

SENSITIVE SECURITY INFORMATION

**U.S. Department of Homeland Security  
Transportation Security Administration (TSA)**



**Transportation  
Security  
Administration**

**Office of Transportation Threat Assessment  
and Credentialing (TTAC)**

**Secure Flight Program**

**Secure Flight/TSA OTSR/TSA-OI  
Business Requirements Document**

**CM Number: SF-REQ-1080**

**Version 1.4**

May 23, 2011

**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.

### Document Revision History

Date	Version	Modified By	Comments
11/15/2007	0.1	(b)(6)	(b)(5),(b)(6)
11/26/2007	0.2		
1/7/2008	0.3		
2/7/08	0.4		
2/20/08	0.5		
3/12/08	1.0		
4/2/08	1.1		
8/28/08	1.2		
4/29/2009	1.3		
5/19/2011	1.4		

**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 of Contents

1	Document Purpose .....	4
2	Document Scope .....	4
3	Document Organization .....	4
4	Organizational Overview .....	4
4.1	Secure Flight Overview .....	4
4.2	TSA OTSR Overview .....	5
4.3	TSA-OI Overview .....	6
4.4	TTAC Vetting Operations Overview .....	6
5	Relationship Overview .....	6
6	Business Requirements .....	7
6.1	Secure Flight's Business Requirements of TSA-OI .....	7
6.2	Secure Flight's Business Requirements of TSA OTSR .....	8
6.3	Secure Flight's Business Requirements of TTAC Vetting Operations .....	8
6.4	TSA OTSR's Business Requirements of Secure Flight, TSA-OI, and/or TTAC Vetting Operations .....	9
6.5	TSA-OI's Business Requirements of Secure Flight, TSA OTSR, and/or TTAC Vetting Operations .....	9
6.6	TTAC Vetting Operations's Business Requirements of Secure Flight, TSA OTSR, and/or TSA-OI .....	9
7	Process Overview .....	10

**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 by 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 Document Purpose

The purpose of this document is to define the business-level requirements for the Secure Flight/TSA Office of Transportation Security Redress (TSA OTSR)/TSA Office of Intelligence (TSA-OI)/TTAC Vetting Operations relationship as needed to support the Secure Flight program's Cleared List capability.

## 2 Document Scope

This document will capture Secure Flight's requirements of TSA OTSR, TSA-OI, and TTAC Vetting Operations as well as TSA-OI's, TSA OTSR's, and TTAC Vetting Operations' requirements of each other and of Secure Flight. This document focuses on the requirements for Secure Flight's current operating capability.

## 3 Document Organization

This document is structured as follows:

- Section 4 (Organizational Overview) provides an overview of Secure Flight, TSA OTSR, TSA-OI, and TTAC Vetting Operations organizations, focusing on each organization's role regarding the creation, maintenance, and distribution of the Cleared List.
- Section 5 (Relationship Overview) provides additional context to the Secure Flight/TSA OTSR/TSA-OI/TTAC Vetting Operations relationship by defining the capabilities and attributes that will be enabled via the Business Requirements defined in Section 6.
- Section 6 (Business Requirements) provides: (1) the requirements that Secure Flight has of TSA OTSR, TSA-OI, and TTAC Vetting Operations; (2) the requirements that TSA OTSR has of Secure Flight, TSA-OI, and TTAC Vetting Operations; (3) the requirements that TSA-OI has of Secure Flight, TSA OTSR, and TTAC Vetting Operations; and (4) the requirements that TTAC Vetting Operations has of Secure Flight, TSA OTSR, and TSA-OI.

## 4 Organizational Overview

### 4.1 Secure Flight Overview

Prior to the implementation of Secure Flight, aircraft operators each conducted their own matching processes in order to identify certain known and suspected terrorists. Because

*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.



each aircraft operator conducted its own matching process, the ability to conduct watch list matching and coordinate law enforcement responses was not consistent across the aviation industry.

The 9/11 Commission recommended that, "Improved use of 'No Fly' and 'Selectee' lists should not be delayed. This screening function should be performed by TSA, and it should utilize the larger set of watch lists maintained by TSA and other government entities." In Q1 FY05, TSA developed the Secure Flight program as a watch list matching solution to fulfill the Congressional mandate to pre-screen passengers against the terrorist watch list.

The May 25, 2010 White House Deputies Committee determined that TSA should match passengers against all records in the Terrorist Screening Database (TSDB) that have a full name and date of birth. Those TSDB records that have full name and date of birth that are not already on the No Fly and Selectee list are referred to herein as the Expanded Selectee List. Please note that the term "Expanded Selectee List" is one used by Secure Flight but does not represent an official subset of the TSDB.

Secure Flight has incorporated the Cleared List into its automated, manual review, and resolution processes to minimize the inconvenience that individuals could incur as a result of the pre-screening process. Having a Cleared List that is current, accurate, and thorough along with an efficient manner by which the general public can engage with the Department of Homeland Security's Traveler Redress Inquiry Program (DHS TRIP) reduces the risk that the Secure Flight program is perceived to be inconveniencing many innocent individuals.

#### 4.2 TSA OTSR Overview

TSA OTSR serves as the component agency responsible for managing DHS TRIP. DHS TRIP is the central processing point for redress inquiries from individuals who seek resolution regarding difficulties experienced during travel screening including denied or delayed airline boarding, denied or delayed entry into the United States, and repeated additional screening. DHS TRIP provides redress for transportation security programs including Secure Flight.

When a traveler applies for redress through DHS TRIP, a Redress Control Number is provided to the traveler. If appropriate, the traveler's information and Redress Control Number is added to the Cleared List. If the traveler is confirmed to match an entry on the No Fly, Selectee, or Expanded Selectee Lists, then the traveler's information is not added to the Cleared List.

**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.

#### 4.3 TSA-OI Overview

TSA-OI disseminates the Cleared List to TSA Secure Flight. Secure Flight receives all records for individuals who have met the TSA OTSR-based criteria for inclusion on the Cleared List. Secure Flight receives regular updates to the Cleared List from TSA-OI.

#### 4.4 TTAC Vetting Operations Overview

TTAC Vetting Operations serves as the lead for all security threat assessments and credentialing initiatives for transportation industry workers, individuals seeking access to critical infrastructure, and domestic passengers. TTAC Vetting Operations is responsible for the development and deployment of automated vetting systems which are used to vet populations including flight crews, hazardous materials crews, transportation workers, etc.

b)(3), 49 U.S.C. § 114(r)

### 5 Relationship Overview

The business-level requirements outlined in Section 6 are intended to enable the following attributes of the Cleared List capability as supported by the Secure Flight/TSA OTSR/TSA-OI/TTAC Vetting Operations relationship.

#### Provision of Cleared List to Secure Flight

The requirements in Section 6 define the provision of the Cleared List by TSA-OI to Secure Flight to support the Secure Flight mission. The requirements in Section 6 also ensure any suspected or known terrorists are rapidly removed from the Cleared List.

#### Retention of Cleared List Transmissions

The requirements in Section 6 define the retention of Cleared List transmissions from TSA-OI to Secure Flight. **Note:** This capability is needed for data integrity, reconciliation, audit, and oversight purposes.

#### Cleared List Currency and Integrity

The requirements in Section 6 define the assurance that the Cleared List that Secure Flight is using is of the utmost currency and integrity. The requirements also describe the vetting process conducted by TTAC Vetting Operations to

**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.

ensure that no known or suspected terrorists are placed on or remain on the Cleared List.

**Security and Privacy Compliance**

The requirements in Section 6 define the compliance to security and privacy regulations and standards.

**Service Level Agreement (SLA) Visibility**

The requirements in Section 6 define an SLA that Secure Flight (the customer) has agreed to with its service providers (TSA OTSR and TSA-OI). Secure Flight has a vested interest in the welfare of the DHS/TSA-level redress process as well as the timely receipt of the Cleared List.

## 6 Business Requirements

This section will list the organizations' business-level requirements of each other in support of the Secure Flight program's Cleared List capability.

### 6.1 Secure Flight's Business Requirements of TSA-OI

The following requirements represent the Secure Flight program's requirements of TSA-OI.

*Cleared List Transmission Requirements:*

- Secure Flight shall receive or have access to all Cleared List records (b)(3) 49 U.S.C. § 114(r)

(b)(3) 49 U.S.C. § 114(r)

*Cleared List Content Requirements:*

- Secure Flight shall receive the following data elements per Cleared List record:

- (b)(3) 49 U.S.C. § 114(r)
- 
- 
- 
- 
- 
- 
- 
- 
- 

- Secure Flight shall receive discreet New, Modify, or Delete identification for each Cleared List record.

**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.



*Transmission Retention Requirements:*

(b)(3) 49 U.S.C. § 114(r)

*Interface Security and Privacy Requirements:*

- The TSA-OI/Secure Flight interface shall meet all DHS and National Institute of Standards and Technology (NIST) security standards for user and data access control and system configuration rules.
- The TSA-OI/Secure Flight interface shall be consistent with all restrictions or conditions imposed by statute or other law, including privacy compliance requirements stated in the Privacy Impact Assessments (PIA) and System of Records Notices (SORN) for Secure Flight and DHS TRIP.
- The TSA-OI/Secure Flight interface shall possess a current Interim Authority to Operate (IATO)/Authority to Operate (ATO) from the TSA Chief Information Security Officer.

