United States Government Accountability Office

GAO

Report to Congressional Requesters

May 2007

AVIATION SECURITY

Efforts to Strengthen International Passenger Prescreening are Under Way, but Planning and Implementation Issues Remain

Accountability * Integrity * Reliability

May 2007

AVIATION SECURITY

Efforts to Strengthen International Passenger Prescreening are Under Way, but Planning and Implementation Issues Remain

GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-07-346, a report to congressional requesters

Why GAO Did This Study

Passenger prescreening—a process that includes matching passengers' identifying information against records extracted from the U.S. government terrorist watch list—is one of several security measures in place to help ensure the safety of commercial flights traveling to or from the United States. DHS has several efforts underway to strengthen international aviation passenger prescreening. This report focuses on certain elements of the passenger prescreening process as well as some of the actions that DHS is taking or has planned to strengthen prescreening procedures. This report is a limited version of the original November 2006 report as various agencies that we reviewed deemed some of the information in the original report to be security sensitive. GAO's work included interviewing officials and assessing relevant documentation from federal agencies, U.S. and foreign air carriers, industry groups, and several foreign countries.

What GAO Recommends

GAO recommended in November 2006 that the Department of Homeland Security (1) complete a strategic plan and develop an evaluation strategy for one of its prescreening programs, (2) take steps to ensure that international and domestic prescreening programs are aligned, and (3) ensure full compliance with applicable privacy laws. DHS generally concurred with these recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-346.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Cathy Berrick at (202) 512-3404 or berrickc@gao.gov.

What GAO Found

Customs and Border Protection (CBP), the Department of Homeland Security (DHS) agency responsible for international passenger prescreening, has planned or is taking several actions designed to strengthen the aviation passenger prescreening process. One such effort involves CBP stationing U.S. personnel overseas to evaluate the authenticity of the travel documents of certain high-risk passengers prior to boarding U.S.-bound flights. Under this pilot program, called the Immigration Advisory Program (IAP), CBP officers personally interview some passengers deemed to be high-risk and evaluate the authenticity and completeness of these passengers' travel documents. IAP officers also provide technical assistance and training to air carrier staff on the identification of improperly documented passengers destined for the United States. The IAP has been tested at several foreign airports and CBP is negotiating with other countries to expand it elsewhere and to make certain IAP sites permanent. Successful implementation of the IAP rests, in part, on CBP clearly defining the goals and objectives of the program through the development of a strategic plan.

A second aviation passenger prescreening effort designed to strengthen the passenger prescreening process is intended to align international passenger prescreening with a similar program (currently under development) for prescreening passengers on domestic flights. The Transportation Security Administration (TSA)—a separate agency within DHS—is developing a domestic passenger prescreening program called Secure Flight. If CBP's international prescreening program and TSA's Secure Flight program are not effectively aligned once Secure Flight becomes operational, this could result in separate implementation requirements for air carriers and increased costs for both air carriers and the government. CBP and TSA officials stated that they are taking steps to coordinate their prescreening efforts, but they have not yet made all key policy decisions.

In addition to these efforts to strengthen certain international aviation passenger prescreening procedures, one other issue requires consideration in the context of these efforts. This issue involves DHS providing the traveling public with assurances of privacy protection as required by federal privacy law. Federal privacy law requires agencies to inform the public about how the government uses their personal information. Although CBP officials have stated that they have taken and are continuing to take steps to comply with these requirements, the current prescreening process allows passenger information to be used in multiple prescreening procedures and transferred among various CBP prescreening systems in ways that are not fully explained in CBP's privacy disclosures. If CBP does not issue all appropriate disclosures, the traveling public will not be fully aware of how their personal information is being used during the passenger prescreening process.

Contents

Table

Figures

Abbreviations

AEA	Association of European Airlines
ALO	Airline Liaison Officer
APIS	Advanced Passenger Information System
APP	Advanced Passenger Processing
AQQ	APIS Quick Query
ATA	Air Transport Association of America
ATS	Automated Targeting System
CBP	Customs and Border Protection
CSI	Container Security Initiative
DHS	Department of Homeland Security
DIMIA	Department of Immigration and Multicultural and Indigenous Affairs
ETA	Electronic Travel Authority
EU	European Union
GPRA	Government Performance and Results Act
IAP	Immigration Advisory Program
IATA	International Air Transport Association
ISI	Immigration Security Initiative
MIO	Migration Integrity Officer
NPRM	Notice of Proposed Rulemaking
NTC	National Targeting Center
PNR	Passenger Name Record
TDY	Temporary Duty
TECS	Treasury Enforcement Communications System
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Database
TSOC	Transportation Security Operations Center
VWP	Visa Waiver Program

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

May 16, 2007

The Honorable John Conyers, Jr.
Chairman
Committee on the Judiciary
House of Representatives

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

The Honorable Daniel K. Inouye
Chairman
The Honorable Ted Stevens
Vice-Chairman
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable F. James Sensenbrenner, Jr.
House of Representatives

During 2005, a number of passengers that the U.S. government identified as a security risk were identified onboard international flights traveling to or from the United States.[1] In certain cases, the resulting security risk was deemed high enough that the U.S. government diverted the flight from its intended destination, resulting in delays for passengers, costs to the air carriers, and government intervention.

