time stamp	Y	The timestamp the current message was created
Verified ID indicator	ID has been verified by ticket counter	N	This field will only be set when the passenger’s information has been verified by ID by an agent at the ticket counter; just a yes or no indicates verification.

* Under the Secure Flight Final Rule, date of birth and gender are mandatory data elements.

***WARNING:* This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

** A record locator is a value assigned by the aircraft operator to a booking for one or more passengers and contains one or more flight segments. The record locator must be unique within the active bookings for that aircraft operator and must persist unchanged for the life of the booking. The life of the booking is from the first to last flight in a given booking. TSA understands that when booking records are divided that one or more of the travelers will be assigned a new record locator number. Guidance on data submission for this case is contained in the Data Submission Rules section of this document. Aircraft operators whose systems do not routinely create a record locator may satisfy this requirement by creating a number consistent with the data element definition and the attributes described above.

*** A passenger reference number is a value assigned by the aircraft operator to each individual included in a booking (each record locator consist of a single booking). The passenger reference number must be unique for each passenger in that booking and must persist unchanged for the life of the booking. The life of the booking is from the first to last flight in a given booking. When individuals are removed from a booking record the passenger reference number(s) for the remaining passenger(s) must remain unchanged. When booking records are divided causing one or more of the travelers to be assigned a new record locator number, the previous passenger reference number is not expected to carry over to the new booking. Guidance on data submission for this case is contained in the Data Submission Rules section of this document. Aircraft operators whose systems do not routinely create a passenger reference number may satisfy this requirement by creating a number consistent with the data element definition and the attributes described above.

4.3 Required Submissions

Passenger Data Transmission

CBP▸ In the APIS Pre-Departure Final Rule, DHS requires the aircraft operator to transmit 100 percent of the passenger data records containing confirmed, cancelled (if previously transmitted), or standby (revenue and non-revenue) international passengers. Data submissions may start approximately 72 hours prior to scheduled flight departure time. Data submission is based on directional travel. Information on bookings made and cancelled before 72 hours prior to flight departure is not required. APIS data can be collected at the first point of travel with an aircraft operator. APIS data must be submitted and validated prior to the passenger gaining access to a flight for which APIS data is required. Submission of data in compliance with the APIS Pre-Departure Final Rule will be sufficient to provide the aircraft operator with an ESTA status message.

TSA▸ In the Secure Flight Final Rule, TSA requires the aircraft operator to transmit 100 percent of SFPD records containing confirmed, cancelled (if previously transmitted), or standby (revenue and non-revenue) domestic and/or international passengers. SFPD transmissions must start approximately 72 hours prior to scheduled flight departure time. Data submission is based on directional travel. SFPD submission must include all of the flight segments meeting the directional travel definition in a single data transmission. Aircraft operators do not need to transmit SFPD records for reservations made and cancelled before 72 hours prior to flight departure.

Directional Travel

Directional travel is defined as one or more flight segments operated by the submitting aircraft operator, which meets *ALL* the following rules:

- Does not include both a flight into the U.S. and a flight departing the U.S.
- Connecting flights may not exceed 12 hours between scheduled arrival and scheduled departure
- The destination is not the origin or a coterminous airport (e.g., JFK, EWR, and LGA)

Note: The submitting aircraft operator may be explicitly authorized by TSA to submit SFPD for certain express aircraft operators. Aircraft operators performing ground handling on behalf of a covered aircraft operator may also submit compliant SFPD on behalf of the covered aircraft operator. Aside from these exceptions, only flight segments operated by the submitting aircraft operator may be transmitted to Secure Flight.

Itinerary

Itinerary data includes the following data elements:

- Aircraft operator code
- Flight number
- Departure airport
- Scheduled date/time of aircraft departure
- Arrival airport

- Scheduled date/time of aircraft arrival

Itinerary data is to be included if and only if it meets all the following rules:

- Unflown flight segments conforming to the directional travel definition
- Does not include future flight segments that extend beyond the flights meeting the criteria for directional travel
- Flown flight segments are not included

Table 6 Example Itinerary: ORD-LHR Roundtrip – Same Aircraft Operator

Direction of Travel	Routing	Requirement
1 – Outbound	ORD – NYC – LHR	The aircraft operator is required to collect and transmit passenger data prior to embarkation from Chicago to New York, with inclusion of the London leg.
2 – Inbound	LHR – NYC – ORD	The aircraft operator is required to transmit passenger data prior to embarkation from London to New York, with inclusion of the Chicago leg.

Passenger Data Collection

Aircraft operators have multiple sources of reservation bookings. Passenger data is collected in various ways at each entry point and ultimately the data is aggregated in an aircraft operator’s system. Booking locations may include, for example, reservations offices, travel agencies, internet-based commerce, self-service devices (kiosks), ticket counters, gate locations, and off-airport aircraft operator ticket offices.

Events when aircraft operators are required to transmit passenger data are shown in Table 7.

Table 7 Passenger Data Required Transmission Timing

Conditions	Requirement	Timing	Method
Initial 72-hour passenger data transmission	The aircraft operator will send initial passenger that includes Secure Flight required data: full name, date of birth and gender to DHS.	Approximately 72 hours before departure of a flight	Batch
New passenger bookings occurring after the initial 72-hour submission and updated passenger data	After initial passenger data transmission, the aircraft operator will send passenger data for 1) any new passenger bookings or 2) any previously submitted passenger bookings when a passenger data is updated or additional Secure Flight or APIS required data is collected (see Section 4.6).	Between 72 hours prior to departure and passenger boarding.	Batch (between 72 and 24 hours prior to scheduled departure) or Interactive (within 24 hours)
Passenger has no stored boarding pass printing result	The aircraft operator will send passenger data to DHS when flight check-in is requested for a passenger who has no stored boarding pass printing result.	Between 24 hours prior to departure and passenger boarding.	Interactive

Table 7 Passenger Data Required Transmission Timing

Conditions	Requirement	Timing	Method
Inhibited passenger presents ID at aircraft operator ticket counter	The aircraft operator will send passenger data verified from an appropriate ID to DHS and include an update indicator for Verified ID.	At the time of check-in from a ticket counter or authorized self-service kiosk.	Interactive
Post departure (international travel only)	Upon departure, the aircraft operator will be required to transmit the Flight Close-out Message. This message communicates the actual movement or cancellation of a flight, the passengers boarded, and the number of passengers boarded.	Post departure – no more than 30 minutes after departure	Batch

As detailed in Table 7, four events trigger an aircraft operator to submit passenger data. The first three apply to all domestic and international passenger travel while the fourth applies only to international flights:

1. 72-hour passenger data submission occurs at 72 hours prior to scheduled departure of the first covered flight of the passenger's directional travel. For passengers with directional travel that includes more than one covered flight segment, the submission must contain itinerary information for all covered flight segments, with no additional 72-hour submission at the scheduled departure time(s) of connecting flight(s). Flight segments operated by other aircraft operators must not be included in the submission. Passenger data for flights departing in a 24-hour period that is 48 to 72 hours from their scheduled departure time may be sent in as a single submission at 72 hours. Alternatively, the aircraft operator may elect to submit data for each flight(s) corresponding to the definition of directional travel at approximately 72 hours prior to its scheduled departure time. The passenger data for the 72 hour submission is sent in batch mode with a low priority.
2. Certain modifications and all cancellations for the subject flight are to be submitted. Aircraft operators submit passenger data in batch mode for departures more than 24 hours in the future, and in interactive mode within 24 hours of schedule flight departure.
3. For a passenger without a boarding pass printing result at check-in, DHS requires submission of the passenger's data in high priority, interactive mode.
4. For domestic travel, TSA does not require the aircraft operators passenger data post departure. For international flights, however, CBP requires a Flight Close-out Message detailing which passengers actually boarded the flight. This message must be sent no later than 30 minutes after departure, as required in the APIS Pre-Departure Final Rule.

For aircraft operators using the preferred MQ Websphere infrastructure for data transmissions, transmissions designated as "batch" must be submitted on the "low priority" queue. Data transmissions designated as "interactive" must be submitted on the "high priority" queue. Unless specifically authorized for a variance in timing, transmissions designated as using both, transmissions occurring greater than 24 hours prior to scheduled flight departure must be submitted on the low priority queue. Transmissions occurring within 24 hours of scheduled flight departure must be submitted on the high priority queue.

4.4 Required Transmission Events

Aircraft operators are required to send data, request boarding pass printing results, manage responses, and send flight reports, as follows.

Table 8 Required Transmission Events

Event	Requirements
Domestic passenger travel	Phase I – Aircraft operators conduct watch list matching of passengers 1. Except as noted in #2 below, aircraft operators must conduct watch list matching of passengers pursuant to applicable security directives and emergency amendments. 2. If the domestic flight is connecting to or from an international flight and the aircraft operator receives a boarding pass printing result from DHS at least 24 hours prior to the scheduled departure of the domestic flight, the aircraft operator may use the boarding pass printing result in lieu of conducting the watch list matching. Phases II and III -- TSA performs watch list matching: 1. DHS requires the submission of SFPD for air travel within the United States. 2. SFPD data must be submitted to TSA approximately 72 hours prior to scheduled flight departure. 3. For reservations received within 72 hours of a scheduled flight, SFPD must be submitted at the time the reservation is received and processed. 4. For “inhibited” passengers whose personal information is verified at check-in thru the verified ID process described in section 5.3.3, SFPD must be submitted with an indication that personal information has been verified 5. DHS will return a boarding pass printing result to the aircraft operator for appropriate action. 6. ESTA requirements are not applicable for domestic travel, therefore the “Not Applicable” code will be returned.
International Passenger inbound to U.S.	Phases I and II – CBP performs APIS functions and watch list matching: 1. Aircraft operators must transmit APIS data to DHS for international travel bound for the United States. Any additional Secure Flight data requirements not applicable for these phases. 2. Aircraft operators must transmit APIS data to DHS for international travel departing pre-clearance locations, bound for the United States. 3. If initially provided, DHS will use the full name, date of birth, gender, and acceptable travel document data to perform watch list matching. 4. At a minimum, the full name and date of birth will be used to perform watch list matching. 5. Passport number and country of issuance will be required for ESTA vetting. 6. DHS will return a boarding pass printing result to the aircraft operator. 7. As APIS data is received, an APIS manifest will be dynamically built. 8. For flights arriving into the United States, access to PNR data is required by CBP. 9. Aircraft operators must validate the data found in the Machine Readable Zone of a passenger’s government issued travel document, with data previously submitted, Validation can occur with the use of a document reader or through visual comparison of data. Phase III – CBP performs APIS functions, TSA performs watch list matching: 1. Aircraft operators must transmit APIS data to DHS for international travel departing pre-clearance locations, bound for the United States. 2. SFPD data must be submitted to TSA approximately 72 hours prior to scheduled flight departure. 3. For reservations received within 72 hours of a scheduled flight, SFPD must be submitted at the time the reservation is received and processed. 4. For “inhibited” passengers whose personal information is verified at check-in thru the verified ID process described in section 5.3.3, SFPD must be submitted with an

Table 8 Required Transmission Events

Event	Requirements
	indication that personal information has been verified. 5. DHS will return a boarding pass printing result to the aircraft operator that includes results of watch list matching and ESTA vetting. 6. As APIS data is received, an APIS manifest will be dynamically built. 7. For flights arriving into the United States, access to PNR data is required by CBP. 8. Passport number and country of issuance will be required for ESTA vetting. 9. Aircraft operators must validate the data found in the Machine Readable Zone of a passenger's government issued travel document, with data previously submitted. Validation can occur with the use of a document reader or through visual comparison of data.
International Passenger outbound from U.S.	Phases I and II – CBP performs APIS functions and watch list matching: 1. Aircraft operators must transmit APIS data to DHS for travel outbound from the United States. Any additional Secure Flight data requirements not applicable for these phases. 2. If initially provided, DHS will use the full name, date of birth, gender, and acceptable travel document data to perform watch list matching. 3. At a minimum, the full name and date of birth will be used to perform watch list matching. 4. A message indicating Travel Authorization via ESTA not applicable will be returned for all outbound APIS transmissions. 5. DHS will return a boarding pass printing result to the aircraft operator 6. As APIS data is received, an APIS manifest will be dynamically built. 7. For flights departing the United States, access to PNR data is required by CBP. 8. Aircraft operators must validate the data found in the Machine Readable Zone of a passenger's government issued travel document, with data previously submitted. 9. Validation can occur with the use of a document reader or through visual comparison of data Phase III – CBP performs APIS functions and TSA performs watch list matching: 1. Aircraft operators must transmit SFPD and APIS data to DHS for travel outbound from the United States for watch list matching. 2. SFPD data must be submitted to TSA approximately 72 hours prior to scheduled flight departure. 3. For reservations received within 72 hours of a scheduled flight, SFPD must be submitted at the time the reservation is received and processed. 4. For "inhibited" passengers whose personal information is verified at check-in thru the verified ID process described in section 5.3.3, SFPD must be submitted with an indication that personal information has been verified 5. A message indicating Travel Authorization via ESTA not applicable will be returned for all outbound APIS transmissions. 6. DHS will return a boarding pass printing result to the aircraft operator. 7. As APIS data is received, an APIS manifest will be dynamically built. 8. For flights departing the United States, access to PNR data is required by CBP. 9. Aircraft operators must validate the data found in the Machine Readable Zone of a passenger's government issued travel document, with data previously submitted. 10. Validation can occur with the use of a document reader or through visual comparison of data.
International-to-international passenger (Passengers originating outside	Phases I and II – CBP performs APIS functions and watch list matching: 1. Aircraft operators are required to transmit APIS data to DHS for passengers holding international-to-international travel itineraries, where they are processed by CBP upon arrival. 2. Separate APIS data transmissions will be required for passenger arrival and departure segments.

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

Table 8 Required Transmission Events

Event	Requirements
the U.S. with a connecting departure from the U.S. to a non U.S. destination)	3. If initially provided, DHS will use the full name, date of birth, gender, and acceptable travel document data to perform watch list matching. 4. At a minimum, the full name and date of birth will be used to perform watch list matching. 5. Passport number and passport country of issuance will be required for ESTA Vetting and the ESTA vetting message will reflect only the status associated with the international arrival portion of the itinerary. 6. DHS will return a boarding pass printing result to the aircraft operator. 7. As APIS data is received, an APIS manifest will be dynamically built. 8. For flights arriving into the United States, access to passenger name record (PNR) data is required by CBP. Phase III – CBP performs APIS functions and TSA performs watch list matching: 1. Aircraft operators are required to transmit APIS data to DHS for passengers holding international-to-international travel itineraries, where they are processed by CBP upon arrival. 2. Separate APIS data transmissions will be required for passenger arrival and departure segments. 3. SFPD data must be submitted to TSA approximately 72 hours prior to scheduled flight departure. 4. For reservations received within 72 hours of a scheduled flight, SFPD must be submitted at the time the reservation is received and processed. 5. For "inhibited" passengers whose personal information is verified at check-in thru the verified ID process described in section 5.3.3, SFPD must be submitted with an indication that personal information has been verified 6. Passport number and passport country of issuance will be required for ESTA Vetting and the ESTA vetting message will reflect only the status associated with the international arrival portion of the itinerary. 7. DHS will return a boarding pass printing result to the aircraft operator. 8. As APIS data is received, an APIS manifest will be dynamically built. 9. For flights arriving into the United States, access to passenger name record (PNR) data is required by CBP.
Domestic passenger with international connecting flight	Phases I and II – CBP performs APIS functions and watch list matching 1. Aircraft operators must transmit APIS data to DHS for domestic passengers with an international connecting flight. Any additional Secure Flight data requirements are not applicable for these phases. 2. APIS data is not required for the domestic portion. However, if initially provided, DHS will use the full name, date of birth, gender, and acceptable travel document data to perform watch list matching. 3. At a minimum, the full name and date of birth will be used to perform watch list matching. 4. DHS will return a boarding pass printing result to the aircraft operator. If the aircraft operator receives the boarding pass printing result at least 24 hours prior to the scheduled departure of the flight, the aircraft operator may use boarding pass printing result for the domestic flight in lieu of the aircraft operator conducting the watch list matching. 5. A message indicating Travel Authorization via ESTA not applicable will be returned for all domestic passengers with an international connecting flight. 6. As APIS data is received, an APIS manifest will be dynamically built for the international connecting flight. 7. For flights departing the United States, access to passenger name record (PNR) data is required by CBP. 8. Aircraft operators must validate the data found in the Machine Readable Zone of a