*Cleared List Metric & SLA Requirements:*

(b)(3) 49 U.S.C. § 114(r)

## 6.2 Secure Flight's Business Requirements of TSA OTSR

The following requirements represent the Secure Flight program's requirements of TSA OTSR.

*Cleared List Currency & Integrity Requirements:*

(b)(3) 49 U.S.C. § 114(r)

*Cleared List Metric & SLA Requirements:*

- On a monthly basis, Secure Flight shall receive (from TSA OTSR):
- The average redress application cycle time (from the receipt of a complete application to adjudication completion).
  - The number of aviation-related complete Redress applications received and (adjudication) completed.

## 6.3 Secure Flight's Business Requirements of TTAC Vetting Operations

The following requirements represent the Secure Flight program's requirements of TTAC Vetting Operations.

**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.

*Cleared List Transmission Requirements*

- TTAC Vetting Operations will notify Secure Flight and OTSR when a Cleared List entry is determined to be a match to an entry on the No Fly, Selectee, or Expanded Selectee Lists.

**6.4 TSA OTSR's Business Requirements of Secure Flight, TSA-OI, and/or TTAC Vetting Operations**

- TTAC Vetting Operations will vet Redress applicants against the No Fly and Selectee lists as well as the TSDB.

(b)(3) 49 U.S.C. § 114(r)

*Cleared List Metric & SLA Requirements:*

On a monthly basis, TSA OTSR shall receive:

- The number of Cleared List receipts from TSA OI to Secure Flight (from Secure Flight)
- The number of Expedite Cleared Updates received by Secure Flight (from Secure Flight)

**6.5 TSA-OI's Business Requirements of Secure Flight, TSA OTSR, and/or TTAC Vetting Operations**

- Secure Flight shall acknowledge successful receipt of each transmission of the Cleared List to TSA-OI.
- OTSR or TTAC Vetting Operations will update TSA-OI in the event that any Cleared List entries are determined to match an entry on the No Fly, Selectee, or Expanded Selectee Lists.

**6.6 TTAC Vetting Operations' Business Requirements of Secure Flight, TSA OTSR, and/or TSA-OI**

- TTAC Vetting Operations will receive regular updates to the Active and the Cleared List from OTSR.

**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 by 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.



- TTAC Vetting Operations will receive a separate file of all pending Redress applicants from OTSR.

## 7 Process Overview

The following steps outline the high-level processes that TTAC Vetting Operations, TSA OTSR, and TSA-OI will employ to provide Secure Flight with the Cleared List. **Note:** The DHS Traveler Redress Inquiry Program (DHS TRIP) has been added into the process flow below to allow for the understanding of how an individual (indirectly) interacts with the aforementioned entities.

### Process Redress Applications and Update Cleared List

1. An individual submits a redress application or inquiry to the DHS TRIP office.
2. DHS TRIP sends a confirmation and a unique redress number (for an application) to the individual when the application or inquiry has been received and is deemed complete.
3. DHS TRIP reviews the application or inquiry to determine to which DHS component agency the application or inquiry should be provided. The DHS component(s) will review the application and reach a determination about a traveler's status.
4. For those applications or inquiries determined to be related to No Fly, Selectee, and/or Expanded Selectee Lists (i.e. an aviation context), DHS TRIP forwards the application or inquiry to TSA OTSR.

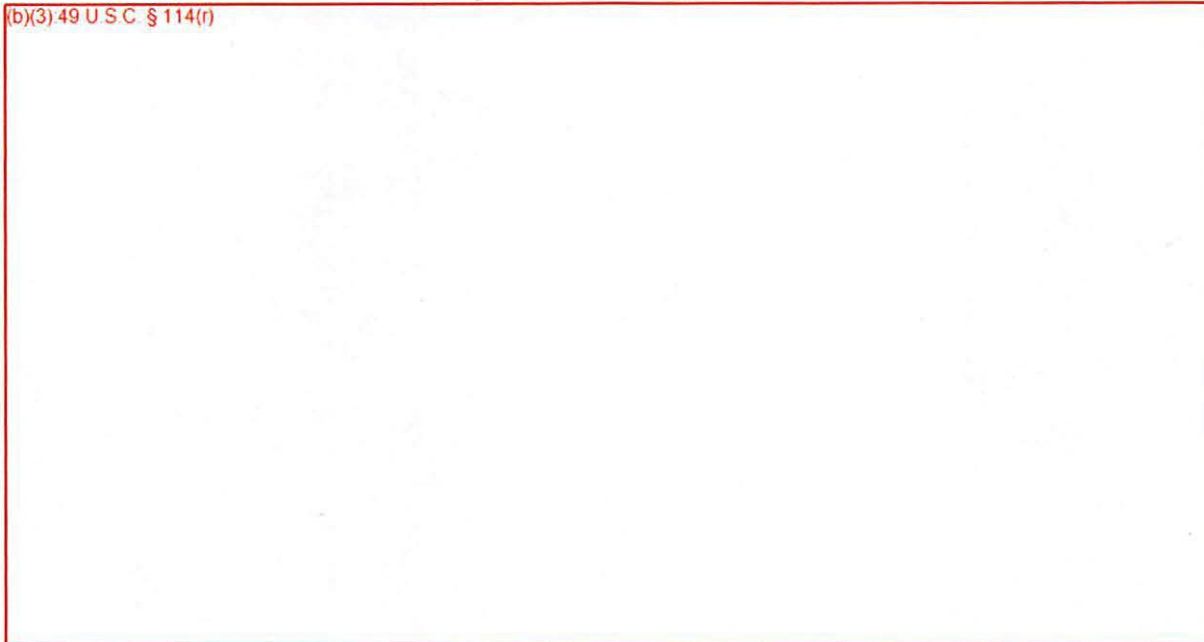
(b)(3) 49 U.S.C. § 114(r)

**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.



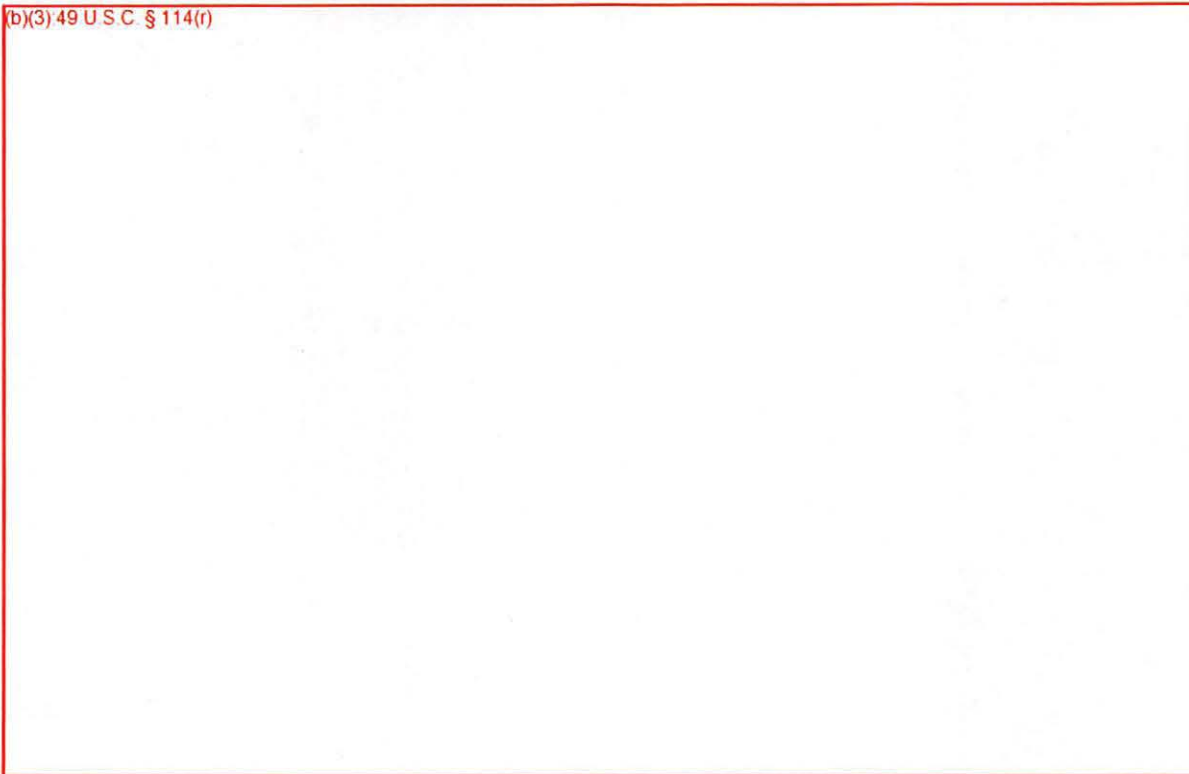
5. DHS TRIP sends a response letter to applicants.