Preventing such high-risk passengers from boarding international flights traveling to or from the United States is the goal of the nation's international aviation passenger prescreening process.[2] These efforts include, among other things:

- **Identity matching:** comparing passengers' identifying information, such as name and date of birth, against records extracted from the U.S.

[1] The specific number of passengers identified by the U.S. government as a security risk is sensitive security information.

[2] A separate process exists for prescreening passengers on U.S. domestic flights.

government terrorist watch list containing the names of known or suspected terrorists.[3]

- **Travel document review:** evaluating the authenticity and completeness of passengers' passports and other travel documents.

- **Risk targeting:** comparing passenger information against a set of targeting rules that are indicators of elevated passenger risk in an attempt to identify possible high-risk passengers who may not be on the terrorist watch list.

The identity matching component of the international passenger prescreening process currently involves separate matching activities conducted by air carriers (prior to a flight's departure) and the federal government (both before and after a flight's departure). In 2004, Congress mandated that the Department of Homeland Security (DHS) issue a proposed plan for completing the U.S. government's identity matching process before the departure of all international flights. Customs and Border Protection (CBP), the DHS agency charged with responsibility for conducting international aviation passenger prescreening, published its proposed plan to strengthen passenger prescreening in July 2006 in a notice of proposed rulemaking.[4] Appendix III provides more detail on the notice of proposed rulemaking and the two prescreening options that CBP provides to air carriers in the proposed rulemaking.

This report is a limited version of the original report that we provided to you on November 20, 2006. The various agencies we reviewed deemed some of the information in that report as Sensitive Security Information or Law Enforcement Sensitive. Therefore, this report omits our findings associated with vulnerabilities we identified in the existing passenger prescreening process and measures that could be taken to address those vulnerabilities. This report also omits key details regarding certain

[3] The U.S. government maintains a single consolidated terrorist watch list. Records are extracted from this consolidated list to conduct various screening activities including aviation passenger prescreening. Additional information about the watch list can be found on pages 7 and 9.

[4] 71 Fed. Reg. 40035, July 14, 2006. A notice of proposed rulemaking (NPRM) is an announcement published in the *Federal Register* of proposed new regulations or modifications to existing regulations, the first stage in the process of creating or modifying regulations. A notice of proposed rulemaking is intended to give the public an opportunity to comment on a proposed rule.

procedures, timeframes and locations associated with the passenger prescreening process. The objectives of the original report addressed:

- the main factors affecting the international passenger prescreening process, and the potential impact of these factors, and
- the status of efforts to address these factors, and the issues, if any, that could affect efforts to strengthen the international passenger prescreening process.

This version of the report focuses on certain elements of the current international aviation passenger prescreening process as well as some of the actions that DHS is taking or has planned to strengthen prescreening procedures. More specifically this report's content addresses:

- the implementation of the Immigration Advisory Program (IAP), a CBP program that assesses risk levels for certain passengers in limited overseas locations;
- the alignment of international and domestic passenger prescreening processes; and
- compliance with privacy laws with respect to information collected to conduct international passenger prescreening.

Although the information provided in this version of the report is more limited in scope, the overall methodology used for our initial report is relevant to this report as well because the information contained in this report was derived from the initial sensitive report. To address the objectives of our initial report we interviewed officials and obtained and analyzed relevant documents from CBP, including the National Targeting Center (NTC); the Transportation Security Administration (TSA), including the Transportation Security Operations Center (TSOC); and the Terrorist Screening Center (TSC). To obtain a cross section of both domestic and foreign air carriers' views about the international passenger prescreening process, including the impact of current U.S. prescreening requirements and the potential impact of future requirements, we interviewed officials from 13 air carriers that fly passengers to and from the United States.[5] We also interviewed officials from two domestic air carrier and passenger travel associations and three international air carrier associations that represent the interests of air carriers and travelers to discuss the impact of current and potential future U.S. international prescreening requirements on their members. We met with foreign government officials in the Netherlands, Poland, the United Kingdom, Australia, and New Zealand to discuss the impact of current and potential future U.S. international prescreening requirements and obtain information about aviation prescreening programs in place in these countries. We also met with officials from the European Union to discuss the impact of U.S. prescreening requirements on air carriers with operations in Europe. Additionally, we interviewed and obtained documents from private sector companies that facilitate the electronic transmission of passenger data between air carriers and government agencies to determine their role, if any, in future international aviation passenger prescreening initiatives. We conducted our work, which took place from April 2005 through October 2006, in accordance with generally accepted government auditing standards. Appendix I contains more detail about our scope and methodology.