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

Table 8 Required Transmission Events

Event	Requirements
	passenger’s government issued travel document, with data previously submitted. Validation can occur with the use of a document reader or through visual comparison of data. Phase III – CBP performs APIS functions, TSA performs watch list matching 1. No special handling is required, TSA will return a boarding pass printing result to the aircraft operator for flights meeting the “directional travel” criteria 2. Aircraft operators must transmit SFPD and APIS data to DHS for travel outbound from the United States. 3. SFPD data must be submitted to TSA approximately 72 hours prior to scheduled flight departure. 4. For reservations received within 72 hours of a scheduled flight, SFPD must be submitted at the time the reservation is received and processed. 5. For “inhibited” passengers whose personal information is verified at check-in thru the verified ID process described in section 5.3.3, SFPD must be submitted with an indication that personal information has been verified 6. A message indicating Travel Authorization via ESTA not applicable will be returned for all outbound APIS transmissions. 7. DHS will return a boarding pass printing result to the aircraft operator. 8. As APIS data is received, an APIS manifest will be dynamically built. 9. For flights departing the United States, access to PNR data is required by CBP. 10. Aircraft operators must validate the data found in the Machine Readable Zone of a passenger’s government issued travel document, with data previously submitted. Validation can occur with the use of a document reader or through visual comparison of data.
International passenger with domestic connecting flight	Phases I and II – CBP performing APIS functions and watch list matching 1. Aircraft operators must transmit APIS data for international passengers with a domestic connecting flight. Any additional Secure Flight data requirements are not applicable for these phases. 2. If initially provided, DHS will use the full name, date of birth, gender, and acceptable travel document data to perform watch list matching. 3. At a minimum, the full name and date of birth will be used to perform watch list matching. 4. DHS will return a boarding pass printing result. The aircraft operator may use the boarding pass printing result for the domestic flight in lieu of the aircraft operator conducting the watch list matching. 5. Passport number and country of issuance will be required for ESTA vetting only if associated to an international arrival to the U.S. 6. As APIS data is received, an APIS manifest will be dynamically built for the international connecting flight. 7. For flights arriving into the United States, access to Passenger Name Record (PNR) data is required by CBP. 8. Aircraft operators must validate the data found in the Machine Readable Zone of a passenger’s government issued travel document, with data previously submitted. Validation can occur with the use of a document reader or through visual comparison of data. Phase III – CBP performs APIS functions, TSA performs watch list matching 1. No special handling is required, TSA will return a boarding pass printing result to the aircraft operator for flights meeting the “directional travel” criteria 2. Aircraft operators must transmit SFPD and APIS data to DHS for international travel bound for the United States. 3. Aircraft operators must transmit APIS data to DHS for international travel departing pre-

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

Table 8 Required Transmission Events

Event	Requirements
	clearance locations, bound for the United States. 4. SFPD data must be submitted to TSA approximately 72 hours prior to scheduled flight departure. 5. For reservations received within 72 hours of a scheduled flight, SFPD must be submitted at the time the reservation is received and processed. 6. For "inhibited" passengers whose personal information is verified at check-in thru the verified ID process described in section 5.3.3, SFPD must be submitted with an indication that personal information has been verified. Passport number and country of issuance will be required for ESTA vetting. 7. DHS will return a boarding pass printing result to the aircraft operator that includes results of watch list matching and ESTA vetting. 8. As APIS data is received, an APIS manifest will be dynamically built. 9. For flights arriving into the United States, access to PNR data is required by CBP. 10. Aircraft operators must validate the data found in the Machine Readable Zone of a passenger's government issued travel document, with data previously submitted. Validation can occur with the use of a document reader or through visual comparison of data.
U.S. overflights	Phase III – TSA performs watch list matching: 1. Aircraft operators must transmit SFPD for passengers on flights that overfly the United States. 2. Aircraft operators are required to transmit crew data for international flights, which fly over the United States. 3. DHS will receive all data required in published Emergency Amendments and Security Directives for flight crew manifests. 4. Any negative boarding pass printing results on operating crew members will be communicated to the aircraft operator by the TSA Crew Vetting Program. 5. An ESTA screening message indicating Travel Authorization via ESTA not applicable will be returned on passenger data on U.S. overflights.
Covered U.S. aircraft operators with flights between two non-U.S. locations	Phase III – TSA performs watch list matching: 1. Aircraft operators must transmit SFPD for flights between two non-U.S. locations operated by covered U.S. aircraft operators. 2. A boarding pass printing result will be returned to the aircraft operator. 3. An ESTA screening message indicating Travel Authorization via ESTA not applicable will be returned on passenger data for U.S.-owned aircrafts that are operating between foreign airports.
Flight Crew Manifest (FCM)	Phases I, II and III – TSA performs watch list matching: 1. DHS will receive the non crew member flight crew manifest information required for international crew members in advance of each scheduled flight's departure, where applicable. 2. Individuals on the international manifest will be watch list matched each time they fly. 3. The international flight crew manifest transmission for TSA crew watch list matching also satisfies CBP's requirements for international crew manifest submissions. 4. If incorrect or incomplete information is received, TSA will ask the aircraft operator for the correct information. 5. TSA will conduct the aviation security threat assessment. 6. Any individual who DHS determines poses or is suspected of posing a security threat will not be authorized to be a crew member or non crew member. DHS will share the information with the appropriate law enforcement and/or intelligence agencies, the aircraft operator making the submission for the crew member, and upon its request, the host government.

Table 8 Required Transmission Events

Event	Requirements
Gate pass (for Secure Flight Rule compliance only)	Phase I - Aircraft operators perform watch list matching: Aircraft operators perform watch list matching pursuant to applicable security directives and emergency amendments. Phases II and III – TSA performs watch list matching: 1. Aircraft operators that issue authorization to enter an U.S. airport sterile areas to non-travelers (e.g. gate pass) must submit SFPD to DHS. The authorization identifies the holder as having a legitimate reason to require access to the sterile area (subject to DHS screening procedures). 2. Aircraft operators must obtain a boarding pass printing result for the non-traveler. DHS will receive the full name, date of birth, and gender and will perform watch list matching. 3. DHS will return a boarding pass printing result to the aircraft operator.
Flight Close-out (for international legs only)	Phases I, II and III – CBP performs APIS function: 1. Aircraft operators will be required to electronically report the flight's departure. 2. The Flight Close-out Message communicates the following: a. Actual flight departure or date and time cancellation b. Number of passengers on board 3. Unique identification of passengers that did not board, but had APIS data previously submitted to DHS.

4.5 Message Business Rules

DHS Response Message

A DHS Response Message will be returned for each Passenger Data Message transmitted.

The DHS Response Message will communicate a boarding pass printing result for each passenger submitted in the message. The message will consist of a dual vetting response representing screening results for watch list and ESTA queries.

The DHS interactive message codes were developed in an effort to meet the statutory requirements of the 9/11 Act while minimizing the operational impact on both DHS and the airline industry by incorporating existing procedures and proposed modifications. Secure Flight and ESTA screening requires that two DHS entities, CBP and the TSA, be involved in the pre-departure screening process. It was determined that a message code consisting of two data characters would be most effective at communicating a dual vetting response. The two-character codes will assist aircraft operators in compliance with watch list and ESTA status verification processes:

Table 9 DHS Security Message Codes

DHS Security Vetting Message	Description
0	Cleared
1	Inhibited
2	Selectee
4	Error

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

Table 10 DHS ESTA Message Codes

DHS ESTA Status Message	Description
Z	Travel Authorization via ESTA not applicable
A	Visa Waiver Program (VWP) Participant Passport-Approved Travel Authorization via ESTA on file
B	VWP Participant Passport-No Application for Travel Authorization via ESTA on file
C	VWP Participant Passport-U.S. Travel Document required
1	Inhibited
X	Insufficient data to provide ESTA status

By utilizing two characters in the pre-departure responses, DHS will minimize confusion associated with the variety of operational scenarios aircraft operators are likely to encounter while ensuring the integrity of the ESTA program and the DHS vetting processes are not compromised. The dual character codes will also incorporate the flexibility required to allow carriers to use discretion when boarding individuals traveling with VWP-eligible country passports who are not seeking admission under the VWP.

Table 11 Operational Scenarios and Associated Messages

Operational Scenarios	CUSRES Message
Ok to Board	
	0Z – Cleared, Travel Authorization via ESTA not applicable
	2Z – Selectee, Travel Authorization via ESTA not applicable
	0A – Cleared, VWP Participant Passport-Approved Travel Authorization via ESTA on file
	2A – Selectee, VWP Participant Passport-Approved Travel Authorization via ESTA on file
OK to Board with Additional U.S. Travel Document	
	0B – Cleared, VWP Participant Passport-No Application for Travel Authorization via ESTA on file
	2B – Selectee, VWP Participant Passport-No Application for Travel Authorization via ESTA on file
	0C – Cleared, VWP Participant Passport-US Travel Document required
	2C – Selectee, VWP Participant Passport-US Travel Document required
Boarding Inhibited	
	11 – Inhibited
Boarding not Authorized Due to Insufficient Data to conduct ESTA Status Verification	
	0X – Cleared, Insufficient ESTA Data
	2X – Selectee, Insufficient ESTA Data

The DHS Response Message acknowledges receipt of the Passenger Data Message.

CBP▶ APIS

Aircraft operators are encouraged to “run” business rule edits based on the APIS

Validation UN/EDIFACT guidelines prior to submitting an APIS manifest. Aircraft operators are responsible for ensuring that any APIS data previously submitted is validated against the data presented by the passenger prior to gaining access to the aircraft. Data validation may be accomplished by scanning the Machine Readable Zone of an individual's travel document. If scanning a Machine Readable Zone is not possible, a visual comparison of the biographic section of the travel document with the data previously submitted will be necessary.

ESTA Validation Aircraft operators can provide a secondary document, when submitting data, to receive a more favorable ESTA status response. The following primary and secondary documents will be used in assessing the ESTA status response:

Acceptable Primary Documents and the expected ESTA status, any other document type sent as the primary document, other than noted below, will result in an ESTA status of 'X' being returned:

- Alien Registration Card
  - Issuing country is blank or 'USA': 'Z'
  - Issuing country is any other value: 'X'
- Permanent Resident Card
  - Issuing country is blank or 'USA': 'Z'
  - Issuing country is any other value: 'X'
- US Merchant Marine Document
  - Issuing country is blank or 'USA': 'Z'
  - Issuing country is any other value: 'X'
- Reentry Permit Refugee
  - Issuing country is blank or 'USA': 'Z'
  - Issuing country is any other value: 'X'
- Facilitation Document: 'Z'
- Nexus Card: 'Z'
- Military Document: 'Z'
- Visa: 'X'
- Passport: VWP participant = Query ESTA

Acceptable Secondary Documents for bypassing ESTA query (Assuming VWP Passport presented as the primary document). Any other secondary document types, other than noted below, will cause the software to query ESTA based on the primary document:

- Alien Registration Card, issuing country is blank or 'USA': 'Z'
- Permanent Resident Card, issuing country is blank or 'USA': 'Z'
- Nexus Card: 'Z'
- Military Document: 'Z'
- Visa, issuing country 'USA': 'Z'

***NOTE:** Aircraft Operators with flights into Guam will receive an ESTA status response based on the passenger's ESTA status for entry into the United States. This ESTA status has no bearing on the passenger's visa waiver status under the Guam Visa Waiver program.

No Transport

Aircraft operators may not transport a passenger for whom an Inhibited boarding pass printing result has been returned or when the aircraft operator has not yet received a boarding pass printing result from DHS. Under certain circumstances, passengers holding connecting international flight itineraries may be able to have a boarding pass issued without a boarding pass printing result; however, the passenger cannot gain access to the aircraft until a boarding pass printing result has been returned. The watch list will be continually evaluated and passengers' active travel itineraries will be continually matched against it. A unique ESTA verification message will not be returned in cases of inhibited boarding. In any case in which an Inhibited message is received, the aircraft operator is prohibited from transporting the passenger. An ESTA status message will be provided if the Inhibited boarding status is downgraded to Cleared or Selectee.

Unsolicited Messages

Unsolicited Messages contain updated boarding pass printing results that result from an update to a watch list. Unsolicited Messages will be sent to the aircraft operator when the watch list matching process alters a passenger's previous boarding pass printing result. In addition, Unsolicited Messages may be sent when a passenger's status is changed from Inhibited to Cleared or Selectee through the resolution process. In such cases, an ESTA status verification message will be sent with the security-related message provided the operator has provided the required data elements. Aircraft operators that receive an Unsolicited Message must update any previously returned boarding pass printing result and boarding guidance with the new result. Unsolicited Messages may be returned at any time during a traveler's active journey. A coordinated effort to manage the updates will be undertaken between DHS and the aircraft operator(s) involved in the passenger's journey.

DHS will develop new processes and enhance existing ones to deal with passengers whose boarding pass printing results change before completing their travel. These updates may decrease a status's security level (e.g., Inhibited to Selectee, Selectee to Cleared) or increase it (e.g., Cleared to Selectee, Cleared to Inhibited, Selectee to Inhibited). DHS will use Unsolicited Messages to communicate changes to the aircraft operator. These messages are called "unsolicited" because the aircraft operator will receive them without making any request to DHS past the initial passenger data transmission.

In the event that the passenger has already been issued a boarding pass and the Unsolicited Message changes the passenger's status to Inhibited (from Cleared or from Selectee) or to Selectee (from Cleared), DHS will send an Unsolicited Message, contact the aircraft operator's security office to coordinate the operational response, and provide additional guidance. If the boarding pass has not been issued, the aircraft operator should follow the Selectee and Inhibited responses outlined in this document.

In the event that the Unsolicited Message changes the passenger's status to Cleared (from Inhibited or from Selectee) or to Selectee (from Inhibited), the aircraft operator should follow the Cleared or Selectee responses outlined in this document.

Alliances

Aircraft operator alliances are recognized as an integral part of aviation commerce. Aircraft operators are encouraged to develop or enhance existing communications systems to allow for the exchange of APIS data and Cleared, Selectee, or Inhibited updated boarding pass printing results when passengers are booked on multiple aircraft operators.

Inhibited Response

Aircraft operators should follow the procedures below in the event that DHS returns an Inhibited response:

1. Within the response, aircraft operators will be provided instructions on their next steps. Aircraft operators will be provided a 24-hour contact number to assist in determining a resolution to Inhibited responses. Depending on the information needed, a Cleared response may be obtained. The aircraft operator must then make a final boarding determination based on the boarding pass printing results and ESTA response, unless otherwise specifically authorized by DHS.
2. Any passenger that receives an Inhibited response may not be boarded or transported until the Inhibited response has been resolved. ESTA status verification messages will not be provided when Inhibited boarding results are sent.
3. Aircraft operators must identify and remove or invalidate any boarding pass for any passenger where an Inhibited response has been received.
4. Aircraft operators must identify and remove or invalidate any boarding pass for any passenger identified as traveling under the VWP where a VWP Participant Passport-No application for Travel Authorization via ESTA on file or VWP Participant Passport-U.S. Travel Document required has been received and no additional U.S. travel document allowing travel has been identified.
5. Any checked baggage must be identified and removed from the aircraft if the response cannot be resolved.

Insufficient Data Procedures

The following procedures should be followed in the event that DHS returns an Error response:

- The aircraft operator must collect additional data from the passenger and resubmit an updated Passenger Data Message to DHS. Once DHS has received a valid message, DHS will respond with the passenger's boarding pass printing result.
- In all cases, any passenger that has received an Error Response may not be boarded or transported until the Error Response has been resolved.

CBP▶ Batch Close-out Transmission

Passengers may request a boarding pass and subsequently not travel. To clearly identify passengers that have boarded an aircraft, aircraft operators will be required to submit a batch flight close-out manifest. The batch flight close-out manifest represents a list of all passengers issued boarding passes. To accomplish this, aircraft operators will have the ability to submit a close-out message indicating passengers that did travel or a close-out message indicating passengers that did not travel. Aircraft operators will only need to provide one message for each flight.

DHS will build APIS flight manifests dynamically as APIS data is received. To ensure that traveling passengers are correctly identified in the DHS system, the flight close-out transmission will be used to reconcile passengers-transmitted to passengers-on-board.

The Flight Close-out Message will provide the flight's actual onboard count. The count may, in some cases, update passenger counts provided in previously filed General Declarations for flights departing the United States. It is common practice for aircraft operators to obtain an outbound clearance indicating projected passenger counts. The actual onboard passenger count provided in the close-out message will update the projected passenger count.

4.6 Data Submission Rules

The tables below define which data elements are required for passenger data submissions and which data elements, when not present or are invalid, will result in an Error Response Message. Additionally, the tables indicate if a data element is defined as qualified or informational for the Secure Flight program and the APIS Pre-Departure Final Rule.

Aircraft operators must submit any passenger data updates to DHS. Some data elements, called "qualified," require watch list matching the passenger again. Examples are first name, last name, and gender. In these cases, aircraft operators must discard the initial boarding pass printing result and apply the new one. These data elements are referred to as qualified data because they qualify the passenger to be watch list matched again. In the future, DHS is considering adding an additional value to the submission of qualified data which will indicate to DHS if a boarding pass has already been issued for the flight segment being resubmitted. This will permit DHS to initiate appropriate operational processes in those rare cases in which a qualified data submission results in an Inhibited result after a boarding pass has been issued.

DHS considers other data elements as informational only, such as aircraft operator code or flight number. DHS will not watch list match the passenger again; therefore, there is no need to discard the boarding pass printing result. These data elements are referred to as informational. If an aircraft operator submits an informational update, DHS will respond with an acknowledgement message.

Passenger cancellations and rebooking will also need to be reported to DHS. These cases include outright cancellation (no rebooking), cancel and rebook, cancellation of one or more members of a multi passenger booking (reduce number in party), and the rebooking of one or more individuals in a multi passenger booking (split PNR).

These data submissions rules are related to watch list matching requirements and do not change the established data requirements for APIS compliance.