(b)(3) 49 U.S.C. § 114(r)



**Provide Updated Cleared List to Secure Flight**

(b)(3) 49 U.S.C. § 114(r)



**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.

~~SENSITIVE SECURITY INFORMATION~~

**U.S. Department of Homeland Security  
Transportation Security Administration (TSA)**



**Transportation  
Security  
Administration**

**Office of Transportation Threat Assessment  
and Credentialing (TTAC)**

**Secure Flight Program**

**Secure Flight / TSA-OI (HQ) DNBL  
Business Requirements Document (BRD)**

**Version 2.0**

December 15, 2009

**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.

### Document Revision History

Date	Version	Modified By	Comments
5/20/2009	0.1	(b)(6)	(b)(5)
6/2/2009	0.2		
6/3/2009	0.3		
6/17/2009	1.0		
6/25/2009	1.0		
12/15/2009	2.0		

**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 of Contents

1	Document Purpose .....	4
2	Document Scope .....	4
3	Document Organization .....	4
4	Organizational Overview .....	5
4.1	Secure Flight Overview.....	5
4.2	TSA-OI Overview.....	5
5	Requirements Overview.....	6
6	Business Requirements .....	7
6.1	Secure Flight’s Business Requirements of TSA-OI.....	7
6.2	TSA-OI’s Business Requirements of Secure Flight.....	9
6.3	Additional Requirements.....	9
7	Process Overview.....	10
7.1	The DNBL Generation & Provision Process .....	10
7.2	The Secure Flight DNBL Matching & Manual Review Process .....	11
7.3	The Secure Flight DNBL Resolution Process.....	12
7.4	The Secure Flight DNBL Maintenance Process .....	14
Appendix A	Acronyms .....	15

**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 Document Purpose

The purpose of this Business Requirements Document (BRD) is to define the business-level requirements for the Secure Flight/Transportation Security Administration Office of Intelligence – Head Quarters (TSA-OI (HQ)) relationship as needed to support the Secure Flight program matching against the Center for Disease Control’s (CDC) “Do Not Board List” (DNBL).

## 2 Document Scope

This BRD will capture Secure Flight’s requirements of TSA-OI (HQ) as well as TSA-OI (HQ)’s requirements of Secure Flight specific to the Secure Flight DNBL process.

This BRD documents the current process which resulted from a Tuesday, November 24, 2009 meeting between Secure Flight and TSA-OI (HQ). It is considered a “living” document due to the changes to this process that will occur periodically over the next several months as additional aircraft operators move to Secure Flight operations. It is expected that full aircraft operator cut-over could take up to 18 months to complete, at which time the TSA-OI (HQ) will no longer be in any of the processes currently defined in this document. Secure Flight will continue to work towards a final process. If/when a change(s) occur, this BRD will be updated to reflect those changes

## 3 Document Organization

This document is structured as follows:

- Section 4 (Organizational Overview) provides an overview of the Secure Flight and TSA-OI (HQ) organizations.
- Section 5 (Requirements Overview) provides additional context to the Secure Flight/TSA-OI (HQ) relationship by introducing and defining the types of requirements that are defined in Section 6 (Business Requirements).
- Section 6 (Business Requirements) provides:
  - Secure Flight’s Requirements of TSA-OI (HQ) (Section 6.1)
  - TSA-OI (HQ)’s Requirements of Secure Flight (Section 6.2)
  - Additional Requirements (Section 6.3)

**Note:** The business requirements defined in Section 6 are specific to the Secure Flight DNBL matching process.
- Section 7 (Process Overview) provides detail on the Secure Flight-based DNBL matching processes.
  - The DNBL Generation and Provision Process (Section 7.1)

**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.

- o The Secure Flight DNBL Matching and Manual Review Process (Section 7.2)
- o The Secure Flight DNBI Resolution Process (Section 7.3)
- o The Secure Flight DNBL Reconciliation Process (Section 7.4)

## 4 Organizational Overview

### 4.1 Secure Flight Overview

Under current, post-9/11 practices and pursuant to TSA Security Directives, aircraft operators comply with these directives through various methods of matching passenger information to the No Fly and Selectee Lists provided by TSA. Because each aircraft operator conducts its own matching process, the ability to conduct watch list matching and coordinate law enforcement responses is not consistent across the aviation industry.

The 9/11 Commission recommended that, "Improved use of 'No Fly' and 'Selectee' lists should not be delayed. This screening function should be performed by TSA, and it should utilize the larger set of watch lists maintained by TSA and other government entities. Aircraft operators should be required to supply the information needed to test and implement this new system." In Q1 FY05, TSA developed the Secure Flight program as a watch list matching solution to fulfill the Congressional mandate to pre-screen passengers against the terrorist watch list.

The Department of Homeland Security Screening Coordination Office (DHS SCO) stated that Secure Flight should begin matching against the DNBL. After further review, TSA Senior Management (Gail Rossides, Greg Wellen, and Keith Kauffman) agreed on Thursday, May 7, 2009 that Secure Flight should begin this process.

### 4.2 TSA-OI (HQ) Overview

Currently, the TSA-OI (HQ)'s Indication and Warning Division is charged with assisting aircraft operators in determining the travel status of all passengers for domestic and international flights that fly into U.S. airspace. The aircraft operators call TSA-OI (HQ)'s Watch center to determine if a person is a match to the Terrorist Screening Center's (TSC) No-Fly and Selectee list. The Office of Intelligence has performed this function since post 9/11 pursuant to TSA Security Directives and Emergency Amendments.

The TSA-OI (HQ) provides threat assessments, security briefings, and intelligence tools that support TSA's 55,000 strong workforce. TSA-OI (HQ)'s focus is not only aviation, but all modes of transportation throughout the United States and abroad. TSA-OI (HQ)

**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.



will continue to work with the aircraft operators until Secure Flight is fully implemented which could take up to 18 months.

TSA-OI (HQ) processes and facilitates the addition of individuals determined to be a public health risk by the CDC. The U.S. Government considers the following diseases for the DNBL: cholera, diphtheria, infectious tuberculosis, plague, smallpox, yellow fever, and viral hemorrhagic fevers, such as Marburg, Ebola and Congo-Crimean, Severe Acute Respiratory Syndrome, and influenza caused by novel or re-emergent influenza viruses that are causing or have the potential to cause a pandemic. The CDC submits DNBL requests to the DHS Health and Human Services (HHS) branch and is then approved by the DHS Chief Medical Officer. Once approved, the request is forwarded to the Transportation Security Operations Center (TSOC) Command Duty Officer (CDO). TSA-OI (HQ) confirms the addition has been approved by TSA Senior Leadership.

## 5 Requirements Overview

The business-level requirements outlined in Section 6 are intended to enable the following attributes of the Secure Flight DNBL matching capability as supported by the Secure Flight / TSA-OI (HQ) relationship.

*Secure Flight's Business Requirements of TSA-OI (HQ) (Section 6.1):*

### **DNBL Provision Requirements**

These requirements in Section 6.1 define the provision of DNBL updates by the TSA-OI (HQ) Watch to Secure Flight.

### **DNBL Content Requirements**

These requirements in Section 6.1 define the data contents that the TSA-OI (HQ) Watch must provide Secure Flight with for each DNBL update.

### **DNBL Content Validation Handling Requirements**

These requirements in Section 6.1 define the validation that Secure Flight will perform on the DNBL update so as to ensure the ingested DNBL data is current, accurate, and thorough.

### **DNBL SID Assignment Requirements**

These requirements will ensure that the SIDs used by Secure Flight and TSA-OI (HQ) will remain in synch.

### **DNBL Retention Requirements**

These requirements in Section 6.1 define the retention of DNBL updates from the TSA-OI (HQ) Watch to Secure Flight. **Note:** This is needed for data integrity, reconciliation, audit, and oversight purposes.

**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.

**DNBL Currency and Integrity Requirements**

These requirements in Section 6.1 define the assurances that Secure Flight and TSA-OI (HQ) will take to ensure the DNBL record set that both organizations (i.e., Secure Flight and TSA-OI (HQ)) have are of the utmost currency and integrity.

*TSA-OI (HQ)'s Business Requirements of Secure Flight (Section 6.2):*

**DNBL Content Requirements**

These requirements in Section 6.2 define the data contents that Secure Flight must provide TSA-OI (HQ) Watch with for each DNBL update.

**DNBL Provision Acknowledgement Requirements**

These requirements in Section 6.2 define the acknowledgements that Secure Flight must provide back to the TSA-OI (HQ) Watch after the TSA-OI (HQ) Watch sends a DNBL update to Secure Flight.

## 6 Business Requirements

This section will list the organizations' business-level requirements of each other in support of the Secure Flight program's DNBL matching capability.

### 6.1 Secure Flight's Business Requirements of TSA-OI (HQ)

The following are Secure Flight's requirements of TSA-OI (HQ).

*DNBL Provision Requirements:*

(b)(3) 49 U.S.C. § 114(r)

**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.

(b)(3) 49 U.S.C. § 114(r)

- The TSA-OI (HQ) Watch shall provide TSA-OI (Secure Flight) with the following DNBL data contents for **Modify or Delete** DNBL updates:

(b)(3) 49 U.S.C. § 114(r)

*DNBL Content Validation Handling Requirements*

- TSA-OI (Secure Flight) will validate the DNBL updates against the following rules:

DNBL Validation Rule	Handling (If Violated)
(b)(3) 49 U.S.C. § 114(r)	

*DNBL SID Assignment Requirements:*

(b)(3) 49 U.S.C. § 114(r)

*DNBL Retention Requirements:*

**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.



- The TSA-OI (HQ) IIS shall retain a copy of all DNBL updates that were sent to Secure Flight (consistent with TSA-OI (HQ) IIS data retention regulations).  
**Note:** Saved copies of the Secure Flight-forwarded TSOC email are sufficient to meet this requirement.

*DNBL Currency and Integrity Requirements:*

(b)(3) 49 U.S.C. § 114(r)

## 6.2 TSA-OI (HQ)'s Business Requirements of Secure Flight

The following are TSA-OI (HQ)'s requirements of Secure Flight.

*DNBL Content Requirements:*

(b)(3) 49 U.S.C. § 114(r)

*DNBL Provision Acknowledgement Requirements*

(b)(3) 49 U.S.C. § 114(r)

## 6.3 Additional Requirements

The following requirements represent additional requirements of the Secure Flight / TSA-OI (HQ) relationship related to the Secure Flight DNBL matching process. These requirements are not included in Section 6.1 or 6.2 because they do not necessarily represent Secure Flight requirements of TSA-OI (HQ) or TSA-OI (HQ)'s requirements of Secure Flight. Rather, they are broader requirements of the Secure Flight / TSA-OI (HQ) DNBL relationship as a whole.

*DNBL Security and Privacy Compliance Requirements:*

**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.

- The TSA-OI (HQ) / Secure Flight interface shall meet all DHS and National Institute of Standards and Technology (NIST) security standards for user and data access control and system configuration rules.
- The TSA-OI (HQ) / Secure Flight interface shall be consistent with all restrictions or conditions imposed by statute or other law, including privacy compliance requirements stated in the Privacy Impact Assessments (PIA) and System of Records Notices (SORN) for Secure Flight and TSA-OI (HQ).

*DNBL Performance Requirements:*

- Secure Flight (OSD) shall update the Secure Flight system and provide a disposition acknowledgement (b)(3) 49 U.S.C. § 114(r)

(b)(3) 49 U.S.C. § 114(r)

## 7 Process Overview

The Secure Flight DNBL end-to-end matching process is comprised of four (4) sub-processes. The four sub-processes are:

- The DNBL Generation and Provision Process (Section 7.1)
- The Secure Flight DNBL Matching and Manual Review Process (Section 7.2)
- The Secure Flight DNBL Resolution Process (Section 7.3)
- The Secure Flight DNBL Reconciliation Process (Section 7.4)

### 7.1 The DNBL Generation & Provision Process

This process refers to how the DNBL is generated and subsequently provided to the Secure Flight program (so that Secure Flight can perform the matching function). For purposes of this document, only the primary flows have been included. Alternative flows will be created during the detailed requirements phase. **Note:** While Steps 1-8 of this process are not part of the Secure Flight program, they have been included to provide context to the broader end-to-end process. Steps 1-8 have been italicized for ease of identification below.

- 1 The local public health center identifies someone with a health threat to the public and contacts CDC Headquarters.*
- 2 The CDC determines that an individual needs to be added to, modified, or removed from the DNBL.*
- 3 The CDC provides the DHS Network Operations Center (NOC) with the individual (and associated identifiers) to be added to, modified, or removed from the DNBL.*
- 4 The DHS NOC contacts the DHS Chief Medical Officer to determine if DHS agrees with CDC's request.*

**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 The DHS NOC Watch officer contacts the TSOC with the DNBL add / modify / removal update.

(b)(3) 49 U.S.C. § 114(r)



16 This process ends.

## 7.2 The Secure Flight DNBL Matching & Manual Review Process

This process refers to how Secure Flight will match Secure Flight Passenger Data (SFPD) against the DNBL. This process includes both the automated matching component as well as the manual review and resolution processes, if required. For purposes of this document, only the primary flows have been included. Alternative flows will be created during the Secure Flight detailed requirements phase.

- 1 The aircraft operator submits SFPD to Secure Flight up to 72 hours prior to the passenger's flight.
- 2 The Secure Flight system matches the SFPD against the No Fly, Selectee, Cleared List, and DNBL as defined in the Secure Flight requirements document, "Aircraft Operator Requests BPPR.doc".

**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. If the Secure Flight system does not find a possible match on the DNBL, the Secure Flight system will return a "Cleared" Boarding Pass Printing Result (assuming no matches were found on the No Fly and Selectee Lists). *The DNBL Matching Process Ends*
- b. If the Secure Flight system finds a possible match on the DNBL, the Secure Flight system will return an "Inhibited" Boarding Pass Printing Result to the submitting aircraft operator.
- c. The Secure Flight system will not attempt to match the DNBL conflict matches against the Cleared list.



- 6 This process ends (i.e., it continues with the Secure Flight DNBL Resolution Process below).

### 7.3 The Secure Flight DNBL Resolution Process

This process refers to how the Secure Flight system will be updated after the appropriate operational entities (e.g., TSOC, Federal Security Director (FSD), etc) respond to a possible DNBL match attempting to check-in at the departure airport of his/her first flight segment. For purposes of this document, only the primary flows have been included. Alternative flows will be created during the detailed Secure Flight requirements phase.



**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.



#### 7.4 The Secure Flight DNBL Maintenance Process

This process refers to how Secure Flight and TSA-OI (HQ) Watch will verify on a recurring basis that Secure Flight and TSA-OI (HQ) Watch are using the most accurate DNBL within their respective processes.

1. (b)(3)49 U.S.C. § 114(r) TSA-OI (HQ)-IIS and Secure Flight will share their DNBL "lists" with each other to ensure that Secure Flight and TSA-OI (HQ) Watch are using the most accurate DNBL within their respective processes.
  - a. If no abnormalities are found, all parties will acknowledge as such.
  - b. If abnormalities are found (e.g., TSA-OI (HQ) Watch has x number of individuals on the list, but Secure Flight has a different number of individuals on the list), TSA-OI (HQ) and Secure Flight will work together to reconcile and correct their lists, as appropriate.

**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.



**Appendix A Acronyms**

Acronyms	Description
BRD	Business Requirements Document
CDC	Center for Disease Control
CDO	Command Duty Officer
CSA	Customer Support Agent
DHS	Department of Homeland Security
DNBL	Do Not Board List
DOB	Date of Birth
FSD	Federal Security Directive
HHS	Health and Human Services
IT	Information Technology
LEO	Law Enforcement Officer
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
OI	Office of Intelligence
PIA	Privacy Impact Assessments
POC	Point of Contact
RFA	Refer for Action
SCO	Screening Coordination Office
SD	Security Directive
SFA	Secure Flight Analyst
TSA-OI (HQ)	Transportation Security Administration Office of Intelligence – Head Quarters
TSA-OI (HQ) IIS	[TSA-OI (HQ)] Intelligence Information Systems
TSA-OI (Secure Flight)	Transportation Security Administration Office of Intelligence – Secure Flight
TSOC	Transportation Security Operations Center

**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.

**U.S. Department of Homeland Security  
Transportation Security Administration**



**Transportation  
Security  
Administration**

**Office of Intelligence and Analysis (OIA)**

**Interface Control Document**

**Between**

**Secure Flight Program**

**and**

**Office of Security Operations**

**Version 0.7**

**June 4, 2012**

## Revision History

Revision Date	Version	Description	Modified By
February 29, 2012	0.1	(b)(5)	(b)(6)
March 19, 2012	0.2		
March 26, 2012	0.3		
March 27, 2012	0.4		
March 27, 2012	0.5		
March 30, 2012	0.6		
June 4, 2012	0.7		



## Table of Contents

<b>1</b>	<b>INTRODUCTION .....</b>	<b>1</b>
1.1	Scope.....	1
1.2	Document Overview .....	1
1.3	Reference Documentation.....	1
<b>2</b>	<b>SYSTEM DESCRIPTION .....</b>	<b>2</b>
2.1	Interface Overview .....	2
2.2	Functional Allocation .....	2
2.3	File Transfer .....	2
2.4	Transactions.....	3
2.5	Security and Integrity.....	3
2.6	Key Contacts .....	3
<b>3</b>	<b>DETAILED INTERFACE REQUIREMENTS.....</b>	<b>4</b>
3.1	Interface Requirements .....	4
3.2	File Requirements .....	4
3.3	Frequency .....	4
3.4	Data Validation Requirements.....	5
3.5	Messaging .....	5
3.6	Error Handling.....	5
<b>4</b>	<b>COMMUNICATIONS PROCEDURES.....</b>	<b>6</b>
4.1	Planned Outage Procedures .....	6
4.2	Unplanned Outage Procedures .....	6
4.3	Change Management Procedures .....	6
<b>5</b>	<b>TIMELINE .....</b>	<b>6</b>
<b>6</b>	<b>SIGNATORY AUTHORITY.....</b>	<b>7</b>

# 1 Introduction

## 1.1 Scope

The Transportation Security Administration's (TSA) Office of Intelligence and Analysis (OIA) Secure Flight program conducts watch list matching of airline passenger data to Federal government watch lists for international and domestic flights. Matching requests are initiated by covered airlines and are either entered directly into a Secure Flight interface or sent from reservation or departure control systems (DCS) through the Department of Homeland Security (DHS) router, which then transmits the passenger data to Secure Flight.