Table 12 SFPD Submission Rules

Data Element	Secure Flight Required Field	Results in Error Response	Qualified or Informational	Results in New Boarding Pass Printing Result
Verified ID indicator	No	No	Qualified	Yes
Last name	Yes	Yes	Qualified	Yes
First name	Yes	Yes	Qualified	Yes
Middle name	No	No	Qualified	Yes
Date of birth*	Yes	No	Qualified	Yes
Gender*	Yes	No	Qualified	Yes
Travel document type ***	No	No	Qualified	Yes
Document number	No	No	Qualified	Yes
Document country of issuance	No	No	Qualified	Yes
Document expiration date ***	No	No	Qualified	Yes
Redress number	No	No	Qualified	Yes
Known Traveler number	No	No	Qualified	Yes
Passenger Name Record locator	Yes	Yes	Never changes**	
Passenger Reference Number	Yes	Yes	Never changes	
Aircraft operator code	Yes	Yes	Informational	No
Flight number	Yes	Yes	Informational	No
Flight itinerary: departure airport code	Yes	Yes	Informational	No
Scheduled date/time of aircraft departure	Yes	Yes	Informational	No
Flight itinerary: arrival airport code	Yes	Yes	Informational	No
Scheduled date/time of aircraft arrival	Yes	Yes	Informational	No

*Under the Secure Flight Final Rule, date of birth and gender are mandatory data elements. However, aircraft operators will submit the data elements as outlined in the AOIP.

** Generally, a Passenger Name Record locator remains unchanged for the life of a booking record (except from split or divided records which are covered elsewhere). In the unlikely event that a Passenger Name Record Locator changes, the aircraft operator may chose to generate a new submission or may elect to submit a qualified change.

*** The Travel Document Type and Document Expiration Date should be considered qualified changes as they are changes to the passenger's information resulting in the submission of a Change Passenger type message. Secure Flight only accepts a Document Type = Passport (P) for SFPD. Other document types required for APIS will not be passed to Secure Flight if provided by the carrier to meet APIS requirements.

Table 13 SFPD Gate Pass (Non-Traveler) Submission Rules

Data Element	Secure Flight Required Field	Results in Error Response	Qualified or Informational	Results in New Boarding Pass Printing Result
Verified ID indicator	No	No	Qualified	Yes
Last name	Yes	Yes	Qualified	Yes
First name	Yes	Yes	Qualified	Yes
Middle name	No	No	Qualified	Yes
Date of birth*	Yes	No	Qualified	Yes
Gender*	Yes	No	Qualified	Yes
Travel document type ***	No	No	Qualified	Yes
Document number	No	No	Qualified	Yes
Document country of issuance	No	No	Qualified	Yes
Document expiration date ***	No	No	Qualified	Yes
Redress number	No	No	Qualified	Yes
Known Traveler number	No	No	Qualified	Yes
Passenger Name Record locator	Yes	Yes	Never changes**	
Passenger Reference Number	Yes	Yes	Never changes	
Aircraft operator code	No	Yes	Qualified	Yes
Airport code	Yes	Yes	Qualified	Yes

*Under the Secure Flight Final Rule, date of birth and gender are mandatory data elements. However, aircraft operators will submit the data elements as outlined in the AOIP.
** Generally, a Passenger Name Record locator remains unchanged for the life of a booking record (except from split or divided records which are covered elsewhere). In the unlikely event that a Passenger Name Record Locator changes, the aircraft operator may choose to generate a new submission or may elect to submit a qualified change.

*** The Travel Document Type and Document Expiration Date should be considered qualified changes as they are changes to the passenger's information resulting in the submission of a Change Passenger type message. Secure Flight only accepts a Document Type = Passport (P) for SFPD. Other document types required for APIS will not be passed to Secure Flight if provided by the carrier to meet APIS requirements.

Table 14 SFPD Submission Rules for Passenger Updates

Update Type	Type of Change	Required Action
Qualified Change – Not Verified Data: Passenger(s) has change in one or more qualified data elements.	Qualified	Submit updated SFPD with message type of Change Passenger for each passenger with changed information.
Qualified Change – Verified Data: Documentation of qualified data elements for passenger is provided and verified at check-in.	Qualified	Submit updated SFPD with message type of Change Passenger for the verified passenger and designate the data as verified.
Cancellation of Reservation: Reservation for all passengers included in last SFPD is cancelled	Informational	Submit updated SFPD with message type of Cancel Reservation.
Reduction-in-Party: Number of passengers in initial SFPD is reduced (e.g., reduction-in-party, Split PNR)	Informational	Submit updated SFPD with message type of Reduction-in-Party that includes remaining passengers assigned to the original reservation record. (Note that new SFPD will be required for other passengers if/when new reservation(s) is created for them.)
Itinerary Change – Change is within 72-hours of scheduled flight departure (Domestic): Itinerary changes for passengers in a previously submitted SFPD to another flight that is scheduled to depart within 72-hours of the time of the scheduled departure of the original flight.	Informational	Submit updated SFPD with message type of Change Flight (or "Change Itinerary" if XML submission) with updated itinerary information.
Itinerary Change – NOT within 72-hours of scheduled flight departure (Domestic): Itinerary changes for passengers in a previously submitted SFPD to a flight with a scheduled departure time greater than 72-hours from the scheduled departure time of the original flight.	Informational	Submit updated SFPD with message type of Change Flight (or "Change Itinerary" if XML submission) with updated itinerary information.
Itinerary Change – International: Itinerary changes for passengers in a previously submitted SFPD to a different flight.	Qualified	Submit updated SFPD with message type of Change Passenger with updated itinerary information.

Table 14 SFPD Submission Rules for Passenger Updates

Update Type	Type of Change	Required Action
Qualified Change and Itinerary Change: A change in one or more qualified data elements for a passenger or passengers occurs at the same time as a change in itinerary,	Qualified And Informational	If itinerary change within the 72-hour data submission period: 1) Submit updated SFPD with message type of Change Passenger for each passenger with changed information. 2) Submit updated SFPD with message type of Change Flight (or "Change Itinerary" if XML submission) with updated itinerary information. OR For itinerary change outside data submission period:: Submit updated SFPD with message type of Cancel Reservation. (Note a new SFPD for the reservation will be required when date of flight is within the allowable data submission period.)
Qualified Change and Reduction-in-Party: A change in one or more qualified data elements for a passenger or passengers occurs at the same time as a reduction-in-party for a different passenger or passengers.	Informational And Qualified	1) Submit updated SFPD with message type of Reduction-in-Party that includes remaining passengers assigned to the original reservation record. 2) Submit updated SFPD with message type of Change Passenger for each passenger with changed information.
Cancelled Flight – Scenario 1: All passengers in SFPD rebooked on another flight with same aircraft operator on a flight that is within the 72-hour data submission period.	Informational	Submit updated SFPD with message type of Change Flight (or "Change Itinerary" if XML submission) with updated itinerary information.
Cancelled Flight – Scenario 2: All passengers in SFPD re-booked on another flight with same aircraft operator, but on a flight that is outside the required data submission period.	Informational	Submit updated SFPD with message type of Cancel Reservation. *(Note: new SFPD for the reservation will be required when date of flight is within the allowable data submission period.)*
Cancelled Flight – Scenario 3: Passengers re-booked on flight(s) of another aircraft operator or using other form of travel.	Informational	Submit updated SFPD with message type of Cancel Reservation.
Cancelled Flight – Scenario 4: -- Some passengers in SFPD re-booked with same aircraft operator on a flight that is within the 72-hour data submission period. -- Others re-booked on another flight or flights that are outside the required data submission period or with booked on flight(s) with another aircraft operator.	Informational	For passengers on flight that is within the data submission period, submit updated SFPD with message type of Reduction-in-Party that includes remaining passengers assigned to the original reservation record. *(Note: new SFPD will be required for other passengers new reservation(s) are created for them.)*

Table 15 APIS Data Submission Rules

Data Element	Flights Inbound to the United States		Flights Leaving the United States		Qualified or Informational	Results in New Boarding Pass Printing Result
	APIS Pre-Departure Required Field	Results in Error Response	APIS Pre-Departure Required Field	Results in Error Response		
Last name	Yes	Yes	Yes	Yes	Qualified	Yes
First name	Yes	Yes	Yes	Yes	Qualified	Yes
Middle name	No	No	No	No	Qualified	Yes
Date of birth	Yes	Yes	Yes	Yes	Qualified	Yes
Gender	Yes	No	Yes	No	Qualified	Yes
Citizenship	Yes	No	Yes	No	Qualified	Yes
Country of residence	Yes	No	No	No	Qualified	Yes
Status on board the aircraft	Yes	No	Yes	No	Qualified	Yes
Travel document type	Yes	No	Yes	No	Qualified	Yes
Document number	Yes	No	Yes	No	Qualified	Yes
Document country of issuance	Yes	No	Yes	No	Qualified	Yes
Document expiration date	Yes	No	Yes	No	Qualified	Yes
Address while in the United States	Yes	No	No	No	Qualified	Yes
Passenger Name Record Locator	No	Yes	No	Yes	Never changes	
Passenger Reference Number	Yes	Yes	Yes	Yes	Never changes	
Passenger itinerary: foreign airport where transportation began (embarkation)	Yes	No	Yes	No	Qualified	Yes
Passenger itinerary: airport of first arrival into U.S.	Yes	No	Yes	No	Qualified	Yes
Passenger itinerary: final airport of destination (debarkation)	Yes	No	Yes	No	Qualified	Yes
Aircraft operator code	Yes	Yes	Yes	Yes	Qualified	Yes
Flight number	Yes	Yes	Yes	Yes	Qualified	Yes
Flight itinerary: last foreign airport of call (departure airport code)	Yes	Yes	Yes	Yes	Qualified	Yes

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

Table 15 APIS Data Submission Rules

Data Element	Flights Inbound to the United States		Flights Leaving the United States		Qualified or Informational	Results in New Boarding Pass Printing Result
	APIS Pre-Departure Required Field	Results in Error Response	APIS Pre-Departure Required Field	Results in Error Response		
Scheduled date/time of aircraft departure	Yes	Yes	Yes	Yes	Qualified	Yes
Flight itinerary: airport of first arrival	Yes	Yes	Yes	Yes	Qualified	Yes
Scheduled date/time of aircraft arrival	Yes	Yes	Yes	Yes	Qualified	Yes

4.7 Message Types

Messages are transmitted between aircraft operators and DHS as shown in Table 16 and Table 17. Further technical detail of message layouts may be found in the appendices.

Table 16 Messages Transmitted from Aircraft Operator to DHS

Message Type ID	Message Type	Uses
PD	Passenger Data Message	Three primary requests: 1. Submit passenger data to request watch list and ESTA status message 2. Submit updates to previously submitted passenger data 3. Submit a watch list matching request for a person requesting access to a sterile concourse
FCO	Flight Close-out Message	Notification of flight departure and the identification of passengers that did or did not board the aircraft. Used for international travel only.
FCM	Flight Crew Manifest Message	A list of crew or certain non-crew passengers entering/leaving the U.S. or overflying U.S. territories. Used for international travel only.
Acknowledge Response	Acknowledge Unsolicited Message	Primary use is for the aircraft operator to acknowledge receipt of an Unsolicited Message.

Table 17 Messages Transmitted from DHS to Aircraft Operator

Message Type ID	Message Type	Uses
DRM	DHS Response Message	Communicate results of DHS watch list matching. Results include: 0Z – Cleared for security Screening and Travel Authorization via ESTA not applicable 2Z – Subject to Selectee Screening and Travel Authorization via ESTA not applicable 0A – Cleared for Security Screening and VWP Participant Passport-Approved Travel Authorization via ESTA on file 2A – Subject to Selectee Screening and VWP Participant Passport-Approved Travel Authorization via ESTA on file 0B – Cleared for Security Screening and VWP Participant Passport-No

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

Table 17 Messages Transmitted from DHS to Aircraft Operator

Message Type ID	Message Type	Uses
		application for Travel Authorization via ESTA on file 2B – Subject to Selectee Screening and VWP Participant Passport-No application for Travel Authorization via ESTA on file 0C – Cleared for Security Screening and VWP Participant Passport-US Travel Document required (ESTA was denied) 2C – Subject to Selectee Screening and VWP Participant Passport-US Travel Document required (ESTA was denied) 0X – Cleared for Security Screening, Data Insufficient to Obtain ESTA status 2X – Subject to Selectee Screening, Data Insufficient to Obtain ESTA status 11 – Inhibited DHS acknowledgement of receipt of a Flight Close-out Message, Cancel Flight Message, or Cancel Reservation message whereby no watch list lookup takes place DHS Unsolicited Message results include: • Boarding pass printing result is negative (Cleared) • Requires further assessment (Selectee) • Exceeds the high-risk threshold (Inhibited)

4.8 Message Timing

Transmission Options Aircraft operators can elect from two submission options: batch or interactive.

Initial Passenger Data The aircraft operator must send an initial Passenger Data Message for watch list matching to DHS for a flight at approximately 72 hours before scheduled departure for Secure Flight. For APIS Pre-Departure and ESTA, the aircraft operator must send an initial Passenger Data Message for watch list matching to DHS for a flight not earlier than 72 hours before scheduled departure. DHS recommends the use of batch submissions for this time-related event. The aircraft operator will receive batch response(s) from DHS. Batch submissions will be used to submit passenger data that is not time sensitive to the aircraft operator.

DHS Responses DHS will watch list match all passenger data transmitted from the aircraft operator to DHS via the message type submitted (i.e. PAXLST for all international itineraries and XML if submitted for a purely domestic itinerary). The initial message sent to DHS must contain minimal passenger personal information to perform watch list matching and should include passport information and country of issuance for ESTA status verification.

Boarding pass printing results will be transmitted from DHS to the aircraft operator as soon as the watch list matching is complete. DHS will process interactive, high-priority messages within 4 seconds of receiving a message, provided that the messages contain no more than 10 passenger records. The two-

***WARNING:* This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

character code contains no alpha character specific to ESTA status in the case of an Inhibited response, because the security-related message takes precedence and no ESTA verification query will take place. An ESTA status message will be provided if the Inhibited boarding status is downgraded to Cleared or Selectee. (Note: the 4-second timeframe pertains to the duration in which the message event exists within the DHS system.) For more information, see Appendix 7.6.3.

An aircraft operator that receives a Selectee Response Message as a boarding pass printing result for a passenger must print the Selectee indicator on the passenger's boarding pass. Boarding passes may not be printed for passengers with Inhibited boarding pass printing results. The receipt of an Error Response Message due to invalid data submission would prevent the boarding of the passenger.

DHS will return these boarding pass printing results:

Boarding Pass Issuance and Boarding Authorized

- **0Z** – Cleared for security Screening and Travel Authorization via ESTA not applicable
- **2Z** – Subject to Selectee Screening and Travel Authorization via ESTA not applicable
- **0A** – Cleared for Security Screening and VWP Participant Passport-Approved Travel Authorization via ESTA on file
- **2A** – Subject to Selectee Screening and VWP Participant Passport-Approved Travel Authorization via ESTA on file

Boarding Pass Issuance Authorized and Boarding Authorized with valid U.S. Government Issued Travel Document or upon obtaining a travel authorization via ESTA

- **0B** – Cleared for Security Screening and VWP Participant Passport-No application for Travel Authorization via ESTA on file
- **2B** – Subject to Selectee Screening and VWP Participant Passport-No application for Travel Authorization via ESTA on file
- **0C** – Cleared for Security Screening and VWP Participant Passport-US Travel Document required (ESTA was denied)
- **2C** – Subject to Selectee Screening and VWP Participant Passport-US Travel Document required (ESTA was denied)

Boarding Pass Issuance Authorized and Boarding not Authorized due to Insufficient Data to submit ESTA Query

- **0X** – Cleared for Security Screening, Data Insufficient to Obtain ESTA status
- **2X** – Subject to Selectee Screening, Data Insufficient to Obtain ESTA status

Boarding Pass Issuance Not Authorized

- **11** – Inhibited from Boarding

Passengers with Cleared boarding pass printing results remain subject to CAPPS Selectee determination.

4.8.1 Message Types and Program Compliance

Each of the message types described in Section 4.7 relate to program compliance as shown in Table 18.

Table 18 Message Types and Program Compliance

Program Compliance	Message Type ID			
	PD	FCO	FCM	DRM
Secure Flight Final Rule	X			X
APIS Pre-Departure Final Rule	X	X	X	X

4.8.2 Domestic Travel – Messages and Responses

SFPD The aircraft operators would submit passenger data records formatted in accordance to the business rules for SFPD in Section 2.1.

DHS Response Messages Similar to the requirements in the APIS final rule, DHS proposes to respond to SFPD in domestic travel with one of the following messages:

- 0Z – Cleared for Security Screening and Travel Authorization via ESTA not applicable
- 2Z – Subject to Selectee Screening and Travel Authorization via ESTA not applicable
- 11 – Inhibited
- 4Z – Error

4.8.2.1 Domestic Travel – Cleared for Security Screening and Travel Authorization via ESTA not applicable

Cleared Response A Cleared for Security Screening and Travel Authorization via ESTA not applicable Response Message will be returned when the Passenger Data Message passes the data element edit requirements and results in a negative watch list match. The Cleared for Security Screening and Travel Authorization via ESTA not applicable Response Message will be DHS’s acknowledgement for receipt of the Passenger Data Message. A Travel Authorization via ESTA not authorized Message will be included since ESTA requirements are not applicable to domestic travel.

Table 19 Cleared for Security Screening Travel Authorization via ESTA not applicable Response Message Data Element List

Data Element	Comments
Message type identifier	Document response
Aircraft operator code	
Flight number	
Flight itinerary: Departure airport code	

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

Table 19 Cleared for Security Screening Travel Authorization via ESTA not applicable Response Message Data Element List

Data Element	Comments
Scheduled date/time of aircraft departure	Should represent scheduled date and time of aircraft departure
Flight itinerary: arrival airport code	
Scheduled date/time of aircraft arrival	Scheduled local date and time of arrival
Passenger Name Record (PNR) Locator	Record locator
Passenger Reference Number	Unique passenger number
Response	0Z – Cleared for Security Screening and Travel Authorization via ESTA not applicable

4.8.2.2 Domestic Travel – Subject to Selectee Screening and Travel Authorization via ESTA not applicable

Selectee Response A Selectee Response Message will be returned when the Passenger Data Message passes the data element edit requirements and results in an apparent watch list match to a Selectee entry. The Selectee Response Message will be DHS's acknowledgement for receipt of the Passenger Data Message. A Travel Authorization via ESTA not applicable Message will be included since ESTA requirements are not applicable to domestic travel.

Table 20 Selectee Response Message Data Element List

Data Element	Comments
Message type identifier	Document response
Aircraft operator code	
Flight number	
Flight itinerary: departure airport code	
Scheduled date/time of aircraft departure	Should represent scheduled date and time of aircraft departure
Flight itinerary: arrival airport code	
Scheduled date/time of aircraft arrival	Scheduled local date and time of arrival
Passenger Name Record (PNR) Locator	Record locator
Passenger Reference Number	Unique passenger number
Response	2Z – Subject to Selectee Screening and Travel Authorization via ESTA not applicable

4.8.2.3 Domestic Travel – Inhibited Response

Inhibited Response An Inhibited Response Message will be returned when the Passenger Data Message passes the data element edit requirements and results in an apparent watch list match to a No Fly entry. The Inhibited Response Message will be DHS's acknowledgement for receipt of the Passenger Data Message. No unique ESTA status response will be included on an Inhibited message.

***WARNING:* This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

Table 21 Inhibited Response Message Data Element List

Data Element	Comments
Message type identifier	Document response
Aircraft operator code	
Flight number	
Flight itinerary: departure airport code	
Scheduled date/time of aircraft departure	Should represent scheduled date and time of aircraft departure
Flight itinerary: arrival airport code	
Scheduled date/time of aircraft arrival	Scheduled local date and time of arrival
Passenger Name Record (PNR) Locator	Record locator
Passenger Reference Number	Unique passenger number
Response	Printing of boarding pass is inhibited
Guidance message	11 – Call Secure Flight Service Center

4.8.2.4 Domestic Travel – Error Response

Error Response An Error Response Message will be returned when passenger data fails business rule edits. The aircraft operator will resubmit the Passenger Data Message when additional data is available to satisfy the business rule edits.

Table 22 Error Response Message Data Element List

Data Element	Comments
Message type identifier	Document response
Aircraft operator code	
Flight number	
Flight itinerary: departure airport code	
Scheduled date/time of aircraft departure	Should represent scheduled date and time of aircraft departure
Flight itinerary: arrival airport code	
Scheduled date/time of aircraft arrival	Scheduled local date and time of arrival
Passenger Name Record (PNR) Locator	Record locator
Passenger Reference Number	Unique passenger number
Response	4Z – Error – Insufficient Data

4.8.2.5 Domestic Travel – Unsolicited Message

Unsolicited Message If an Inhibited, or a Selectee, or Cleared Response Message, along with a Travel Authorization via ESTA not applicable Message, was sent as an Unsolicited Message from DHS, the aircraft operator must send an Acknowledgement Response Message. Should additional intervention be required, DHS will coordinate this with the aircraft operator's designated point of contact.

Table 23 Unsolicited Message – Aircraft Operator Response Data Element List

Data Element	Comments
Message type identifier	Acknowledge response
Aircraft operator code	
Flight number	
Flight itinerary: departure airport code	
Scheduled date/time of aircraft departure	Should represent scheduled date and time of aircraft departure
Flight itinerary: arrival airport code	
Scheduled date/time of aircraft arrival	Scheduled local date and time of arrival
Passenger Name Record (PNR) Locator	Record locator
Passenger Reference Number	Unique passenger number
Response	Includes status of Boarding Pass or Error if Unknown Passenger N - Boarding pass not issued Y - Boarding pass issued E - Error (Use if passenger reservation not found)

4.8.3 International Travel-Messages and Responses

4.8.3.1 Boarding not Authorized Due to Insufficient ESTA Data

Transmission of data that does not include the passport number and passport country of issuance will not be sufficient to obtain ESTA status verification. Watch list vetting can be obtained without passport number and country of issuance; however, until an acceptable ESTA status message is received, boarding is restricted.

Table 24 - Cleared or Selectee and Insufficient ESTA data

Data Element	Comments
Message type identifier	Document response
Aircraft operator code	
Flight number	
Flight itinerary: last foreign port/place of call (departure port code)	
Scheduled date/time of aircraft departure	Should represent scheduled date and time of aircraft departure
Flight itinerary: Port/place of first arrival	
Scheduled date/time of aircraft arrival	Scheduled local date and time of arrival
Passenger Name Record (PNR) Locator	Record locator

Table 24 - Cleared or Selectee and Insufficient ESTA data

Data Element	Comments
Passenger Reference Number	Unique passenger number
Passport Information	Not provided
Response	0X or 2X – Subject Cleared or subject to Selectee Screening and Insufficient ESTA Data

4.8.3.2 Boarding Pass and Boarding Authorized

0Z – Cleared for Security Screening and Travel Authorization via ESTA not applicable. This response will be returned when the Passenger Data Message passes the mandatory data element edit requirements, results in a negative watch list match, and the traveler is not a VWP national or has been determined not required to comply with ESTA. The Cleared for Security Screening and ESTA not applicable message is the DHS acknowledgement for receipt of the Passenger Data Message.

Table 25 - Cleared for Security and Travel Authorization via ESTA not applicable

Data Element	Comments
Message type identifier	Document response
Aircraft operator code	
Flight number	
Flight itinerary: last foreign port/place of call (departure port code)	
Scheduled date/time of aircraft departure	Should represent scheduled date and time of aircraft departure
Flight itinerary: Port/place of first arrival	
Scheduled date/time of aircraft arrival	Scheduled local date and time of arrival
Passenger Name Record (PNR) Locator	Record locator
Passenger Reference Number	Unique passenger number
Passport Information	Passport number and country of issuance
Response	0Z – Cleared for Security Screening and Travel Authorization via ESTA not applicable. Boarding and boarding pass issuance is authorized.

2Z – Subject to Selectee Screening and Travel Authorization via ESTA not applicable. This response will be returned when the Passenger Data Message passes the mandatory data element edit requirements, results in an apparent watch list match to a Selectee record, and the traveler is not a VWP national or has been determined not required to comply with ESTA. The Subject to Selectee Screening and ESTA not applicable message is the DHS acknowledgement for receipt of the Passenger Data Message.

Table 26 - Subject to Selectee Screening and Travel Authorization via ESTA not applicable

Data Element	Comments
Message type identifier	Document response
Aircraft operator code	

Table 26 - Subject to Selectee Screening and Travel Authorization via ESTA not applicable

Data Element	Comments
Flight number	
Flight itinerary: last foreign port/place of call (departure port code)	
Scheduled date/time of aircraft departure	Should represent scheduled date and time of aircraft departure
Flight itinerary: Port/place of first arrival	
Scheduled date/time of aircraft arrival	Scheduled local date and time of arrival
Passenger Name Record (PNR) Locator	Record locator
Passenger Reference Number	Unique passenger number
Passport Information	Passport number and country of issuance
Response	2Z – Subject to Selectee Screening and VWP Participant Passport-Travel Authorization via ESTA not applicable. Boarding and boarding pass issuance is authorized.

0A – Cleared for Security Screening and VWP Participant Passport-Approved Travel Authorization via ESTA on file. This response will be returned when the Passenger Data Message passes the mandatory data element edit requirements, results in a negative watch list match, and the traveler has an approved electronic travel authorization obtained via the ESTA. The Cleared for Security Screening and Approved ESTA on File Message is the DHS acknowledgement for receipt of the Passenger Data Message.

Table 27 - Cleared for Security Screening and VWP Participant Passport-Approved Travel Authorization via ESTA on File

Data Element	Comments
Message type identifier	Document response
Aircraft operator code	
Flight number	
Flight itinerary: last foreign port/place of call (departure port code)	
Scheduled date/time of aircraft departure	Should represent scheduled date and time of aircraft departure
Flight itinerary: Port/place of first arrival	
Scheduled date/time of aircraft arrival	Scheduled local date and time of arrival
Passenger Name Record (PNR) Locator	Record locator
Passenger Reference Number	Unique passenger number
Passport Information	Passport number and country of issuance
Response	0A – Cleared for Security Screening and VWP Participant Passport-Approved Travel Authorization via ESTA is on File. Boarding pass issuance and passenger boarding is authorized.

2A – Subject to Selectee Screening and VWP Participant Passport-Approved Travel Authorization via ESTA on File. This response will be returned when the Passenger Data Message passes the mandatory data element edit requirements, results in an apparent watch list match to a Selectee record, and the traveler has an approved electronic travel authorization obtained via the ESTA. The Subject to Selectee Screening and Approved ESTA on File Message is the DHS acknowledgement for receipt of the Passenger Data Message.

Table 28 - Subject to Selectee Screening and VWP Participant Passport-Approved Travel Authorization via ESTA on File

Data Element	Comments
Message type identifier	Document response
Aircraft operator code	
Flight number	
Flight itinerary: last foreign port/place of call (departure port code)	
Scheduled date/time of aircraft departure	Should represent scheduled date and time of aircraft departure
Flight itinerary: Port/place of first arrival	
Scheduled date/time of aircraft arrival	Scheduled local date and time of arrival
Passenger Name Record (PNR) Locator	Record locator
Passenger Reference Number	Unique passenger number
Passport Information	Passport number and country of issuance
Response	2A – Subject to Selectee Screening and an approved travel authorization via ESTA is on File. Boarding pass issuance and passenger boarding is authorized.

4.8.3.3 Boarding Authorized after Verification of additional U.S. Issued Travel Documents

VWP country nationals will be required to produce an additional valid U.S. Government issued travel document or obtain travel authorization via ESTA prior to receiving authorization to board. Aircraft operators will be required to resubmit a boarding pass authorization when a traveler completes an ESTA enrollment after receiving a boarding pass authorization indicating No ESTA Application on File.

0B – Cleared for Security Screening and VWP Participant Passport-No application for Travel Authorization via ESTA on File. This response will be returned when the Passenger Data Message passes the mandatory data element edit requirements, results in a negative watch list match, but the subject is a VWP country national with no ESTA application on file. The Cleared for Security Screening and VWP Participant but No ESTA Application on File Message is the DHS acknowledgement for receipt of the Passenger Data Message.

Table 29 - Cleared for Security Screening and VWP Participant Passport-No application for Travel Authorization via ESTA on File

Data Element	Comments
Message type identifier	Document response
Aircraft operator code	
Flight number	
Flight itinerary: last foreign port/place of call (departure port code)	
Scheduled date/time of aircraft departure	Should represent scheduled date and time of aircraft departure
Flight itinerary: Port/place of first arrival	
Scheduled date/time of aircraft arrival	Scheduled local date and time of arrival
Passenger Name Record (PNR) Locator	Record locator

Table 29 - Cleared for Security Screening and VWP Participant Passport-No application for Travel Authorization via ESTA on File

Data Element	Comments
Passenger Reference Number	Unique passenger number
Passport Information	Passport number and country of issuance
Response	0B – Cleared for Security Screening and subject has a VWP Participant Passport-No application for Travel Authorization via ESTA on File. Boarding is authorized if the traveler presents an additional valid U.S. Government issued travel document or obtains travel authorization via ESTA.

2B – Subject to Selectee Screening and VWP Participant Passport-No application for Travel Authorization via ESTA on File. This response will be returned when the Passenger Data Message passes the mandatory data element edit requirements, results in an apparent watch list match to a Selectee record, and the subject is a VWP country national for which there is no ESTA application on file. The Subject to Selectee Screening and No ESTA Application on File Message is the DHS acknowledgement for receipt of the Passenger Data Message.

Table 30 - Subject to Selectee Screening and VWP Participant Passport-No application for Travel Authorization via ESTA on File

Data Element	Comments
Message type identifier	Document response
Aircraft operator code	
Flight number	
Flight itinerary: last foreign port/place of call (departure port code)	
Scheduled date/time of aircraft departure	Should represent scheduled date and time of aircraft departure
Flight itinerary: Port/place of first arrival	
Scheduled date/time of aircraft arrival	Scheduled local date and time of arrival
Passenger Name Record (PNR) Locator	Record locator
Passenger Reference Number	Unique passenger number
Passport Information	Passport number and country of issuance
Response	2B – Subject to Selectee Screening and subject has a VWP Participant Passport-No application for Travel Authorization via ESTA on File. Boarding is authorized if the traveler presents an additional U.S. Government issued travel document or obtains travel authorization via ESTA.

0C – Cleared for Security Screening and VWP Participant Passport-US Travel Document Required. This response will be returned when the Passenger Data Message passes the mandatory data element edit requirements, results in a negative watch list match, but the subject is a VWP country national who applied for an ESTA and was denied. The Cleared for Security Screening and VWP Participant but Visa or other accepted U.S. travel document required (ESTA was denied) message is the DHS acknowledgement for receipt of the Passenger Data Message.

Table 31 - Cleared for Security Screening and VWP Participant Passport-US Travel Document Required

Data Element	Comments
Message type identifier	Document response
Aircraft operator code	
Flight number	
Flight itinerary: last foreign port/place of call (departure port code)	
Scheduled date/time of aircraft departure	Should represent scheduled date and time of aircraft departure
Flight itinerary: Port/place of first arrival	
Scheduled date/time of aircraft arrival	Scheduled local date and time of arrival
Passenger Name Record (PNR) Locator	Record locator
Passenger Reference Number	Unique passenger number
Passport Information	Passport number and country of issuance
Response	0C – Cleared for Security Screening and VWP Participant Passport-US Travel Document Required. Subject is a VWP national and requires a U.S. travel document. Boarding is authorized only if the traveler presents an additional U.S. Government issued travel document.

2C – Subject to Selectee Screening and VWP Participant Passport-US Travel Document Required. This response will be returned when the Passenger Data Message passes the mandatory data element edit requirements, results in an apparent watch list match to a Selectee record, and the subject is a VWP country national who applied for an ESTA and was denied. The Subject to Selectee Screening and Visa or other U.S. accepted travel document required (ESTA was denied) message is the DHS acknowledgement for receipt of the Passenger Data Message.

Table 32 - Subject to Selectee Screening and VWP Participant Passport-US Travel Document Required

Data Element	Comments
Message type identifier	Document response
Aircraft operator code	
Flight number	
Flight itinerary: last foreign port/place of call (departure port code)	
Scheduled date/time of aircraft departure	Should represent scheduled date and time of aircraft departure
Flight itinerary: Port/place of first arrival	
Scheduled date/time of aircraft arrival	Scheduled local date and time of arrival
Passenger Name Record (PNR) Locator	Record locator
Passenger Reference Number	Unique passenger number
Passport Information	Passport number and country of issuance
Response	2C – Subject to Selectee Screening and VWP Participant Passport-US Travel Document Required. Boarding is authorized only if the traveler presents an additional U.S. Government issued travel document.

4.8.3.4 Boarding and Boarding Pass Issuance Not Authorized

11 – Inhibited from Boarding. This response will be returned when the Passenger Data Message passes the mandatory data element edit requirements and results in an apparent watch list match to a No Fly entry. DHS will not provide an ESTA status verification in the case of an Inhibited boarding. The Inhibited from Boarding Message is the DHS acknowledgement for receipt of the Passenger Data Message.

Table 33 - Inhibited from Boarding

Data Element	Comments
Message type identifier	Document response
Aircraft operator code	
Flight number	
Flight itinerary: last foreign port/place of call (departure port code)	
Scheduled date/time of aircraft departure	Should represent scheduled date and time of aircraft departure
Flight itinerary: Port/place of first arrival	
Scheduled date/time of aircraft arrival	Scheduled local date and time of arrival
Passenger Name Record (PNR) Locator	Record locator
Passenger Reference Number	Unique passenger number
Passport Information	Passport number and country of issuance
Response	11 – Inhibited. Boarding pass issuance and boarding is not authorized.

4.8.3.5 International Travel – Error Response

Error Response An Error Response Message will be returned when passenger data fails business rule edits for watch list matching or ESTA status verification. The aircraft operator should resubmit the Passenger Data Message when additional data is available to satisfy the business rule edits.

Table 34 Error Response Message Data Element List

Data Element	Comments
Message type identifier	Document response
Aircraft operator code	
Flight number	
Flight itinerary: last foreign port/place of call (departure port code)	
Scheduled date/time of aircraft departure	Should represent scheduled date and time of aircraft departure
Flight itinerary: port/place of first arrival	
Scheduled date/time of aircraft arrival	Scheduled local date and time of arrival
Passenger Name Record (PNR) Locator	Record locator
Passenger Reference Number	Unique passenger number

Table 34 Error Response Message Data Element List

Data Element	Comments
Response	4X (inbound) or 4Z (outbound) – Error. Insufficient data.

4.8.3.6 International Travel – Unsolicited Message

DHS Message If any of the above messages was sent as an Unsolicited Message from DHS, an Acknowledgement Response Message will be required from the aircraft operator. The aircraft operator acknowledgement of the Unsolicited Message must indicate if a boarding pass has been issued. This will aid in determining next steps in handling of the passenger. Should additional intervention be required, DHS will coordinate this with the aircraft operator's designated point of contact.