While not the creator (system of record) of any watch list, Secure Flight must receive, process, and reconcile (ensure Secure Flight watch list data is an accurate mirror of the source system data) data from list providers in order to meet its mission of passenger vetting.

The scope of this Interface Control Document (ICD) is to describe the interface specification for Secure Flight to receive and reconcile watch list data from Office of Security Operations (OSO), herein referred to as the list provider. The watch list data covered by this document is the Pre ✓ Disqualification Protocol (PDP).

## 1.2 Document Overview

This document contains design specifications to define the interface between the list provider and Secure Flight. This document will provide a description of the processes, messages, and validation rules used to exchange information between these entities.

## 1.3 Reference Documentation

The table below lists the reference documents used during the creation of this document.

Document	Description

## 2 System Description

### 2.1 Interface Overview

The interface between Secure Flight and the list provider used to receive and reconcile watch list data will not be automated. An automated interface is planned for a future release.

### 2.2 Functional Allocation

The interface between the list provider and Secure Flight will be a manual file transfer via a shared folder on the TSA network. The shared folder will be utilized as the secure medium for the list provider to post list updates. Secure Flight will access and download the list update and send an acknowledgement to the list provider.

### 2.3 File Transfer

The list provider will create a file containing all Secure Flight applicable records, encrypt it using the current TSA password, and post it to the shared folder. Once posted, the list provider will send an email to (b)(3)49 U.S.C. § 114(r) to notify Secure Flight a new version of the list is available. When notified, Secure Flight will access the shared folder to download and validate the posted file. When downloaded, Secure Flight will send an email notification to the list provider indicating the status of the download.

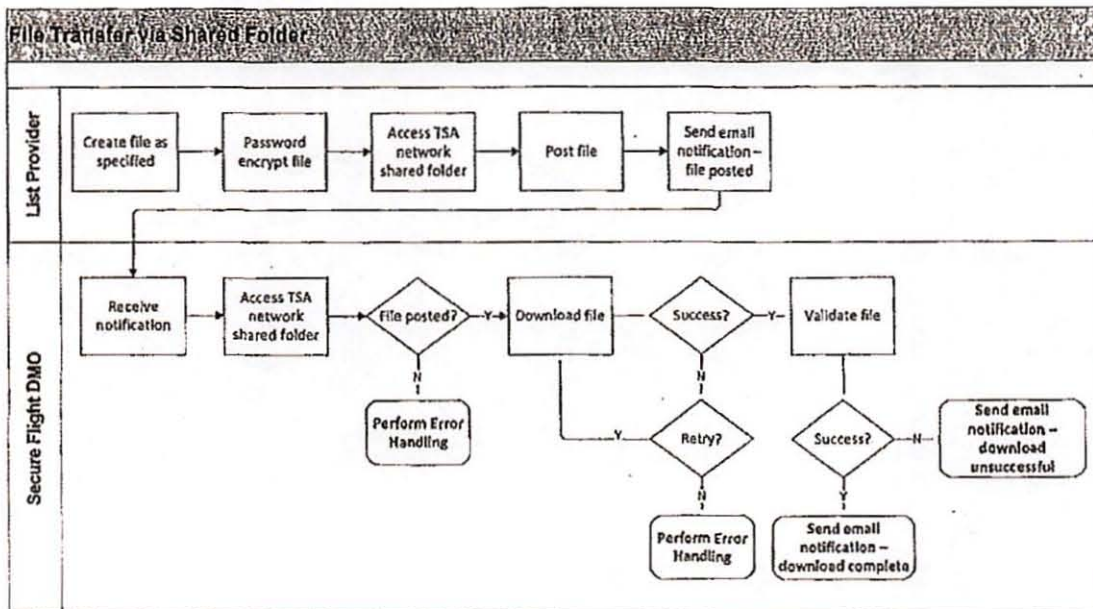


Figure 1: File Transfer via Shared Folder Process Flow



## 2.4 Transactions

List providers must be able to support the following transaction types, which are supported by the manual file transfer.

**Table 1: List Update Transaction Types**

Transaction Type	Comments
Entire List	Consists of <i>all</i> Secure Flight applicable records (not to exceed 50,000 records) in the source system

## 2.5 Security and Integrity

The TSA shared network folder inherits the TSA network security, which provides for data privacy and security.

Files posted to a TSA shared network folder must be encrypted or password protected.

## 2.6 Key Contacts

The following defines the ownership and key contacts for the subject interface.

**Table 2: Key Contacts**

Organization	Role	Name	Contact Information
Secure Flight	Operations Manager	(b)(6)	(b)(6);(b)(3);49 U.S.C. § 114(r)
Secure Flight	Data Management Organization (DMO)		
Secure Flight	Operational Services Division (OSD)	Any	
OSO PARIS	System Owner	Frederick P Falcone	
OSO PARIS	ISSO	(b)(6)	
OSO PARIS	Program Manager		
OSO PARIS	Resource Center	Watch Person	

### 3 Detailed Interface Requirements

#### 3.1 Interface Requirements

The interface between the list provider and Secure Flight will not be automated. The list provider and Secure Flight will utilize the following shared TSA network folder to submit and receive updated lists -

\\tsahqf001.network.ad.tsa.gov\tsa\TSASharedFolders\Secureflight\List\PDP.

The following sections specify the details for this interface (NOTE: An automated interface is planned for a future release).

#### 3.2 File Requirements

The list provider will export a file from their source system for each transaction type as agreed. The file must be comma separated value (CSV) format. Table 3 below defines the content required in each file. The file should be named as follows: PDP List\_[YYYYMMDD].

**Table 3: Required File Content**

File Id	Mandatory?	Expected Format	Comments/ Acceptable Values
---------	------------	-----------------	--------------------------------

(b)(3) 49 U.S.C. § 114(r)

#### 3.3 Frequency

The list provider will post the file as described in Section 3.2 (b)(3) 49 U.S.C. § 114(r)

(b)(3) 49 U.S.C. § 114(r)

Posts will be stored on the shared network folder for a period of 7 days. The list provider is responsible for managing retention of posts as defined.

### 3.4 Data Validation Requirements

Secure Flight will validate the file per the requirements identified in Section 3.2.

### 3.5 Messaging

When posted, the list provider will send email notifications to [OIA.SecureFlight.Data@tsa.dhs.gov](mailto:OIA.SecureFlight.Data@tsa.dhs.gov).

Upon completion (or attempt) to download the file, Secure Flight personnel will send an email notification to the list provider (to [PARIS@tsa.dhs.gov](mailto:PARIS@tsa.dhs.gov) and [ComplianceAnalysis@tsa.dhs.gov](mailto:ComplianceAnalysis@tsa.dhs.gov)) indicating the disposition of the download attempt.

### 3.6 Error Handling

Impacted Team	Scenario	Handling
List Provider	(b)(3) 49 U.S.C. § 114(r)	(b)(3) 49 U.S.C. § 114(r)
Secure Flight		Contact PARIS Resource Center Phone at 571-227-5590.
Secure Flight		Contact PARIS Resource Center Phone at 571-227-5590.
Secure Flight		As part of the email notification back to the list provider once the file is downloaded, indicate the download was unsuccessful and the error encountered. Request a "re-post".
Secure Flight		As part of the email notification back to the list provider once the file is downloaded, indicate the download was unsuccessful and the error encountered. Request a "re-post".
Secure Flight		As part of the email notification back to the list provider once the file is downloaded, indicate the download was unsuccessful and the error encountered, identifying the impacted records. Request a "re-post" of the impacted records.



## 4 Communications Procedures

### 4.1 Planned Outage Procedures

When the list provider has a planned outage (e.g., maintenance window), they should contact Secure Flight personnel at (b)(3) 49 U.S.C. § 114(r) to communicate the planned outage.

### 4.2 Unplanned Outage Procedures

When the list provider encounters unplanned outage, they should contact Secure Flight personnel at (b)(3) 49 U.S.C. § 114(r) to communicate the recovery steps and actions to be taken.

### 4.3 Change Management Procedures

When either entity requires changes to this agreement that impacts the interface, they must contact the other party for approval.