Table 35 Unsolicited Message – Aircraft Operator Response Data Element List

Data Element	Comments
Message type identifier	Acknowledge Response
Aircraft operator code	
Flight number	
Flight itinerary: last foreign port/place of call (departure port code)	
Scheduled date/time of aircraft departure	Should represent scheduled date and time of aircraft departure
Flight itinerary: port/place of first arrival	
Scheduled date/time of aircraft arrival	Scheduled local date and time of arrival
Passenger Name Record (PNR) Locator	Record locator
Passenger Reference Number	Unique passenger number
Response	Includes status of Boarding Pass or Error if Unknown Passenger N - Boarding pass not issued Y - Boarding pass issued E - Error (Use if passenger reservation not found)

4.8.4 Flight Close-out Message (International Travel)

CBP▶ The following table identifies the data elements required in a Flight Close-out Message. The Flight Close-out Message can be coded to indicate the passengers who boarded the aircraft or the passengers who did not board the aircraft. Detailed examples of the Flight Close-out Message are provided in the UN/EDIFACT Guide.

Table 36 Flight Close-out Message

Data Element	Comments
Message type identifier	Passengers on board Passenger not on board Flight cancellation
Aircraft operator code	

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

Table 36 Flight Close-out Message

Data Element	Comments
Flight number	
Flight itinerary: last foreign port/place of call (departure port code)	
Actual date/time of aircraft departure	Should represent actual time of aircraft departure
Flight itinerary: port/place of first arrival	
Estimated date/time of aircraft arrival	Estimated local time of arrival
Total number of passengers	Total number of passengers on board the aircraft
PNR Locator	Aircraft operator will either provide a list of all unique identifiers for passengers that boarded the aircraft or provide a list of all unique identifiers for passengers that did not board. Aircraft operators cannot mix lists of boarded and not boarded passengers in the same Flight Close-out Message. Based on aircraft operator submission, a unique identifier may be PNR locator and Passenger Reference Number combined. When submitting a flight cancellation, unique identifier reference is not necessary.
Passenger Reference Number	Unique passenger number

4.8.5 Flight Crew Manifest Message (International Travel)

CBP▸ The data elements for a flight crew manifest submission have not changed for this process. Data elements to submit must match what has been previously submitted for an aircraft operator's flight crew manifest or master crew list.

Table 37 Flight Crew Manifest Message

Data Element	Comments
Last name	Complete last name, as it appears on the master crew list
First name	Complete first name, as it appears on the master crew list
Middle name	If available, complete middle name, as it appears on the master crew list
Date of birth	Complete date of birth, as it appears on the master crew list
Gender	M or F
Citizenship	As it appears on the master crew list
Country of residence	As it appears on the master crew list
Status on board the aircraft	As it appears on the master crew list
Travel document type	As it appears on the master crew list
Document number	As it appears on the master crew list
Document country of issuance	As it appears on the master crew list
Document expiration date	As it appears on the master crew list
Permanent address	As it appears on the master crew list
Crew member itinerary: foreign airport where transportation began (embarkation)	Generally based on itinerary of the aircraft
Crew member itinerary: airport of first arrival into U.S.	Generally based on itinerary of the aircraft

Crew member itinerary: final airport of destination (debarkation)	Generally based on itinerary of the aircraft
Aircraft operator code	IATA/ICAO carrier code
Flight number	Aircraft operator-identified flight number
Flight itinerary: last foreign airport of call (departure airport code)	Generally based on itinerary of the aircraft
Scheduled date/time of aircraft departure	Based on local date and time of departure airport
Flight itinerary: airport of first arrival	Generally based on itinerary of the aircraft
Scheduled date/time of aircraft arrival	Based on local date and time of arrival airport

4.9 Message Formatting

DHS Message Syntax

The United Nations Economic Commission adopted a standard data format known as UN/EDIFACT – United Nations/Electronic Data Interchange for Administration, Commerce, and Trade – for Europe (UNECE). A version of the UN/EDIFACT PAXLST and CUSRES message set has been codified by the World Customs Organization (WCO) and the International Air Transportation Association (IATA) for worldwide use by all scheduled aircraft operators and border control authorities. Additional PAXLST and CUSRES message segments, data elements, and code values have been defined by DHS as necessary to meet the requirements set forth in DHS and TSA regulations and Security Directives and Emergency Amendments.

These UN/EDIFACT PAXLST and CUSRES message sets shall be used for batch and interactive submissions to DHS. This document is based on the WCO/IATA/ICAO standards and contains guidelines for aircraft operators to follow in the preparation and transmission (batch or interactive) of the passenger/crew manifest data for processing by DHS.

In order to implement new requirements of the UN/EDIFACT PAXLST and CUSRES message sets, DHS has made changes to the existing PAXLST and CUSRES definitions. This document is based on the WCO/IATA/ICAO Advance Passenger Information Guidelines and contains guidelines for aircraft operators to follow in the preparation and transmission of the passenger/crew manifest data for processing by DHS.

Message Formats

DHS supports two electronic message formats, XML and UN/EDIFACT, for the exchange of passenger and crew data.

UN/EDIFACT

The PAXLST and CUSRES UN/EDIFACT message sets support all DHS program requirements. Aircraft operators covered under the APIS Pre-Departure Final Rule are required to provide their data in UN/EDIFACT format.

XML

In addition to the UN/EDIFACT message set, DHS will support XML for electronic message interchange for purely domestic passenger itineraries. The XML message set can be found in Appendix 7.5.

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

Table 38 UN/EDIFACT Messages Sets and DHS Message Types

UN/EDIFACT Message Set	Message Type Supported
PAXLST (for both batch and interactive queries)	Passenger Data Non-traveler (Gate Pass) Data Flight Close-out Master Crew List Flight Crew Manifest
CUSRES (for both batch and interactive queries)	Cleared Response Selectee Response Error Insufficient Data Response Inhibited Response Unsolicited Message Acknowledge Unsolicited Response Acknowledge Flight Close-out

4.10 Secure Flight Network/Message Connectivity

All of the technical sections up to this point have assumed that the aircraft operators have the telecommunication infrastructure necessary to provide transactional messages to and from DHS using the DHS Router. Aircraft operators who have existing connectivity to the DHS Router must review their existing connectivity to ensure it has the capability to support the additional messages required for Secure Flight. Aircraft operators who are not connected to the DHS Router but have the system capability to send transactional messages will need to review options for connectivity to the DHS Router with CBP.

4.11 Alternative Transmission Method

For aircraft operators who do not have the telecommunications infrastructure necessary to support connectivity through the DHS router, DHS has developed an alternative data transmission mechanism. This alternative method of data transmission, eSecure Flight, supports internet-enabled manual submission or electronic upload of data for passengers and non travelers (gate pass requestors) to Secure Flight. It also enables controlled login and access to passenger matching results via the internet. Further details on eSecure Flight will be provided in a separate document to those covered aircraft operators that request it.

4.12 Alternative SFPD Submission Method

Foreign air carriers that are unable to meet the 72-hour Secure Flight submission requirement utilizing the UN/EDIFACT formatted message may choose to use an alternative submission method through the PNR Pull/Push connection currently supported by CBP. The Department of Homeland Security (DHS) supports this alternative method for foreign air carriers to facilitate compliance with the Secure Flight 72-hour requirement. Foreign air carriers should understand that this alternative method for SFPD submission is an interim accommodation for foreign air carriers that currently cannot comply with normal SFPD submission (as outlined in the Secure Flight Final Rule). This interim method will expire in April 2011. In order to use this alternative procedure, the foreign air carrier must fulfill the following requirements:

1. In addition to the current PNR Pull/Push submission data requirements, all covered foreign air carriers are required to have the SFPD elements for all ticketed passengers in the foreign air carrier's reservation system at 72 hours prior to scheduled flight departure.

2. Foreign air carriers must provide the data elements listed in Table 5 – Secure Flight Passenger Data Elements to TSA under this alternative method. The submitted data elements must include *Passenger Reference Number, Record Locator, and Aircraft Operator code.*

3. DHS will use the existing PNR Pull/Push connection to meet the Secure Flight 72-hour submission requirement. This submission does not supersede the currently established 72-hour PNR Pull/Push requirement with CBP or any subsequent submissions (i.e., 24-hours, 8-hours, wheels up). DHS **will NOT** provide a DHS Response Message (DRM) for passengers whose data is included in the 72-hour submission. SFPD elements included in the submission process must be in a prescribed format as detailed in Section 4.12.2.2.

4. All of the SFPD elements must be transferred to the Departure Control System (DCS) from the Reservation system including the *Passenger Reference Number, Record Locator, and Aircraft Operator code.* For all ticketed passengers, the foreign air carrier is required to submit data to DHS as SFPD as soon as the DCS is initialized. This submission must occur no later than 24 hours prior to scheduled flight departure. DHS will then respond with a DRM to DCS for this submission.

5. For any ticketed passenger whose data was collected prior to the assumption of SFPD submission by the DCS, the *Passenger Reference Number, Record Locator, and Aircraft Operator code* associated to each passenger must be passed from the reservation system to the departure control system. **The same *Passenger Reference Number, Record Locator, and Aircraft Operator code* that passes from the reservation system to the departure control system must also be included in the SFPD that is submitted from the DCS to DHS.** These values will be used to match the passenger data received from the reservation system to the passenger data received from the DCS.

Once passenger data is resident in the DCS, it is the responsibility of the foreign air carrier to meet all message submission requirements described in Table 7 – Passenger Data Required Transmission Timing, Table 8 – Required Transmission Events and Table 14 – SFPD Submission Rules for Passenger Updates.

4.12.1 Deployment

Foreign air carriers requesting to use this alternative procedure must notify Secure Flight through the Secure Flight mailbox at SecureFlight@dhs.gov. DHS will work with the foreign air carrier and their technical teams to ensure the proper processes are implemented.

After the alternative SFPD submission method has been implemented, if a foreign air carrier plans to alter its method of PNR transmission (address, URL, data format, etc.) the foreign air carrier must notify Secure Flight through the Secure Flight mailbox at SecureFlight@dhs.gov. The notification must occur no later than 90 days in advance of the scheduled change. Additionally, the foreign air carrier must identify an individual who will be the Secure Flight Project Manager to implement the change and provide contact information for that individual (full name, email, office number, etc.). The foreign air carrier's IIR should also be included on any communications with Secure Flight.

4.12.2 Technical Guidance

The purpose of this section is to provide guidelines to foreign air carriers for the preparation and transfer of passenger data using the alternative SFPD submission method. These implementation guidelines identify the DHS technical requirements for collecting passenger data from foreign air carriers.

4.12.2.1 Secure Flight Passenger Data Elements

Table 39 SFPD Elements below outlines the Secure Flight data elements sent by the foreign air carrier as part of the alternative SFPD submission method through the PNR Pull/Push connection currently supported by CBP. The data element labels associated with the data elements are identified (if necessary), along with any length constraints.

Table 39 SFPD Elements

Data Element	Data Element Label	Data Type	Length	Edits/Rules
Last name	lastname	A	35	Alphabetic, no numeric or special characters, except dash (-) and single quote (‘).
First name	firstname	A	35	A single character name is allowed, however, **may** result in a higher occurrence of “Inhibited” responses. Alphabetic, no numeric or special characters, except dash (-) and single quote (‘).
Middle name	middlename	A	35	Alphabetic, no numeric or special characters, except dash (-) and single quote (‘).
Date of birth	dob	AN	7	Valid day within a month, valid month, and valid year Date of Birth. Format ‘DDMonYY' where: DD - Day Mon - Month

***WARNING:* This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

Data Element	Data Element Label	Data Type	Length	Edits/Rules
				YY - Year
Gender	gender	A	1	M or F
Redress number	redressNumber	AN	13	Unique number assigned to passenger by DHS to promote resolution with previous watch list alerts.
Known Traveler number	travelerNumber	AN	25	Assigned passenger number as known to DHS to facilitate passenger clearance.
Document Type	documentType	AN	2	Codified value: P - Passport
Document number	documentNumber	AN	35	Alphanumeric, no special characters
Document Country of issuance	documentCountry	AN	3	Validated against the ISO country code list (ISO 3166)
Document expiration date	documentExpirationDate	AN	7	Date formatted as ' DDMonYY' where: DD - Day Mon - Month YY – Year
Record Locator	N/A (currently provided in the PNR and does not need to be provided in the prescribed formats)	AN	6	A PNR/Unique Identifier must be provided.
Passenger Reference Number	PassengerReferenceNumber	AN	25	To uniquely identify a passenger within a passenger name record locator. For a single passenger PNR, a default value may be assigned by the carrier.
Aircraft operator code	N/A (currently provided in the PNR and does not need to be provided in the prescribed formats)	AN	3	Validated against the IATA/ICAO aircraft operator code list. Aircraft operator Code either AN2 or AN3.
Flight number	N/A (currently provided in the PNR and does not need to be provided in the prescribed formats)	AN	8	Flight Information. Up to eight (8) characters of data may be transmitted. Formatted as aircraft operator code and Flight Number: - Aircraft operator code is in either AN2 or AN3 - Flight number up to 4 digits (numeric).
Flight itinerary: departure airport	N/A (currently provided in the PNR and does not need to be provided in the prescribed formats)	AN	3	Validated against the IATA airport code list. Flights departing and/or arriving into United States are identified by the airport codes provided. A departure or arrival is identified based on the “Location Function Code Qualifier.”
Scheduled date/time of aircraft departure	N/A (currently provided in the PNR and does not need to be provided in the	AN	10	Format: YY - Year MM - Month

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

Data Element	Data Element Label	Data Type	Length	Edits/Rules
	prescribed formats)			DD – Day hh - 24 Hour mm- Minutes Local time
Arrival airport	N/A (currently provided in the PNR and does not need to be provided in the prescribed formats)	AN	3	Validated against the IATA airport code list. Flights departing and/or arriving into United States are identified by the airport codes provided. A departure or arrival is identified based on the "Location Function Code Qualifier."
Scheduled date/time of aircraft arrival	N/A (currently provided in the PNR and does not need to be provided in the prescribed formats)	AN	10	Format: YY - Year MM - Month DD – Day hh - 24 Hour mm- Minutes Local time

4.12.2.2 PNR Pull/Push Message Formats

Foreign air carriers requesting this option may choose to use the International Air Transport Association (IATA) AIRIMP 33rd Edition format of the Special Service Request (SSR) DOCS and DOCO elements to accommodate the transmission of Secure Flight Passenger Data. If a foreign air carrier chooses this option they need to be aware that the submission of the Passenger Reference Number is not accommodated in this format. In order to meet the requirement of providing the Passenger Reference Number, foreign air carriers must designate the location of the Passenger Reference Number in the PNR, or provide this data element utilizing one of the formats described in 4.12.2.2.1 - 4.12.2.2.3 below with leading data element delimiters (/ or ,) for other required data elements.

The following message formats contained in this manual are solely the creation of DHS. DHS will maintain the message formats and manage any necessary updates. The following sections provide examples of the message formats that may be used.

4.12.2.2.1 OSI Format

The sample below illustrates how the required SFPD elements must be incorporated in the message format. This sample does not include all data elements currently being provided in the 72-Hour PNR submission.

```
<lineNumber> OSI SFA
<lastname>/<firstname>/<middlename>/<dob>/<gender>/<redressNumber>/<travelerNumber>/<documentType>/<documentNumber>/<documentCountry>
<lineNumber> OSI SFB <documentExpirationDate>/<passengerReferenceNumber>

1 OSI SFA ROGERS/GINGER/LYNN/15JAN54/F/12345/98765/P/444444444/US
2 OSI SFB 01JAN12/1.1
3 OSI SFA ASTAIRE/FRED//11MAY52/M/5262627/87847877/P/444444123/US
4 OSI SFB 21FEB13/2.2
```

4.12.2.2.2 Amadeus Style Format (within RM section)

The sample below illustrates how the required SFPD elements must be incorporated in the message format. This sample does not include all data elements currently being provided in the 72-Hour PNR submission.

```
<lineNumber> RM SFA
<lastname>/<firstname>/<middlename>/<dob>/<gender>/<redressNumber>/<travelerNumber>/<documentType>/<documentNumber>/<documentCountry>
<lineNumber> RM SFB <documentExpirationDate>/<passengerReferenceNumber>

1 RM SFA ROGERS/GINGER/LYNN/15JAN54/F/12345/98765/P/444444444/US
2 RM SFB 01JAN12/1.1
```

```
3 RM SFA ASTAIRE/FRED//11MAY52/M/5262627/87847877/P/444444123/US
4 RM SFB 21FEB13/2.2
```

4.12.2.2.3 Comma Separated Format

The sample below illustrates how the required SFPD elements must be incorporated in the message format. This sample does not include all data elements currently being provided in the 72-Hour PNR submission.

```
SFPD-DATA
<lastname>,<firstname>,<middlename>,<dob>,<gender>,<redressNumber>,<travelerNumber>,<documentType>,<documentNumber>,<documentCountry>,<documentExpirationDate>,<passengerReferenceNumber>
```

```
SFPD-DATA ROGERS,GINGER,LYNN,15JAN54,F,12345,98765,P,444444444,US,01JAN12,1.1
SFPD-DATA ASTAIRE,FRED,11MAY52,M,5262627,87847877,P,444444123,US,21FEB13,2.2
```

4.12.2.2.4 XML Style Format

The sample below illustrates how the required SFPD elements must be incorporated in the message format. This sample does not include all data elements currently being provided in the 72-Hour PNR submission.

```
<sfpd>
  <lastname/>
  <firstname/>
  <middlename/>
  <dob/>
  <gender/>
  <redressNumber/>
  <travelerNumber/>
  <documentType/>
  <documentNumber/>
  <documentCountry/>
  <documentExpirationDate/>
  <passengerReferenceNumber/>
</sfpd>
```

```
<sfpd>
  <lastname>ROGERS</lastname>
  <firstname>GINGER</firstname>
  <middlename>LYNN</middlename>
  <dob>15JAN54</dob>
  <gender>F</gender>
  <redressNumber>12345</redressNumber>
  <travelerNumber>98765</travelerNumber>
  <documentType>P</documentType>
```

```
<documentNumber>4444444444</documentNumber>
<documentCountry>US</documentCountry>
<documentExpirationDate>01JAN12</documentExpirationDate>
```

4.13 72 Hour Continuous Submission Alternative

To assist the airline industry in meeting compliance with the Secure Flight program in a timely manner, DHS has approved an alternative to the full, interactive SFPD submission process. This permanent alternative is the 72 Hour Continuous Submission alternative. In order to use this alternative, foreign air carriers must fulfill the following requirements:

> The foreign air carrier must submit SFPD to DHS beginning at 72 hours prior to scheduled flight departure as UN/EDIFACT. The initial SFPD submissions will be of message type new with any subsequent changed SFPD submissions following the qualified and informational message guidance as described in the UN/EDIFACT Implementation Guide. Foreign air carriers will continuously submit new and changed (qualified and informational messages) SFPD after the initial 72 hour submission promptly after a reservation is made or changed up through flight departure.