## 5 Timeline

This ICD shall be in effect upon the date of signing. This ICD is valid for the duration of the list provider Authority to Operate (ATO) granted at the time of the latest date on either signature in section 6 of this document. At that time it must be reviewed, updated, and reauthorized. If the parties wish to extend this agreement, they may do so by reviewing, updating, and reauthorizing this agreement. The newly signed agreement should explicitly supersede this agreement and will be referenced by title and date.

This ICD will be reviewed annually at a minimum to coincide with the annual self assessment or whenever a significant change occurs. This ICD shall remain in effect until modified, superseded, or canceled by either party by written notification. To ensure continuity of operations, it is agreed that any modifications to this ICD will be provided in writing thirty (30) days in advance.

## 6 Signatory Authority

I agree to the terms of this Interface Control Document

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Date)

Name (b)(6)

Secure Flight

**Frederick P. Falcone**

Digitally signed by Frederick P. Falcone  
DN: cn=Frederick P. Falcone, o=Compliance,  
ou=QSO, email=(b)(6), c=US  
Date: 2012.06.19 09:49:10 -04'00'

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Date)

Frederick P Falcone  
PARIS System Owner

## 6 Signatory Authority

I agree to the terms of this Interface Control Document

(b)(6)

[Redacted Signature]

(Signature)

06/19/2012

(Date)

Name (b)(6)

Secure Flight

Frederick P. Falcone

Digitally signed by Frederick P. Falcone  
DN: cn=Frederick P. Falcone, o=Compliance,  
ou=OSO, email=(b)(6)=US  
Date: 2012.06.19 09:49:10 -04'00'

(Signature)

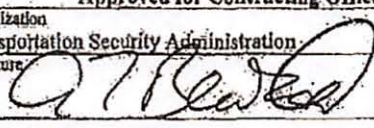
(Date)

Frederick P Falcone  
PARIS System Owner



Bar Code

**U.S. Department of Homeland Security  
Reimbursement Agreement Between Agencies**

Parties to the Agreement:						
Provider Agency				Customer Agency		
Provider Cost Center	RCN	RCN Description		Customer Contact	Phone	
Provider Contact (b)(6)		Phone 703-553-(b)(6)		TSA Contracting Officer: A.T. Bewick 571-227-(b)(6)		
Customer Number	Customer Alias		HSTS02-10-X-DAD007			
Provider Name OIT/TASPO Office of Information & Technology, U.S. Customs & Border Protection				Customer Name (if billing address is different, specify on reverse side) Department of Homeland Security (DHS)/ Transportation Security Administration (TSA)		
Address				Address 601 South 12 <sup>th</sup> Street- TSA-25		
City	State	Zip		City Arlington	State VA	Zip 22202
Duration:						
This agreement shall become effective on: 12/25/09			and shall continue through		09/30/2011	
Provide the Following Services or Goods:						
<i>Brief explanation of work or services to be performed and basis for determining cost:</i>						
The purpose of this agreement is utilize to provide Customs Border Patrol specialized programmers and computers system access resources to the Office of Intelligence/Front Office.						
(Attach additional sheet for continuation of explanation, (if necessary))				Fund Certification (Signature and Date)		Estimated Amount \$500,000.00
Customer Financing:						
<i>(Customer agency will indicate accounting data to be charged by completing applicable blocks. Federal agencies will be billed by OPAC, except for billings among the OBD's and USAS, billings within an organization, and billings to the Department of Defense.)</i>						
Agency Location Code 70-11-00-01	Appropriation Symbol See Below	AFC	PB	Cost Center	Document No. See Below	Obl Month
						Obl SOC
						Pay SOC
Other Accounting Information (Where applicable, multiple Obligation Month and SOC data should be identified in this block. Customers not using the FMIS may use this block to describe unique data required for their accounting systems.) SEE 2 <sup>ND</sup> PAGE						
Approvals:						
(See reverse side of form.)						
Approved for Provider Office:				Approved for Contracting Officer:		
Organization CBP				Organization Transportation Security Administration		
(b)(6)				Signature 		
(b)(6)				Title A.T. Bewick Contracting Officer		

\*When intrafund billing data are manually submitted to the billing office, the Provider Intrafund Data block on the reverse side must be completed by the provider of the goods or service.

DHS Form 07(0-1)  
Rev. June 2003

Provider Intrafund Data (For crediting revenues to the Provider)			
Document No. HSTS02-10-X-DAD007	Obligation Month 04/10	Obligation SOG	Payment SOG
Other Accounting Information (Where applicable, multiple Obligation Month and SOG data should be identified in this block.)			

Billing Address		
Name United States Coast Guard Finance Center/TSA Interagency Agreements		
Address P.O. Box 4112		
City Chesapeake	State VA	Zip 23326-4112
Contact Customer Service	Phone 757-523-6940	

#### Conditions of Agreement

1. Financing:

The charges for services shall include both direct and indirect costs applicable to the agreement. Advance payments are made on an estimated cost basis. If the estimated advance is different from the actual costs, proper adjustment (refund or additional billing) on the basis of the actual costs incurred shall be made upon completion of the work. (The frequency of billing, such as monthly, quarterly, etc., must be stated in the narrative portion of the form.)

2. Other Provisions:

Funding allocations:

5TS101A000D2010HQA010GE00077005090500DAD-54000000000000-253D-TSA DIRECT-DEF. TASK-D

**Interagency Agreement  
HSTS02-10-X-DAD007**

Between the  
Transportation Security Administration  
And the  
U.S. Customs and Border Protection

**PART A – General Terms & Conditions**

**A.1. Purpose**

This Part of the IA (hereinafter "Part A") describes the terms and conditions that govern the provision of acquisition assistance between the Transportation Security Administration; hereinafter "the Requesting Agency" and U.S. Customs and Border Protection hereinafter "the Servicing Agency."

No fiscal obligations are created through the execution of Part A. A fiscal obligation arises when the Transportation Security Administration demonstrates a bona fide need, provides the necessary requirements and funding information to the Servicing Agency and both parties execute a funding document using Part B of this IA or an alternate funding document.

**A.2. Authority**

The parties' authority to enter into this interagency agreement is (check applicable box):

The Aviation and Transportation Security Act (ATSA), Public Law 107-71

The Economy Act (31 U.S.C. 1535)

Franchise Fund (e.g., 31 U.S.C. 501 note) or Revolving Fund (e.g., 40 U.S.C. 321)

Identify specific statutory authority \_\_\_\_\_

Other (Identify specific statutory authority or authorities)

*As noted in DHS Management Directive 125-02, "Interagency Agreements," issued August 15, 2008, an Interagency agreement must cite a statute upon which the agreement is based. Each Interagency agreement may rely upon only one statute. This means that an Interagency Agreement should cite the Economy Act only when a more specific authority is not available.*

---



**A.3. Part A Identifier**

**Insert the Procurement Request Number and IA number here in this table:**

<b>Procurement Request Number</b>	<b>2110200DAD007</b>
<b>Interagency Agreement Number</b>	<b>HSTS02-10-X-DAD007</b>

**A.4. Scope**

a. Organizations authorized to request acquisition assistance

The following organizations in the Transportation Security Administration are authorized to obtain assistance from the Servicing Agency. **Office of Intelligence, Deputy Administrator's Office.**

b. Organizations authorized to provide acquisition assistance

The organizations in the Servicing Agency are authorized to provide assistance to the Transportation Security Administration. **Passenger Systems Program Office, Office of Information Technology.**

c. Types of products or services that may be acquired

(b)(3) 49 U.S.C. § 114(r)

d. Limitations

The following restrictions apply: None

**A.5. Period of Agreement**

The terms and conditions described in Part A of the IA become effective when signed by authorized officials of both agencies and remain effective until 1 year from date of execution, unless amended in accordance with Section 11 or terminated in accordance with Section 12. The period may be extended by mutual agreement between the parties up to 5 years from the date of execution.

**A.6. Roles & Responsibilities of Servicing Agency & Transportation Security Administration**

The effective management and use of interagency contracts is a shared responsibility of the Transportation Security Administration and the Servicing Agency. The parties hereby agree to the following roles and responsibilities, which are derived from the Checklist in Appendix 1 of *Interagency Acquisitions*, guidance issued by the Office of Federal Procurement Policy.

TSA is responsible for providing:

(b)(3) 49 U.S.C. § 114(r)

CBP is responsible for providing:

(b)(3) 49 U.S.C. § 114(r)

#### **A.7. Billing & Payment**

The Transportation Security Administration will pay the Servicing Agency for costs of each contract or task/delivery order. Billings may include the amounts due under the contract or order plus any assisted service fees identified in Part B of this IA.

IPAC is the method of reimbursement to CBP for services performed under this IA.

TSA Agency Code: 7011001

Address for submission of invoices:

USCG Finance Center  
TSA Interagency Agreements  
PO Box 4112  
Chesapeake, VA 23327-4112  
Phone Number: 757-523-6940



The Transportation Security Administration shall be responsible for interest owed under the Prompt Payment Act except that the Servicing Agency shall be responsible for interest owed to the contractor due to delays created by actions of the Servicing Agency.