1. DHS will provide a DHS Response Message (DRM) to the submitted SFPD requests. The foreign air carriers are not required to store or acknowledge the DRMs for the SFPD between the 72-hour initial submission and the time that the DCS is initialized.

2. Once the DCS is initialized (and not later than 24 hours prior to flight departure), the foreign air carrier must re-submit all SFPD with the message type of change passenger and continue to submit new and changed (qualified or informational) SFPD as UN/EDIFACT. DHS will provide a DRM for the SFPD submitted from the DCS. The foreign air carriers will receive the DRMs and must store and apply the boarding pass printing result as instructed by the DRM.

Once the DCS is initialized for a flight (and not later than 24 hours prior to flight departure), it is the responsibility of the foreign air carrier to meet all message submission requirements described in Table 7 – Passenger Data Required Transmission Timing, Table 8 – Required Transmission Events and Table 14 – SFPD Submission Rules for Passenger Updates.

Foreign air carriers requesting the use of this permanent alternative must advise their assigned International Industry Representative (IIR) and Airline Implementation Manager (AIM) prior to the inception of operational testing.

5 OPERATIONS GUIDE

The operations guide portion of the Consolidated User Guide describes ongoing, post-implementation procedures and processes for aircraft operators to follow in complying with the applicable regulations in the APIS Pre-Departure Final Rule, the Secure Flight Final Rule, and the ESTA Interim Final Rule. It describes operating scenarios and events, redress, problem resolution, issues management, change management, and account management.

Fundamental Compliance

In compliance with the applicable regulations, the aircraft operator will transmit to CBP 100 percent of the required passenger data for confirmed, cancelled (if cancelled after initial submission), or standby for international travel on all commercial flights arriving in or departing from the United States. TSA has a similar compliance standard for domestic and international covered flights in the Secure Flight rule. This submission does not modify or supersede the aircraft operators' required evaluation and handling of CAPPS Selectees.

5.1 Privacy Notice

TSA▸ TSA requires aircraft operators and aircraft operator-owned reservations outlets to make a privacy notice available to passengers prior to collecting information for the Secure Flight program under certain circumstances. Aircraft operators must provide the following privacy notice on its Website or self-serve kiosk prior to collecting a passenger's passenger information.
Aircraft operators must also ensure that third party websites for reservations for their flights also provide the following privacy notice prior to collecting passenger information.

> "The Transportation Security Administration (TSA) requires you to provide your full name, date of birth, and gender for the purpose of watch list screening, under the authority of 49 U.S.C. section 114, the Intelligence Reform and Terrorism Prevention Act of 2004 and 49 C.F.R parts 1540 and 1560. You may also provide your Redress Number, if available. Failure to provide your full name, date of birth, and gender may result in denial of transport or denial of authority to enter the boarding 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 review the system of records notice and the privacy impact assessment, please see the TSA Web site at www.tsa.gov."

5.2 Technology Service Desk

DHS is committed to providing support to all aircraft operators in their transition, integration process, and ongoing interaction with DHS. To meet this need, DHS will do the following:

- Institute a single point of contact for each program for routine interaction
- Operate a service center to assist in the resolution of apparent matches to watch list entries.
- Provide an operations support desk for real-time technical support calls

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

Points of Contact

Both Secure Flight and APIS Pre-Departure will designate an account manager for each aircraft operator. The account manager will serve as the aircraft operator's principal point of contact during implementation planning, testing, and cutover. Once the aircraft operator cuts over to full use of the respective program, the account manager will continue to serve as the single point of contact.

Service Center

To assist aircraft operators and law enforcement officers, DHS established the DHS Service Center and the Secure Flight Service Center. The purpose of these centers is to provide assistance to aircraft operators in the event a passenger is identified as having a boarding pass restriction resulting from a possible watch list match or the aircraft operator is experiencing a communication disruption with DHS. Law enforcement officers will be able to contact the DHS Service Center or Secure Flight Service Center should they need assistance in the process of determining if the identified passenger is the actual subject of interest. DHS is currently researching an industry solution that will provide aircraft operators the opportunity to assist VWP travelers in meeting ESTA requirements. The DHS Service Center is not intended to provide guidance on requirements associated with the ESTA Interim Final Rule.

The telephone numbers for the DHS Service Center and Secure Flight Service Center will be provided prior to cutover.

Operations Support Desk

CBP▸ has established a Technology Service Desk for identifying system issues. When an aircraft operator detects failures in the DHS response process, aircraft operator representatives, preferably from their operational support staff, should contact the support desk to determine the extent of an identified system issue and initiate problem analysis and resolution.

The Technology Service Desk will provide implementation and operations support. It will provide technical assistance throughout the aircraft operator's transition to DHS's assumption of watch list operations. The Technology Service Desk will provide ongoing, steady-state technical support to include emergency procedures and guidance for handling system outages.

TSA▸ Aircraft operators will call the Secure Flight Service Center to reach the Operations Support Desk for Secure Flight.

The telephone number for the Operations Support Desk will be provided prior to cutover.

5.3 Operating Carrier Responsibilities

The APIS Pre-Departure regulations, Secure Flight Final Rule, and ESTA Interim Final Rule apply to the operating carrier on which a passenger is to be flown. While the operating carrier may elect to have other organizations perform certain business functions on their behalf, it remains the responsibility of the operating carrier to comply with the respective regulation. Two examples to which this guidance would apply are code shared flights and ground handling arrangements.

5.3.1 Reservations

TSA▶ Reservations Data

Under the Secure Flight rule, the aircraft operator is responsible for requesting and collecting a passenger’s full name, date of birth, gender, and Redress Number (if available). The rule encourages aircraft operators to develop and adopt an industry standard method for conveying the full name, date of birth, gender, and redress number among aircraft operators, reservation providers, and Global Distribution Systems. Aircraft operators are not expected to validate the data collected during the reservations process.

The criteria for an appropriate full name is the name as it appears on the individual’s verifying identity documents as defined in 49 CFR 1560.3. Recognizing that a single character can legitimately be a complete first name, the data definitions provide for a one character first name. If, for example, a middle initial is reflected on the verified identity document, then a middle initial is to be recorded as the middle name for DHS purposes.

5.3.2 Passenger Check-in

TSA▶ Boarding Passes

A passenger or non-traveler’s request for a boarding pass or authorization to enter an U.S. airport sterile area is the point at which automated aircraft operators will use their check-in systems to enforce the appropriate passenger handling for the boarding pass printing result provided to them. Aircraft operators using boarding control procedures other than printed boarding passes must adopt an equivalent with the approval of their assigned TSA Principal Security Inspector (PSI) or International Industry Representative (IIR).

CBP▶ ESTA Status

ESTA passengers with Cleared boarding pass printing results may be issued a boarding pass at check-in. Although ESTA status query results will not be a determining factor for boarding pass printing results, the aircraft operator must verify that any travelers attempting travel under the VWP have complied with the requirement to obtain an electronic travel authorization via the ESTA prior to permitting boarding of the flight.

TSA▶ Check-in Statuses

All passengers with an Inhibited boarding pass printing result at check-in must be directed to the airport for resolution. The aircraft operator will engage in the resolution process described in section 5.3.4.

Aircraft operators may provide organizations and/or individuals acting on behalf of the aircraft operator (e.g., third party ground handlers, etc.) with the information regarding Selectee and Inhibited boarding pass printing results. Third party ground handlers submitting SFPD on the behalf of a covered aircraft operator must comply with the requirement to maintain the record locator number and passenger reference number that was submitted as early as 72 hours prior to flight departure by the covered aircraft operator for each individual. Aircraft operators must comply with the approved procedures in their security program and any applicable Security Directives or Emergency Amendments for processing passengers/baggage with Selectee and Inhibited results whether those activities are performed by their own employees or organizations/individuals acting on the aircraft operator's behalf.

In the unlikely event that the passenger lacks a boarding pass printing result, an aircraft operator may initiate a watch list matching request from any approved check-in location or process. The most common reason for an absent boarding pass printing result is insufficient time between submission of the watch list matching request and the attempted check-in transaction (e.g., go-show) or due to a system malfunction by either the aircraft operator or TSA. In such cases, the aircraft operator would be provided an interactive means (see Section 4.1) to submit a request for immediate watch list matching.

TSA anticipates that aircraft operators may perform the check-in process via common use devices, e.g., Common Use Terminal Equipment (CUTE), Multi Use Self-Service Equipment (MUSE), and Common Use Self-Service (CUSS) kiosks if compliant functionality has been enabled on these devices.

Approved check-in locations for each of the boarding pass printing results are summarized in Table 40. Note: Aircraft operators may be authorized to accept and process verifying ID at a self-service kiosk.

Table 40 Approved Check-in Locations by Boarding Pass Printing Result

Location	Cleared	Selectee	Inhibited
Internet/off-site	Yes	No	No
Airport self-service kiosk	Yes	No -	No – passenger check-in will be allowed only if verified ID collection at a kiosk is authorized (see note above) and if a Cleared boarding pass printing result is achieved during resolution (see Section 5.3.4).
Airport counter (agent)	Yes	Yes	No – passenger check-in will be allowed only if Cleared boarding pass printing result is achieved during resolution or his/her status is downgraded to Selectee (see Section 5.3.4).

Internet/Off-site

All passengers with a Cleared boarding pass printing result for the TSA security check can obtain their boarding pass via an off-site location (e.g., Internet, off-airport kiosk, etc.) if available. If a passenger attempting to check in off-site does not have a Cleared boarding pass printing result, the aircraft operator system must direct the passenger to the airport for check-in.

If a passenger attempting to check in off-site does not have a boarding pass printing result, the aircraft operator system may generate a watch list-matching request to DHS and obtain a boarding pass printing result. Once the boarding pass printing result is received, the aircraft operator can process the check-in request consistent with the result received.

Although ESTA status query results will not be a determining factor for boarding pass print results, the aircraft operator must verify that any travelers attempting travel under the VWP have complied with the requirement to obtain an electronic travel authorization via the ESTA.

Airport Self-service

All passengers with a Cleared boarding pass printing result may use an airport self-service kiosk to obtain a boarding pass. If a passenger does not have a boarding pass printing result, the kiosk should generate a watch list matching request to DHS and process the check-in request consistent with the boarding pass printing result received.

Any passenger attempting to check in at an airport self service kiosk with a Selectee or Inhibited boarding pass printing result must be directed to airport check-in representatives and the aircraft operator will follow the resolution process in Section 5.3.4 unless the aircraft operator has been authorized to accept verifying identification at their kiosk. If authorized to do so, the kiosks can initiate an updated SFPD with the verifying identification indicator set. Passengers receiving a Cleared boarding pass printing result may then be issued a boarding pass. Those receiving an Inhibited result following the verifying identification process must be directed to airport check-in representatives and the aircraft operator will follow the resolution process in Section 5.3.4

Although ESTA status query results will not be a determining factor for boarding pass print results, the aircraft operator must verify that any travelers attempting travel under the VWP have complied with the requirement to obtain an electronic travel authorization via the ESTA.

Ticket Counter Check-In

Aircraft operators will be authorized to issue boarding passes to passengers identified as Cleared. Passengers with a Selectee or Inhibited result require resolution of their status. See the resolution process in Section 5.3.4 for details.

Although ESTA status query results will not be a determining factor for boarding pass print results, the aircraft operator must verify that any travelers attempting travel under the VWP have complied with the requirement to obtain an electronic travel authorization via the ESTA.

CBP▸ See Data Validation, Section 5.3.3.

Gate Passes

TSA▸ Aircraft operators have existing processes to issue authorization to enter an U.S. airport sterile area to non-travelers (e.g. gate passes). Aircraft operators must obtain a Cleared boarding pass printing result prior to issuing the authorization. Non-travelers must present a valid government ID (photo, full name, date of birth) at the ticket counter. The aircraft operator will then submit an SFPD to Secure Flight for watch list matching.

Refer to the UN/EDIFACT or XML guide, as appropriate, for the authorization to enter an U.S. airport sterile area to non-travelers request data requirements.

Aircraft operators must not issue an authorization to enter an U.S. airport sterile area to non-travelers for whom the aircraft operators receive a Selectee or Inhibited boarding pass printing result. Aircraft operators, however, may follow the procedures in Section 5.3.4 to attempt to resolve Selectee or Inhibited boarding pass printing result to obtain a Cleared message for non-travelers.

Aircraft operators will receive a Travel Authorization via ESTA not applicable code for gate requests for authorization to enter an U.S. airport sterile area to non-travelers.

5.3.3 Data Validation

Data Validation

CBP▸ Data collected for international travel must be validated by the aircraft operator or those acting as agents of the aircraft operator. Collecting the data found in the Machine Readable Zone of the individual’s travel document typically performs this validation: full name, date of birth, document type, document number, document country of issuance, document expiration, gender, and nationality.

Aircraft operators should validate any data or claims by a traveler that they possess an additional U.S.-issued travel document that supersedes ESTA requirements.

TSA▸ TSA requires that data collected for domestic and international travel be validated at the ticket counter or a self service device (kiosks) that accepts Verifying Identity Documents, as defined in 49 CFR 1560.3, for those passengers whose boarding pass printing results reflect an Inhibited boarding pass printing result.

When a VID is required, Aircraft Operators can manually check the VID or they can employ kiosks that, as required by the Secure Flight Final Rule, are capable of determining that the identification is a valid VID, authenticating the VID, and reading and transmitting passenger information from the VID.

5.3.4 Passenger Handling – Airport Procedures and Resolution of Boarding Pass Printing Result

Cleared Passenger

TSA▶ Passengers with a Cleared response may check in using any approved check-in facility offered by the aircraft operator or its handling agents.

Selectee Airport Procedures

TSA▶ The aircraft operator must comply with the AOSSP, MSP, security directives, emergency amendments, and any other regulatory requirements for selectee processing and selectee baggage acceptance and handling.

The watch list contains names of persons who are permitted to travel, but who must be designated as a Selectee. Passengers receiving a Selectee boarding pass printing result are to be handled according to applicable TSA procedures.

There are criteria defining individuals exempted from CAPPS Selectee status (e.g., on duty military personnel traveling in uniform) today. Please note that there are no similar exemptions for Secure Flight Selectees.

Inhibited Resolution

TSA▶ The Inhibited resolution process can only be performed by an aircraft operator at a staffed check-in location (typically the departure airport). If a passenger has a boarding pass printing result of Inhibited, but can provide additional information to the aircraft operator and/or law enforcement officer that proves they are not a true watch list match, then the person may be cleared.

Aircraft operators who are authorized to capture verifying identification at a kiosk may elect to perform steps one and two below at a kiosk. Resolution processing for step three and higher must be performed by an aircraft operator representative.

Step 1 – Check-in representatives (agent) ask the passenger to present a valid travel ID or authorized travel document. Documents requirements are detailed in each program's published regulation.
Note: If the passenger presents the agent with a government ID that has a date of birth with the year only and does not have another valid travel ID with full date of birth, the agent must contact the Secure Flight Service Center, speak with a Customer Support Agent and continue the Resolution process (Step 3). They should not proceed to Step 2 below.

Step 2 – The agent determines if the name, date of birth, gender, or other travel document details (as applicable) are already correct and complete in the passenger's record in the aircraft operator's system. If the passenger presents a government ID with a date of birth with year only and does not have another valid travel ID, the agent must contact the Secure Flight Service Center and speak with a Customer Support Agent. Incorrect or incomplete information is updated by the agent. Additionally, the agent adds a Redress Number, should the passenger provide one. The aircraft operator's system then resubmits the data to DHS with a "verified ID" indicator. If the DHS response to the resubmission is either Cleared or Selectee, the appropriate handling for either status can proceed and the passenger can proceed to the security screening checkpoint and the gate. If the boarding pass printing result remains Inhibited, proceed to step three.

Step 3 – The aircraft operator calls the Secure Flight Service Center. The Customer Support Agent asks the aircraft operator routine questions to validate the call (no special training is required to respond to these questions; responses are used for tracking purposes [e.g., logging service request], recording, callbacks, if needed, quality assurance, etc.).

Step 4 – The Secure Flight Service Center follows specific standard operating procedures in determining if the passenger is the person of interest. In some cases, TSA may request passenger resolution information from the aircraft operator. This information includes, but is not limited to, the following:

1. Passenger Record Locator and Airport Station Code
2. Type of verifying identity document the passenger presented
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

In those cases where the boarding pass printing result changes from Inhibited to Cleared or Selectee, DHS will send the appropriate boarding pass printing result as an Unsolicited Message to the aircraft operator, which may, in turn, release the boarding pass for issuance.