**A.8. Small Business Credit**

Any contract actions executed by the Servicing Agency on behalf of the Transportation Security Administration will allocate the socio-economic credit to the Transportation Security Administration at the lowest FIPS 95-2 Agency/Bureau component as identified by the Transportation Security Administration. If the code is not provided, the Servicing Agency will allocate the credit to the highest Transportation Security Administration FIPS 95-2 Code.

**A.9. Notification and Reporting**

For any contract actions executed by the Servicing Agency on behalf of the Transportation Security Administration (for "assisted acquisition"), the servicing agency will provide to the TSA Contracting Officer identified in this agreement, not less than four days prior to its planned award, information identifying the awarded contractor and official business address, amount and type of contract, the identities, official business addresses, and amounts and types of subcontract of all major subcontractors, so that the TSA can comply with Congressional and public notification requirements.

**A.10. Contract Termination, Disputes and Protests**

If a contract or order awarded pursuant to this IA is terminated or cancelled or a dispute or protest arises from specifications, solicitation, award, performance or termination of a contract, appropriate action will be taken in accordance with the terms of the contract and applicable laws and regulations. The Transportation Security Administration shall be responsible for all costs associated with termination, disputes, and protests, including settlement costs, except that the Transportation Security Administration shall not be responsible to the Servicing Agency for costs associated with actions that stem from errors in performing the responsibilities assigned to the Servicing Agency. The Servicing Agency shall consult with the Transportation Security Administration before agreeing to a settlement or payments to ensure that the Servicing Agency has adequate time in which to raise or address any fiscal or budgetary concerns arising from the proposed payment or settlement.

**A.11. Review of Part A**

The parties agree to review jointly the terms and conditions in Part A at least annually if the period of this agreement, as identified in Section 5, exceeds one year. Appropriate changes will be made by amendment to this agreement executed in accordance with Section 11. The parties further agree to review performance under this IA to determine if expectations are being met and document a summary of their assessment. The responsible reviewing official at each agency shall sign and date the assessment.

**A.12. Amendments**

Any amendments to the terms and conditions in Part A shall be made in writing and signed by both the Servicing Agency and the Transportation Security Administration.

**A.13. IA Termination**

This IA may be terminated upon thirty (30) calendar days written notice by either party. If this agreement is cancelled, any implementing contract/order may also be cancelled. If the IA is terminated, the agencies shall agree the terms of the termination, including costs attributable to each party and the disposition of awarded and pending actions.

If the Servicing Agency incurs costs due to the Transportation Security Administration's failure to give the requisite notice of its intent to terminate the IA, the Transportation Security Administration shall pay any actual costs incurred by the Servicing Agency as a result of the delay in notification, provided such costs are directly attributable to the failure to give notice.

**A.14. Interpretation of IA**

If the Servicing Agency and Transportation Security Administration are unable to agree about a material aspect of either Part A or Part B of the IA, the parties agree to engage in an effort to reach mutual agreement in the proper interpretation of this IA, including amendment of this IA, as necessary, by escalating the dispute within their respective organizations.

If a dispute related to funding remains unresolved for more than [60] calendar days after the parties have engaged in an escalation of the dispute, the parties agree to refer the matter to their respective Agency Chief Financial Officers with a recommendation that the parties submit the dispute to the CFO Council Intragovernmental Dispute Resolution Committee for review in accordance with Section VII of Attachment 1 to the Treasury Financial Manual, Volume 1, Bulletin No. 2007-03, Intragovernmental Transactions, Subject: Intragovernmental Business Rules, or subsequent guidance.

**A.15. Signatures**

TRANSPORTATION SECURITY ADMINISTRATION OFFICIAL:

Signature: A. T. Dewick Date: 8 June 2010

Name: A.T. DEWICK  
Title: Contracting Officer  
Agency: ISA  
Address: 701 S. 12th Street, YSA-25, Arlington, VA 22202  
Phone: 571-227-(b)(6)

CUSTOMS AND BORDER PROTECTION OFFICIAL:

Signature: (b)(6) Date: 6/29/10

Name: \_\_\_\_\_  
Title: CONTRACTING OFFICER  
Agency: CBP  
Address: 1300 PENNSYLVANIA AVE NW  
Phone: (b)(6)



**Model Interagency Agreement**  
**PART B – Requirements & Funding Information**

**B.1. Purpose**

This Part of the IA (hereinafter "Part B") serves as the funding document. It provides specific information on the requirements of [The Transportation Security Administration], hereinafter "the Requesting Agency" sufficient to demonstrate a bona fide need and identifies funds associated with the requirement to allow [U.S. Customs and Border Protection], hereinafter "the Servicing Agency," to provide acquisition assistance and conduct an interagency acquisition.

**B.2. Authority**

The parties' authority to enter into this interagency agreement is (check applicable box):

- The Economy Act (31 U.S.C. 1535)
- Franchise Fund (e.g., 31 U.S.C. 501 note) or Revolving Fund (e.g., 40 U.S.C. 321)
- Identify specific statutory authority The Aviation and Transportation Security Act (ATSA), Public Law 107-71
- Other (Identify specific statutory authority or authorities)

**B.3. Part B Identifier**

Insert common agreement number(s) to identify Part B on other documents.

**B.4. General Terms & Conditions**

Activities undertaken pursuant to this document are subject to the general terms and conditions set forth in Part A, HSTS02-10-X-DAD007.

**B.5. Project Title - Application development and maintenance services, project and security support services.**

**B.6. Description of Products or Services / Bona Fide Need**

TSA is using CBP computer programming capabilities (specialized programmers and computer systems—Automated Targeting System) to develop software that supports our (TSA's) screening mission. TSA has requested programming of CBP's computer systems to automate tasks that relate to TSA's aviation security mission. CBP has completed work on behalf of TSA, and in addition to this upfront computer programming, CBP has also configured their systems to provide TSA with metrics information and feedback regarding these tasks.

This is an ongoing requirement (there is not a "product" per se, but a continuing series of software refinements and feedback results to match TSA's needs. The cost is incurred in programmer time and overtime in supporting TSA's mission, as opposed to costs incurred supporting the CBP mission. The software modifications are customized for TSA, and therefore require additional computer programmer time and expertise beyond what CBP is using to accomplish their core mission.

**1.0 OVERVIEW AND BACKGROUND**

As per the attempted terrorist attack on December 25, 2009, the Transportation Security Administration (TSA) requires rule changes to the Automated Targeting System (ATS) to be performed by Customs and Border Protection (CBP)/ Targeting & Analysis Systems Program Office (TASPO).

**2.0 SCOPE OF WORK**

CBP has enhanced its security measures through the creation of new targeting rules, modifications of existing rules and by conducting intelligence driven special operations.

**3.0 PERIOD OF PERFORMANCE, LOCATION AND HOURS OF PERFORMANCE**

Location: Work required under this order shall be performed at the Government site.

**4.0 DELIVERABLES**

All deliverables are Data to be delivered in electronic format to the COTR. No other office automation product shall be used, unless approved by the Government.

## 5.0 GOVERNMENT FURNISHED RESOURCES

The Government will furnish the means for periodic updates as applicable.

## 6.0 TRAVEL AND OTHER DIRECT COSTS

No travel is anticipated in conjunction with this delivery order. However, should travel be necessary, all travel shall be in accordance with the Federal Travel Regulations (for travel in 48 contiguous states), the Joint Travel Regulations, DoD Civilian Personnel, Volume 2, Appendix A (for travel to Alaska, Hawaii, Puerto Rico, and U.S. territories and possessions), and if required by the SOW, the Standardized Regulations (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" (for travel not covered in the Federal Travel Regulations or Joint Travel Regulations).

The Government does not anticipate any Other Direct Costs (ODCs). In the event there is a requirement for ODCs, advance approval of the COTR is required.

## 7.0 CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE.

CBP COTR:

Name: Phil Landfried  
Address: 5971 Kingstowne Village Pkwy.  
5<sup>th</sup> floor mailroom  
Alexandria, Virginia 22315  
Tel. #: (b)(6)  
Fax #: (571) 468-1478  
Email: (b)(6)

## 8.0 SECURITY, PRIVACY AND DISCLOSURE OF INFORMATION.

### Privacy.

Since data processed at Customs and Border Protection may contain Privacy Act information, the Contractor must read, sign and adhere to appropriate nondisclosure requirements for Privacy Information.

### Disclosure of Information.

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this Task Order and shall not be



divulged or made known in any manner to any persons except as may be necessary in the performance of the Task Order.

The Contractor shall not use, disclose, or reproduce data, which bears a restrictive legend, other than as required in the performance of this task.

The Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor's responsible employees.

Each officer or employee of the Contractor or any of its Subcontractors to whom any Government records may be made available or disclosed, shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C 641. That section provides, in pertinent part, that whoever knowingly converts to their use or the use of another, or without authority, sells, conveys, or disposes of any record of the United States or whoever receives the same with intent to convert it to their use or gain, knowing it to have been converted, shall be guilty of a crime punishable by a fine up to \$10,000 or imprisoned up to ten years, or both.

"All services provided under this task order must be compliant with DHS Information Security Policy, identified in MD4300.1, *Information Technology Systems Security Program* and 4300A *Sensitive Systems Handbook*."

**OAST (Office on Accessible Systems and Technology) Compliance**  
**DHS Accessibility Requirements Tool (DART)**  
**Accessibility Requirements (Section 508 Compliance)**

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable standards have been identified:

36 CFR 1194.21 -- Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this

standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

**36 CFR 1194.31 – Functional Performance Criteria**, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

**36 CFR 1194.41 – Information Documentation and Support**, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required "1194.31 Functional Performance Criteria", they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply:

**36 CFR 1194.2(b) – (COTS/GOTS products)**, When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards.

When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires approval from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

**36 CFR 1194.3(b) – Incidental to Contract**, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

## **9.0 ACCEPTANCE CRITERIA**

- **Accuracy** - All deliverables shall be accurate in presentation, technical content, and adherence to accepted elements of style.
- **Clarity** – All deliverables shall be clear and concise; engineering terms shall be used as appropriate. All diagrams shall be easy to understand and relevant to the supporting narrative.
- **Conformance** – All deliverables shall conform to the U.S. Customs Service SDLC.
- **Specifications Validity** – All deliverables shall satisfy the requirements of the Government as specified herein.
- **File Editing** – All text and diagrammatic files shall be editable by the Government.
- **Timeliness** – All deliverables shall be submitted on or before the due date specified in this Task Order.

**B.7. Projected Milestones**

<b>Event</b>	<b>Projected Date</b>
<b>Automated Targeting System (ATS) Support</b>	<b>At date of IA execution - Ongoing</b>
<b>AQQ Support</b>	<b>At date of IA execution - Ongoing</b>
<b>Performance reporting by Servicing Agency</b>	<b>As required by COTR</b>
<b>Procurement Milestone Dates</b>	<b>As specified by COTR</b>

**B.8. Billing and Payment**

The Servicing Agency will pay contractor invoices from amounts identified in section 13 on a reimbursable basis. The Servicing Agency will present an itemized statement to the Transportation Security Administration for reimbursement of incurred contract costs and assisted services support costs. The Transportation Security Administration will pay reimbursable billings to the Servicing Agency from funds identified in section 12. See section 7 of Part A for additional terms and conditions addressing billing and payment.



Reimbursable billings are delinquent when they are 30 or more calendar days old (from date of the billing). When billings remain delinquent over 30 calendar days and the Transportation Security Administration has not indicated a problem regarding services, the Servicing Agency may choose not to award any new contract/orders or modifications to existing contract/orders for the Transportation Security Administration (or the client within) and termination of existing services will be considered and negotiated with the Transportation Security Administration.

#### **B.9. Description of Acquisition Assistance**

The Servicing Agency will provide the following services to the Transportation Security Administration.

The Servicing Agency will provide the following services to the Requesting Agency. The Servicing Agency will provide cradle-to-grave acquisition support services to the Requesting Agency. These services shall include preparing a solicitation, conducting a competition, including evaluation of offers and source selection, and invoice processing and payment. The Servicing Agency's specific roles and responsibilities are delineated in Section A.6 along with the associated roles and responsibilities of the Requesting Agency.

**B.10. Fees**  
N/A

**B.11. Obligation Information**

Servicing Agency and Transportation Security Administration shall complete the table below. HSTS02-10-X-DAD007	Requirement Application development and maintenance services, project and security support services.	Type of Requirement Severable Service
---	---	--

**B.12. Transportation Security Administration Funding Information**

Basic Appropriation Symbol	2110200DAD007
Amount Obligated	\$500,000.00
Fund Citation (Line of Accounting)	STS101A000D2010HQA010GE000077005000500DAD-5400000000000000-253D-TSADIRECT-DEF. TASK-D
Appropriation expiration date	9/30/2011
Unique restrictions on funding (if any)	None
TSA Agency Location Code (ALC)	70110001
TSA DUNS/BPN Number:	11-274-6297

The total Not To Exceed (NTE) funding limit on this Interagency Agreement is \$2,500,000.00

**B.13. Servicing Agency Funding Information**

The Servicing Agency shall complete the table below. Basic appropriation symbol (Treasury account symbol)
Fund citation (line of accounting)
Business event type code
Agency location code (8-digit) for IPAC
DUNS/BPN number (Business Partner Network or BPN #)

(b)(3)

**B.14. Description of Requesting-Agency Specific Restrictions**

This section identifies unique restrictions applicable to the Transportation Security Administration regarding acquisition, other than funding. [Insert description e.g., the Berry Amendment]

Note: unique restrictions on funding should be identified in paragraph B. 12.

**B.15. Small Business Credit**

The Servicing Agency shall use the following FIPS 95-2 Code to Identify the Transportation Security Administration in FPDS: [the Transportation Security Administration should insert the lowest FIPS 95-2 Agency/Bureau component]. Note: If the code is not provided, the Servicing Agency will allocate the credit to the highest Transportation Security Administration FIPS 95-2 Code.

**B.16. Amendments**

Any amendments to the terms and conditions in Part B shall be made in writing and signed by both the Servicing Agency and the Transportation Security Administration.

<b>B.17. Contact Information</b>	
Servicing Agency Contracting POC	Transportation Security Administration Program Office POC
Name (b)(6)	Name Michael Munnis
Address	Address 601 South 12th Street, Arlington, VA 20598-6010
Email (b)(6)	Email (b)(6)
Phone/Fax (b)(6) 571-468-1478	Phone/Fax 703-601-(b)(6)
Servicing Agency Financial POC	Transportation Security Administration Financial POC
Name (b)(6)	Name (b)(6)
Address DHS- Customs & Border Protection National Finance Center PO Box 68908 Indianapolis, IN 46268	Address 601 South 12th Street, Arlington, VA 20598-6014
Email (b)(6)	Email (b)(6)
Phone/Fax (b)(6) 317-298-1038	Phone/Fax 571-227-(b)(6)

<b>Requesting Agency Contracting POC</b>
A.T. Bewick
601 South 12th Street, Arlington, VA 20598-6025
(b)(6)
571-227-(b)(6)



**B.18. Signatures**

<p>By signing this document, the Transportation Security Administration confirms that a bona fide need exists and that funds are for the designated purpose, meet time limitations, and are legally available for the acquisition described in this document; that all unique funding and procurement requirements, including all statutory and regulatory requirements applicable to the funding being provided, have been disclosed to Servicing Agency; and all internal reviews and approvals required prior to transferring funds to the Servicing Agency have been completed. The Servicing Agency's acceptance of this document creates an obligation on the part of the Transportation Security Administration.*</p>		<p><b>CUSTOMS AND BORDER PROTECTION</b></p>	
<p>(b)(6)</p>		<p>(b)(6)</p>	
<p>Signature</p>	<p>Date</p> <p>6/29/10</p>	<p>Date</p> <p>6/29/10</p>	
<p>(b)(6)</p>		<p>(b)(6)</p>	
<p>Name</p> <p>Contracting Officer</p>		<p>Name</p> <p>(b)(6)</p>	
<p>Title</p> <p>Transportation Security Administration</p>		<p>Title</p> <p>CONTRACTING OFFICER</p>	
<p>Agency</p>		<p>Agency</p> <p>CBP</p>	

**ATTACHMENTS (1)**

1. DHS Interagency Agreement Form 710-1A

List Overview						
List	List Owner	List Update Frequency	Approximate List Size (6/2012)	Most Recent MOU Date	Additional Documents	Begin Matching Date
No Fly List Selectee List Expanded Selectee List	Terrorist Screening Center (TSC)	(b)(3) 49 U.S.C. § 114(r)		Most recent version signed 9/12/2010 between DHS and TSC.	ICD signed 11/08/2011 between SF and WLS. ISA signed 3/11/2010 between TSA and WLS.	1/27/2009 4/11/2011
Do Not Board List (DNBL)	Centers for Disease Control (CDC)	As Needed	80	No MOU required as internal TSA entity provided SF with DNBL records from CDC.	Business Requirements Document was updated on 12/5/2009. Later process update provided to DHS Secretary on 12/5/2011	8/25/2009
Cleared List	DHS Traveler Redress Inquiry Program (TRIP)	(b)(3) 49 U.S.C. § 114(r)		No MOU required as DHS TRIP is operated by TSA.	Business Requirements Document was updated on 5/23/2011.	1/27/2009
(b)(3) 49 U.S.C. § 114(r)						6/10/2010
						9/8/2011
Pre <sup>TM</sup> Disqualification Protocol List	TSA Office of Security Operations (OSO)	Daily, Monday-Friday	19,000	No MOU required as agreement is within TSA.	ICD signed 6/19/2012. ConOps signed 6/2012.	6/28/2012

\*The list size is based on the number of identities, not the number of records (aliases) which is what Secure Flight matches against.

**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