Step 5 – Should the passenger remain inhibited, the aircraft operator must not accept the passenger for transportation, unless otherwise specifically authorized by TSA. The agent should inform the individual that there is an issue with the reservation that must be resolved before travel can be authorized.

Step 6 – Should DHS determine that the passenger is authorized to board an aircraft or to enter an U.S. airport sterile area; the appropriate boarding pass printing result will be sent to the aircraft operator, which can, in turn, release the boarding pass.

Step 7 – Aircraft operators must verify through the updated boarding pass authorization that a VWP traveler has complied with the ESTA Interim Final Rule.

Deporting a Passenger

TSA▶ In rare situations, it will be necessary for a law enforcement officer[1] or other

[1] A sworn employee of a government entity (Federal – to include U.S. military police, U.S. Capitol Hill Police, State, Territorial, Tribal and local, including U.S. military police) or rail carrier under 49 U.S.C. 28101, with full

with Inhibited Status

authorized representative of DHS’s Immigration and Customs Enforcement (ICE) to request a boarding pass for the purpose of deporting a person whose name appears on a watch list (No Fly List). The process requires close coordination between the aircraft operator, law enforcement officer, and any other affected government agencies. The following are the procedures to assist the aircraft operator with a better understanding of their participation in the process and how to obtain a boarding pass printing result for the inhibited deportee.

1. A normal reservation for travel is made with the aircraft operator for the deportee and escort(s) (including a full name, DOB, and gender).
2. The aircraft operator submits the reservation (via SFPD) to DHS for screening as normal.
3. After automated watch list matching is performed, DHS returns an Inhibited boarding pass printing result to the aircraft operator.
4. A completed Detention and Removal Office request waiver form is transmitted to the appropriate government agencies. A copy of the waiver should be submitted to and kept on file with the Secure Flight Service Center before scheduled time of departure.
5. Deportee and escort(s) approach the ticket counter at the airport and provide credentials and the waiver letter. The check-in agent accesses the reservation of the Inhibited deportee and contacts the Secure Flight Service Center (same procedures at the ticket counter as for any other inhibited traveler).
6. The Secure Flight Service Center reviews the inhibited record and waiver letter and transmits a Cleared boarding pass printing result from Secure Flight via an unsolicited update back to the aircraft operator. The check-in agent can print the boarding pass.
7. DHS emails a one-time waiver for the Inhibited passenger to the aircraft operator for the provided destination.

No Fly Airport Procedures

TSA▸ Aircraft operators must not issue a boarding pass and must deny transportation, to passengers for whom the resolution process has been completed and who continue to have an Inhibited boarding pass printing result, unless otherwise specifically authorized by TSA.

5.3.5 Irregular Operations Procedures

Irregular operations often cause aircraft operators to modify passenger data as the passenger is accommodated on another flight. Handling the modified reservation and existing boarding pass printing result will be determined by the flight on which the passenger was rebooked. Passengers protected online (same aircraft operator) will be handled differently from those protected offline (with another aircraft operator).

power of arrest, who is trained and commissioned to enforce the public criminal laws of the jurisdiction(s) in which he/she is commissioned.

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

For a passenger rebooked on flights operated by the same aircraft operator scheduled to depart on the same day, DHS will require submission of an informational update Passenger Data Message. Secure Flight permits the continued application of the existing boarding pass printing result for same-day travel with the same aircraft operator. APIS Pre-Departure will provide a new result. Informational updates are not required for changes to scheduled departure times or scheduled arrival times, unless the date of flight departure or flight arrival changes. The aircraft operator will not receive a boarding pass printing result in response to an informational update.

If the modification involves accommodation on a flight operated by another aircraft operator, the aircraft operator on whom the passenger has been rebooked will be required to submit a new Passenger Data Message and obtain a new boarding pass printing result.

An aircraft operator is not required to inform DHS that a modified passenger data record was triggered by an irregular operation. Standard Passenger Data Messages will be used in transmitting the watch list matching request to DHS.

5.4 Redress Process

DHS has established the DHS Traveler Redress Inquiry Program (DHS TRIP). DHS TRIP is a single point of contact for individuals to request redress if the individual believes that he or she has been improperly or unfairly delayed or prohibited from boarding an aircraft or entering a sterile area as a result of a DHS program. DHS TRIP provides domestic and international passenger redress while working with relevant DHS components to review and respond to requests for redress.

The redress process does not involve aircraft operator intervention, with the exception of directing the passenger to DHS TRIP for redress application and processing. Information about the redress process is available on the DHS TRIP website http://www.dhs.gov/trip.

Once the claim is adjudicated, the individual will be provided a redress number and, if appropriate, added to the Cleared List. DHS will incorporate the Cleared List in the watch list matching process to limit the likelihood of future misidentification.

DHS TRIP will also be available to individuals who dispute their ESTA adjudication decision.

5.5 System Outage Procedures

The following sections outline the procedures aircraft operators should follow depending on the state of their transition of watch list matching to DHS.

5.5.1 Secure Flight Definition of an Outage

For the purposes of this discussion, an outage can occur at various points in the Secure Flight process which prevents:

- SFPD from reaching Secure Flight or
- DRM from reaching the aircraft operators

***WARNING:* This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

5.5.2 Secure Flight Outage Strategy

Secure Flight has put in place a number of mechanisms to minimize the likelihood and duration of an outage with systems operated by DHS. Because Secure Flight employs a highly redundant architecture, including operations of two fully redundant sites and systems in geographically distinct locations, many failures will have no impact to system uptime.

Secure Flight, however, cannot control or prevent outages caused by failures of systems or processes operated by aircraft operators, their suppliers, or partners. To assist with these outage situations, Secure Flight has processes to assist the aircraft operators in minimizing disruption to operations. Watch list matching of passengers in advance will limit the impact of any short duration outages.

5.5.3 Secure Flight Outage Declaration and Communication

During any outage, it will be imperative for affected aircraft operators and Secure Flight to work together to diagnose the problem and implement a strategy for its resolution. Rapid response and continued communication will help minimize the impact of the outage and ensure the timeliest resolution to normal operations. Secure Flight maintains a number of mechanisms to quickly respond to an outage including:

- A Secure Flight Service Center operating 24 hours a day 365 days a year and trained in handling Secure Flight outage related calls
- A Crisis Management Team on call 24 hours a day 365 days a year consisting of key personnel required to declare an outage and put in place mechanisms to return to normal operations

Aircraft Operator Detects an Outage: In the event that the aircraft operator detects an outage that impacts the aircraft operator's ability to communicate with Secure Flight, the aircraft operator's designated point(s) of contact should call the Secure Flight Service Center immediately and begin working with Secure Flight to address the outage. Aircraft operators should use this mechanism to report any outage or service degradation, regardless of its source. Secure Flight will inform the caller if Secure Flight has already declared an outage, the current status, and any steps that should be taken, based on direction coming from Secure Flight's Crisis Management team.

Initially, when it is determined that the aircraft operator issue affects Secure Flight's operations, a warning order is communicated to the aircraft operator. Secure Flight will then make a determination to declare an outage, communicate the activation order, and provide the activation order code to the aircraft operator authorizing the activation of the appropriate alternate procedure(s). Secure Flight will continue to monitor the outage situation and communicate status until the system issue is resolved. Upon resolving the issue, Secure Flight will notify the aircraft operator, issue the deactivation order, and provide the deactivation order code authorizing the submission of passenger data through the normal process (prior to the outage).

> Note: The activation and deactivation order codes can be up to 30 alphanumeric characters in length and include the Secure Flight supervisor's initials, the carrier code, date, time, and activation/deactivation indicator. These codes must be logged by the aircraft operator for compliance purposes and represent documentation between the aircraft operator and TSA to activate or deactivate the specified outage alternative.

Secure Flight Detects an Outage:

The procedures include the authority and capability to identify an outage and rapidly work to address its cause. When Secure Flight detects an issue and determines that there is an impact to operations, Secure Flight communicates the warning order to the aircraft operator. Upon declaration of an outage by Secure Flight, the activation order and activation order code is communicated to the aircraft operator authorizing the activation of the appropriate alternate procedure(s). Secure Flight will continue to monitor the outage situation and communicate status until the system issue is resolved. Upon resolution of the issue, Secure Flight will notify the aircraft operator, issue the deactivation order, and provide the deactivation code authorizing the submission of passenger data through the normal process (prior to the outage).

> Note: The activation and deactivation order codes can be up to 30 alphanumeric characters in length and include the Secure Flight supervisor's initials, the carrier code, date, time, and activation/deactivation indicator. These codes must be logged by the aircraft operator for compliance purposes and represent documentation between the aircraft operator and TSA to activate or deactivate the specified outage alternative.

5.5.4 Secure Flight Outage Options

One or more of the alternate procedures listed below will be invoked during an outage based on available knowledge and the protocols of Secure Flight's Crisis Management Team.

Table 41 Secure Flight Outage Options

Option	Prior TSA Authorization Required	Activation / Deactivation Code Required
1. Aircraft operator contacts sister city to receive watch list matching results	No	No
2. Use existing Secure Flight boarding pass printing results to process passengers	Yes	Yes
3. Fall back to pre-Secure Flight watch list matching processes	No	No
4. Aircraft operator contact the Secure Flight Service Center to receive watch list matching results	Yes	Yes
5. Aircraft operator sends passenger data to Secure Flight via eSecure Flight	Yes	Yes
6. Designate passengers who have not been cleared by Secure Flight as "Selectee" for a period of time	Yes	Yes

Aircraft operators may automatically initiate options 1 and 3, but must be specifically and formally authorized by TSA to use all other Secure Flight outage options. The following outage responses may be activated individually or collectively in a combination of responses depending upon the nature and expected duration of the outage.

5.5.4.1 Aircraft Operator Contacts Sister City to Receive Watch List Matching Results

This option enables the aircraft operator to contact an alternate site (i.e. sister city, operations center, etc.) for watch list matching results.

The aircraft operator will execute the following procedures:

1. The aircraft operator representative notifies their resources that they can now contact an alternate site (i.e. sister city, operations center, etc.).
2. The down city provides the alternate site with the names of the passengers that need to be submitted for watch list matching.
3. The alternate site performs the following:
    a. Submits the passenger data (from the down city – as necessary) to Secure Flight for watch list matching.
    b. Receives boarding pass printing results from Secure Flight.
    c. Verifies the boarding pass printing results.
    d. Provides the results to the down city.
4. The down city manually checks-in and processes passengers for travel.
5. The aircraft operator will begin submitting passenger data through the normal process (prior to the system outage) when the issue is resolved.

5.5.4.2 Use Existing Secure Flight Boarding Pass Printing Results to Process Passengers

When authorized by TSA, during an outage, aircraft operators may use existing "Cleared" boarding pass printing results returned by Secure Flight to process passengers with either informational and qualified changes (i.e., Name, Date of Birth, Gender, etc.) that occur subsequent to the receipt of the "Cleared" result. The requirement to submit informational and qualified change messages will be suspended, and the aircraft operator can rely on the most recently received boarding pass printing result.

If Secure Flight determines that an outage has occurred, Secure Flight will contact the aircraft operator's point(s)-of-contact (POC) to provide the activation order code authorizing the aircraft operator to use existing boarding pass printing results during the outage. Once authorization is given, the aircraft operator and Secure Flight will execute the following procedures:

1. The aircraft operator point(s)-of-contact notifies the respective aircraft operator responsible parties that Secure Flight has declared that an outage has occurred and that boarding pass printing results processed prior to the outage can be used to process passengers.
2. The aircraft operator uses boarding pass printing results returned by Secure Flight prior to the outage. Passengers with a "Cleared" or "Selectee" result may be issued a boarding pass. **Note: aircraft operators may not issue a boarding pass to passengers who have "Inhibited" boarding pass printing results or for whom the aircraft operator has not yet received a result unless they are processed using another outage option approved by TSA.**
3. The aircraft operator and/or Secure Flight resolve the system outage issues, and Secure Flight provides the deactivation order code to the aircraft operator authorizing the aircraft operator to resume submitting passenger data through the normal process.
4. The aircraft operator must submit data for all passengers processed during the outage to Secure Flight.

5.5.4.3 Fall Back to Pre-Secure Flight Watch List Matching Processes

The Watch List Fall Back option allows aircraft operators to access the watch list (through their security personnel/operations center) and to use the watch list matching processes set forth in the SD 1544-01-20 series and the SD 1544-01-21 series and EA 1546-01-17 series and EA 1546-01-18 series to perform watch list matching. The details of this may vary from aircraft operator to aircraft operator. All aircraft operators opting to fall back to pre-Secure Flight watch list matching processes must comply with TSA Security Directives and Emergency Amendments that define the requirements of aircraft operator passenger watch list matching. For example, passengers matching “Selectee” or “No Fly” list entries must be cleared through TSA in accordance with existing Security Directives and Emergency Amendments or security program requirements governing passenger watch list matching. It should be noted that aircraft operators who are cutover to Secure Flight must contact the Secure Flight Service Center for resolution.

Aircraft operators may program their systems to automatically fall back to pre-Secure Flight watch list matching processes after 4 attempts to submit SFPD on an interactive message (that is a message placed on the high priority queue within 24 hours of scheduled flight departure) without a response. The aircraft operator must notify the Secure Flight Service Center upon executing this option. Aircraft operators will be subject to a compliance determination if this outage option is activated incorrectly (i.e., alternative is implemented when no real outage exists).

The aircraft operator and Secure Flight will execute the following procedures:

1. The aircraft operator attempts to make requests on an interactive message (that is a message placed on the high priority queue within 24 hours of scheduled flight departure) and does not receive a response after executing the following steps:
    a. The aircraft operator submits SFPD and pauses prior to attempting resubmission of SFPD.
    b. After 4 attempts to submit SFPD, the aircraft operator does not receive a response.
2. The aircraft operator notifies the responsible parties that they may activate the fall back to pre-Secure Flight watch list matching processes.
3. The aircraft operator notifies the Secure Flight Service Center of the outage detection and their fall back to pre-Secure Flight matching processes.
4. The aircraft operator accesses the watch list based on the current Web Board process and begins watch list matching based on their pre-Secure Flight procedures. **Note**: **Aircraft operators who choose this option must continue to load the watch list updates (Cleared, Selectee and No Fly lists) Monday through Friday.**
5. The aircraft operator and/or Secure Flight resolve the system outage issue and Secure Flight provides the deactivation order code to the aircraft operator authorizing the aircraft operator to resume submitting passenger data through the normal process.
6. The aircraft operator must submit data for passengers processed during the outage to Secure Flight.

5.5.4.4 Aircraft Operator Contacts the Secure Flight Service Center to Receive Watch List Matching Results

This option authorizes the aircraft operator to call the Secure Flight Service Center for watch list matching results.

Upon receipt of the outage declaration, the Crisis Management Lead will coordinate with the Airline Implementation Managers (AIMs), the TSA Alerts System, and/or designees to contact the aircraft operator’s POCs and communicate the activation order code authorizing the aircraft operator to contact the Secure Flight Service Center to receive watch list matching results. Upon receipt of formal authorization, the aircraft operator and Secure Flight will execute the following procedures:

1. The aircraft operator representative notifies their resources that an outage has occurred and to contact the Secure Flight Service Center for boarding pass printing result.
2. The aircraft operator utilizes boarding pass printing results obtained from the Secure Flight Service Center.
3. The aircraft operator and/or Secure Flight resolve the system outage issues and Secure Flight provides the deactivation order code to the aircraft operator authorizing the aircraft operator to begin submitting passenger data through the normal process (prior to the system outage).

5.5.4.5 Aircraft Operator Sends Passenger Data to Secure Flight via eSecure Flight

This option authorizes aircraft operators to send passenger data to Secure Flight via eSecure Flight temporarily in the event of an outage associated with the aircraft operator or DHS .
Note: Additional capabilities are being implemented to accommodate this option in the future.

Upon receipt of the outage declaration, the Crisis Management Lead will coordinate with the Airline Implementation Managers (AIMs), the TSA Alerts System, and/or designees to contact the airline POCs and communicate the activation order code authorizing the aircraft operator to send passenger data and receive boarding pass printing results via eSecure Flight during the outage. Upon receipt of formal authorization, the aircraft operator and Secure Flight will execute the following procedures:

1. The aircraft operator representative notifies their resources that an outage has occurred and provide authorization to send passenger data and receive boarding pass printing results via eSecure Flight.
2. Secure Flight will confirm account activation and provide the aircraft operator with a temporary password (access to eSecure Flight system).
3. The aircraft operator representative notifies their resources that they can now access the eSecure Flight system to send passenger data and receive and apply boarding pass printing results. Note: If an aircraft operator chooses to use this option, it does not relieve them from satisfying their APIS submission responsibilities as they relate to international arrival and departure requirements.
4. The aircraft operator and/or Secure Flight resolve the system outage issues and Secure Flight provides the deactivation order code to the aircraft operator authorizing the aircraft operator to begin submitting passenger data through the normal process (prior to the system outage).

5.5.4.6 Designate Passengers Who Have Not Been Cleared By Secure Flight as “Selectee” for a Period of Time

This option authorizes the aircraft operator to designate all passengers not cleared by Secure Flight prior to the outage as “Selectee.” Passengers with existing “Cleared” boarding pass printing results can be issued boarding passes. The use of informational and qualified change messages will be suspended and the aircraft operator can rely on the most recently received boarding pass printing result. All passengers who have not been cleared by Secure Flight must proceed to the ticket counter or airport kiosk, and aircraft operators will designate them as “Selectee” upon check-in.

TSA may authorize the aircraft operator to designate a certain percentage (less than 100%) of the passengers not cleared by Secure Flight as "Selectee." Aircraft operators must program their systems so that they can select a setting from 100% to any percentage lower than 100% with random selection. The default setting is 100% unless otherwise notified by TSA.

If Secure Flight determines that an outage has occurred, Secure Flight will contact the aircraft operator's point(s)-of-contact to communicate the activation order code authorizing the aircraft operator to designate passengers who have not been watch list matched as "Selectee" for a period of time.

Upon receipt of formal authorization by TSA to implement this option, the aircraft operator and Secure Flight will execute the following procedures:

1. The aircraft operator(s) notifies passengers who have not been cleared by Secure Flight that check-in must occur at the ticket counter or kiosk.
2. The aircraft operator(s) designates all passengers (or a percentage of passengers if authorized by TSA) who have not been cleared by Secure Flight as Selectee.
3. Passengers designated as Selectee proceed to the check point for enhanced screening.
4. The aircraft operator and/or Secure Flight resolve the system outage issue and Secure Flight instructs the aircraft operator to resume submitting passenger data through the normal process.
5. The aircraft operator must submit data for all passengers processed during the outage once Secure Flight returns to normal operations.

NOTE: During a documented Secure Flight outage, aircraft operators are required to submit APIS data to CBP using alternative means, for flights arriving into or departing from the United States. Aircraft operators are expected to coordinate alternative submission procedures with their National APIS Account Manager and the local CBP Port office impacted.

5.5.5 CBP Outage Declaration and Communication

In many cases, it is not immediately evident which component of a communications system is not operating properly. A delay may result while identifying the outage cause.

The APIS Pre-Departure system is in outage status when an aircraft operator is not able to obtain a watch list matching result. An aircraft operator determines a system outage when either five AQQ Cleared requests are submitted (allowing for the delivery and return of the message, including a four-second processing time period) and no response is returned by DHS, or a single APIS batch submission is transmitted (allowing for the delivery and return of the message, including a 30 minute processing time period) and no response is returned by DHS.

Aircraft operators are encouraged to develop the most appropriate alternative methods to mitigate the impact an outage may cause and to submit APIS data as early in the process as possible, to receive a screening result. When an outage is identified, aircraft operators may board those passengers who already have a boarding pass printing result. It should be noted that complete APIS data is still required.

The following guidance provides several options for aircraft operators during outage situations:

Aircraft operators can revert to other methods for providing APIS data to CBP and apply screening results without prior coordination with DHS, which is preferred by most operators. These methods include:

- Transmitting data from an alternate station, location, or system
- Backup system or alternate service providers such as SITA/ARINC
- eAPIS submission including manifest upload function
- New web service for system-to-system connectivity (email replacement)

Many aircraft operators have indicated preference for using their internal watch list matching as a backup during outages. The operators can revert to using their internal watch list results. This temporary option can be used as long as the aircraft operator continues to obtain the watch list from DHS. TSA is working on additional outage procedures for contacting the Secure Flight Service Center when Secure Flight becomes operational and assumes watch list matching responsibility for all covered flights.

5.5.6 CBP Outage Options

Aircraft operators must implement the following procedures to notify DHS when they identify an outage:

1. An aircraft operator submits an email message to AQQoutages@dhs.gov.
   - The email message must identify aircraft operator codes and the flight number impacted or potentially impacted by the outage. The subject line of the e-mail message should include the aircraft operator code, flight number, and date of the flight.

2. An aircraft operator contacts the impacted CBP ports and provides each port with the impacted flights information.

Once an outage is identified and appropriate notifications have been initiated, aircraft operators will provide periodic updates to the AQQ Outage mailbox in 60-minute increments. For example, if an aircraft operator notifies the AQQ Outage mailbox of an outage at 2:00 pm and the outage is still in effect at 3:00 pm, the operator should submit another update.

When an aircraft operator resolves an outage, the operator will email the AQQ Outage mailbox so that appropriate notification can be provided to CBP management.

During outages, aircraft operators will continue to collect APIS data and continue to provide either AQQ or APIS batch submissions. In the event the aircraft operator is unable to collect required APIS data, they must take alternative measures to gather the data. When the outage is resolved, the aircraft operator will be able to electronically submit the required APIS data.

During outages, the electronic gathering of APIS data may be limited. However, with the various enforcement programs associated with APIS, CBP still expects the submission of APIS data.

If a system outage impacts the submission or confirmation of a Flight Close-Out message, the aircraft operator should send an email message to AQQoutages@dhs.gov. CBP expects aircraft operators to submit the Flight Close-Out message. In cases of non-compliance, CBP will take in to consideration the circumstances surrounding its submission.

CBP will communicate with aircraft operators through alternative mechanisms when it identifies a CBP outage. These may include posting a message to the CBP website or generating an email notification message.

5.6 System Outage Procedures-ESTA Status Verification

An alternative mechanism for confirming ESTA status in the event of an outage is currently being explored and will be provided in the future.

5.7 Interline Through Check-In

This section explains TSA Secure Flight policy regarding through check-in for interline itineraries and appropriate utilization of passenger verified ID information.
In through check-in situations, when the originating aircraft operator has received a “Cleared” or “Selectee” boarding pass printing result for a passenger, the originating aircraft operator may issue a boarding pass on behalf of any downline aircraft operators on the itinerary. Even if the originating aircraft operator has received a “Cleared” or “Selectee” boarding pass printing result, the downline aircraft operator must also obtain a “Cleared” or “Selectee” boarding pass printing result for the passenger prior to allowing the passenger to board.

In through check-in situations, when a passenger has gone through the Secure Flight verified ID process, the aircraft operator that conducted the verified ID process may pass the verified ID indicator and verified ID data to the downline aircraft operator(s) operating the subsequent connecting flight(s). The downline aircraft operator(s) may then use the verified ID indicator and the verified ID data provided by the originating aircraft operator to submit verified ID to Secure Flight. The downline aircraft operator(s) may request a boarding pass printing result for the passenger from Secure Flight using the verified ID indicator and the verified ID data provided by the originating aircraft operator.

Example: A passenger is booked on one aircraft operator (AO1) for the first leg of an itinerary and a different aircraft operator (AO2) for the second leg.

Previously in this scenario, TSA required both AO1 and AO2 to submit Secure Flight Passenger Data (SFPD) for the passenger, and AO1 was prohibited from issuing a boarding pass for the passenger’s second leg on AO2 (assuming all flights are domestic). Under the revised policy, both AO1 and AO2 still must submit SFPD for the passenger. However, upon receiving a “Cleared” or “Selectee” boarding pass printing result, AO1 may issue a boarding pass to the passenger for the second or subsequent legs (that meet the definition of directional travel as defined in the CUG) even if those flights are operated by a different aircraft operator.

Even if boarding pass printing results received by AO1 were “Cleared” or “Selectee”, if AO2 has received an “Inhibited” response from Secure Flight for the passenger, AO2 is still responsible for prohibiting the passenger from boarding.

When an inhibited passenger completed the verified ID process with AO1, AO1 may pass the ID data for name, date of birth, gender, passport information, redress number, known traveler number, and the verified ID indicator to AO2. AO2 may subsequently request a boarding pass printing result for the passenger to TSA using that verified ID data.

5.8 Standby Passengers

For a passenger who is listed as a standby passenger on one or more flights while confirmed on another flight, the aircraft operators must submit passenger data for the confirmed flight to Secure Flight. Aircraft operators should not submit passenger data for additional standby segment(s). If a passenger is subsequently confirmed on a standby flight, the aircraft operator must then submit an informational update for the passenger to Secure Flight.

5.9 Ticketed Reservation

Section 1560.101(a)(1) of the Secure Flight Final Rule (Chapter XII, of Title 49, Code of Federal Regulations) requires that "Each covered aircraft operator must request the full name, gender, date of birth, and Redress Number for passengers on a covered flight…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."

For the purpose of complying with Section 1560.101(a)(1):

The following guidelines apply for the purpose of complying with Section **1560.101(a)(1) of the Secure Flight Final Rule. TSA intends to carefully monitor the efficacy of these guidelines and will modify them as necessary to ensure full and effective implementation of the Secure Flight Final Rule.**

a) Aircraft operators may delay the collection of date of birth, gender, and Redress Number until the reservation is ticketed.
b) A reservation is considered to be ticketed at the time a customer pays for air transportation or seat or when the aircraft operator is informed that the customer has done so.
c) Reservations for which no payment is required (e.g., frequent flyer miles redemption, voucher use, companion pass redemption, use of coupon, and others) are to be considered ticketed at issuance of a travel authorization.
d) Travel Authorization is defined as: "Any electronic or written document that authorizes an individual to travel on an aircraft operator's aircraft."

All ticketed reservations must include full name, date of birth, and gender within 72 hours of scheduled time of departure. If the aircraft operator has not collected full name, date of birth, and gender for ticketed reservations within 72 hours of departure, the aircraft operator is non-compliant with the Secure Flight Final Rule.

If a passenger refuses to provide full name, date of birth, and gender, a boarding pass must not be issued to the passenger and the passenger must not be permitted to enter a sterile area or board an aircraft.

Exceptions

For domestic flight reservations initially made prior to August 15, 2009, aircraft operators are not required to collect date of birth, gender, or Redress Number even if a reservation is subsequently updated after August 15, 2009. For international flight reservations initially made prior to October 31, 2009, aircraft operators are not required to collect date of birth, gender, or Redress Number even if a reservation is subsequently updated after October 31, 2009. Please note that TSA may not be able to clear reservations lacking full name, date of birth, or gender and inhibited passengers will be required to supply a Verifying Identity Document to the aircraft operator prior to the issuance of a boarding pass.

TSA understands that some third parties (i.e., travel agent systems and other aircraft operators) might not provide full SFPD to covered aircraft operators after August 15, 2009. In light of this, TSA will accommodate reservations obtained through third parties that may not contain date of birth, gender, and Redress Number. Reservations without date of birth, gender, and Redress Number will not be rejected by TSA prior to November 1, 2010. However, TSA expects aircraft operators to work with third parties to obtain full SFPD as quickly as possible and expects to see a steady month-by-month increase in full SFPD submission rates until November 1, 2010 at which point almost all reservations should contain full SFPD. Please note that prior to November 1, 2010, while TSA will not reject SFPD without date of birth and gender from these excepted channels, TSA may not be able to clear reservations lacking full name, date of birth, or gender and inhibited passengers will be required to supply a Verifying Identity Document to the aircraft operator prior to the issuance of a boarding pass.

5.10 ESTA Resubmission

In the event that a passenger traveling to the United States has not received a favorable ESTA authorization and informs the aircraft operator representative that they have updated their ESTA information, the aircraft operator must resubmit an SFPD (message type = new) to DHS in order to receive both a watch list matching result and ESTA status in the DHS Response Message. Details regarding a new passenger message can be found in Part 4 UN/EDIFACT Implementation Guidelines of the Consolidated User Guide.

5.11 Lap Children

DHS' policy on Lap Children is tied to the individual boarding pass policies of each aircraft operator. If the aircraft operator requires a boarding pass for Lap Children, it must submit the SFPD for Lap Children. If the aircraft operator does not require a boarding pass for Lap Children, then TSA will not require the aircraft operator to submit SFPD for Lap Children.

For international flights, aircraft operators that require a boarding pass for Lap Children must submit the SFPD for Lap Children. Aircraft operators who do not require boarding passes for Lap Children flying on an international flight do not need to provide SFPD for Lap Children. For flights arriving into or departing from the United States, CBP requires the transmission of full and complete APIS data for each individual onboard the aircraft, including Lap Children.

5.12 Ground Handling

Aircraft operators have asked TSA for clarification regarding the processing of Secure Flight transactions when an aircraft operator's flight is "ground handled" by a different aircraft operator or ground services organization (e.g. Air France ground handling Delta Airlines flights departing Paris). In this context, ground-handling services typically include:

- Check-in counter services for passengers
- Departure gate services
- Passenger services at transfer counters, customer service counters, airline lounges, etc.

In addressing these situations, the following principles apply:

- The Passenger Reference Number (PRN), Record Locator Number, and Aircraft Operator Code must remain the same for all submissions for a given passenger's directional travel.
- The Aircraft Operator Code and flight number must be that of the operating carrier
- In the event of a security issue with a passenger, TSA will contact the operating carrier regardless of whether the passenger record has been transferred to a ground handler.
- Secure Flight will send solicited and unsolicited messages to the address (e.g. queue) of the most recent submission of Secure Flight Passenger Data (SFPD) for the affected passenger.

Various ground handling scenarios could meet the principle above. The scenarios described below are not necessarily an exhaustive description of possible scenarios.

Scenario A: The operating carrier passes SFPD to the ground handler prior to 72 hours before scheduled flight departure. The ground handler submits all SFPD to Secure Flight for the ground handled passengers (including the 72-hour submission). Secure Flight sends response to the ground handler.

Scenario B: The operating carrier submits all SFPD for the passenger to Secure Flight and receives all responses from Secure Flight. The ground handler accesses the operating carrier's Departure Control System (DCS) in a manner that supports ground handling. The ground handler does not submit SFPD to Secure Flight for the operating carrier's passengers. Secure Flight does not send responses to the ground handler for the operating carrier's passengers.

Scenario C: The operating carrier holds the passenger record until 24-to-48 hours pre-flight at which time the record handling passes to the ground handler. Under this scenario, the following events take place:

1. Prior to the operating carrier passing the passenger record to the ground handler:
   a. The operating carrier submits SFPD to meet the 72-hour data submission requirement.
   b. The operating carrier submits SFPD changes/adds/deletes prior passing the record handling to the ground handler.
2. After the operating carrier passes the passenger record to the ground handler:
   a. Upon receipt of the passenger record from the operating carrier, the ground handler must immediately send a SFPD message (change passenger message type) to TSA using the same Passenger Reference Number (PRN), Record Locator Number, and Aircraft Operator Code as previously submitted by the operating carrier for that particular passenger. (The immediate submission of SFPD message to TSA is required so that TSA transmits subsequent unsolicited boarding pass printing result changes to the ground handler.)

b. When the passenger record passes to the ground handler, the operating carrier may optionally pass a boarding pass printing result received from TSA for that passenger record.
c. The ground handler submits SFPD changes/adds/deletes after the record handling pass to the ground handler.

In Scenarios A and C above, TSA recognizes that the operating carrier will require the ability to reset the address to which unsolicited messages would be directed from that of the ground handler to that of the operating carrier primary system for the purpose of receiving unsolicited updates, especially in the case of passengers with directional travel qualified connecting flights. The operating carrier may send a SFPD message (change passenger message type) to TSA using the same Passenger Reference Number (PRN), Record Locator Number, and Aircraft Operator Code as previously submitted for that particular passenger to establish the required "reply to" address.

5.13 Duplicate Message Submissions

In order to maintain the desired message response times and eliminate unnecessary transmissions, DHS seeks to proactively reduce needless and erroneous message traffic. DHS requires aircraft operators to submit an initial new SFPD message. After this initial SFPD message is transmitted, subsequent transmissions associated with this initial SFPD should be submitted as a qualified or informational update (see Table 14 – SFPD Submission Rules for Passenger Updates). DHS understands that duplicate messages will be received from aircraft operators as a result of the following submission alternatives and/or events.

1. Alternative SFPD Submission Method via the PNR pull/push connection with CBP (see Section 4.12)

   - Initial submission via the 72 Hour PNR Pull/Push

   - Subsequent SFPD submissions once the DCS is initialized (not later than 24 hours prior to flight departure). These SFPD submissions will be identified with a message type of "new".

2. 72 Hour Continuous Submission Alternative (see Section 4.13)

   - Initial submission beginning at 72 hours prior to scheduled flight departure with continued submission of SFPD (new and changed – qualified or informational) up until the DCS is initialized.

   - Re-submission of SFPD once the DCS is initialized (not later than 24 hours prior to flight departure). These SFPD submissions will be identified as qualified updates.

3. Interactive Message Response Timeouts

   - If the aircraft operator sets a timeout parameter on interactive request messages and experiences a timeout, they are to re-transmit the messages they had previously submitted.

If the aircraft operator has not implemented one of above submission alternatives or has not experienced a message timeout, they are required to follow the guidance as described in Table 7 – Passenger Data Required Transmission Timing.

5.14 No Fly Waiver Letters

Under Secure Flight Final Rule, **§ 1560.105 Denial of transport or sterile area access; Designation for enhanced screening** if TSA sends a covered aircraft operator a boarding pass printing result that states a passenger must be placed on inhibited status, the covered aircraft operator must not issue a boarding pass and must not allow that individual to board an aircraft. However, this does not include a provision for individuals on the No Fly List who must be escorted, by governing bodies, to another location within or outside of the United States on a Secure Flight covered flight. To address this issue, Secure Flight has developed the following process for the issuance of one-time waivers.

1. The aircraft operator receives an Inhibited boarding pass printing result from Secure Flight.
2. The aircraft operator contacts the Secure Flight Service Center for resolution.
3. Secure Flight renders a cleared status for the No-Fly passenger and returns a cleared boarding pass printing result.
4. The aircraft operator issues a boarding pass to the passenger.

6 OTHER GOVERNMENTAL PROGRAMS AND REQUIREMENTS

6.1 The Centers for Disease Control and Prevention (CDC)

The CDC is developing programs to more readily identify travelers as necessary to prevent the introduction, transmission or spread of communicable diseases and to ensure that CDC has the tools it needs to respond to public health emergencies and disease threats.