Results in Brief

DHS has several efforts underway to strengthen international aviation passenger prescreening. Two of these efforts include:

- **Conducting overseas review of some high-risk passengers' travel documents.** One prescreening effort that CBP has under way is designed to increase the level of scrutiny given to the travel documents of certain high-risk passengers before they board international flights traveling to the United States. Under this pilot program, called the Immigration Advisory Program (IAP), CBP assigns officers to selected foreign airports where they utilize an automated risk-targeting system that identifies passengers as potentially high-risk—including passengers who do not need a visa to travel to the United States. CBP officers then personally interview some of these passengers and evaluate the authenticity and completeness of these passengers' travel

[5] To help ensure the information we obtained was representative of air carriers that fly different volumes of passengers to the United States, we selected seven carriers that fly more than 1 million passengers annually into the United States, four carriers that fly between 500,000 and 1 million passengers annually into the United States, and two carriers that fly less than 500,000 passengers annually into the United States.

documents. Successful implementation of the IAP rests, in part, on CBP clearly defining the goals and objectives of the program.

- **Aligning international and domestic prescreening programs.** A second prescreening effort under way is designed to align international passenger prescreening with a similar program under development for prescreening passengers on domestic flights. The Transportation Security Administration—a separate agency within DHS—is developing a domestic passenger prescreening program called Secure Flight. Once Secure Flight is operational, TSA will be operating a domestic passenger prescreening system, and CBP will be operating an international passenger prescreening system. As currently envisioned, both programs will screen passengers whose itinerary includes both an international flight and a domestic connection within the United States. If the two programs are not effectively aligned, each program could result in separate implementation requirements for air carriers. This could result in additional costs to the air carriers and the U.S. government, and cause confusion and inconvenience to passengers. CBP and TSA officials stated that they are taking some steps to coordinate their prescreening efforts, but they have not yet made all key policy decisions.

In addition to these efforts to strengthen certain international passenger prescreening procedures, one other issue, while not aimed at strengthening the capabilities of international aviation passenger prescreening, nonetheless requires consideration in the context of these efforts. This issue is:

- **Providing assurances of privacy protection as required by federal privacy law.** Federal privacy law requires agencies to inform the public about how the government uses their personal information. Although CBP officials have stated that they have taken and are continuing to take steps to comply with these requirements, the current prescreening process allows passenger information to be used in multiple prescreening procedures and transferred among various CBP prescreening systems in ways that are not fully explained in CBP's privacy disclosures. Although CBP recently published additional privacy disclosures related to its use of passenger data during the prescreening process, CBP's current public disclosures do not fully explain its uses of personal information during the entire prescreening process. If CBP does not issue all appropriate disclosures, the traveling public will not be fully aware of how their personal information is being used during the passenger prescreening process.

To help DHS ensure progress on efforts to strengthen the international passenger prescreening process, we recommended in our November 2006 report that the Secretary of the Department of Homeland Security and the Commissioner of Customs and Border Protection take the following steps: (1) complete a strategic plan and develop an evaluation strategy for the Immigration Advisory Program pilot, (2) further align domestic and international passenger prescreening processes and coordinate prescreening efforts, and (3) ensure that international passenger prescreening programs are in full compliance with federal privacy laws. We provided a draft of this report to DHS and DOJ for their review and comment. DHS, in its written comments, generally concurred with the recommendations in the report. DHS and DOJ both provided technical comments that we incorporated as appropriate. In its written comments, DHS outlined the status of various efforts that it has in progress or planned to address the recommendations. For example, DHS stated that CBP has efforts under way to capture additional data in order to properly evaluate the IAP's performance, and that there are ongoing efforts by CBP and TSA to align procedures, systems and functional requirements for their respective passenger prescreening programs. DHS also noted in its comments the recent and planned efforts to publish new privacy disclosure documents, such as the November 2006 system of records for its automated targeting system, which would supplement its other existing public disclosure documents. The full text of DHS's comments is provided in appendix IV.

Background

Passenger prescreening is one security measure among many implemented both before and after the terrorist attacks of September 11 designed to strengthen the security of U.S. commercial aviation. Together, these various measures combine to form a multi-layered aviation security approach. Although the prescreening of passengers on international flights traveling to or from the United States predated the September 11, 2001 terrorist attacks, this process was strengthened after the attacks.

Current International Passenger Prescreening Process Relies on Two Different Sets of Passenger Data and Involves Multiple Steps

The current international passenger prescreening process relies on two different sets of passenger data and involves multiple prescreening steps carried out by air carriers and CBP. The two sets of passenger data include:

Passenger Name Record (PNR) data, such as name, address, and billing information that passengers provide to air carriers, travel agents, or online travel companies when making a flight reservation.

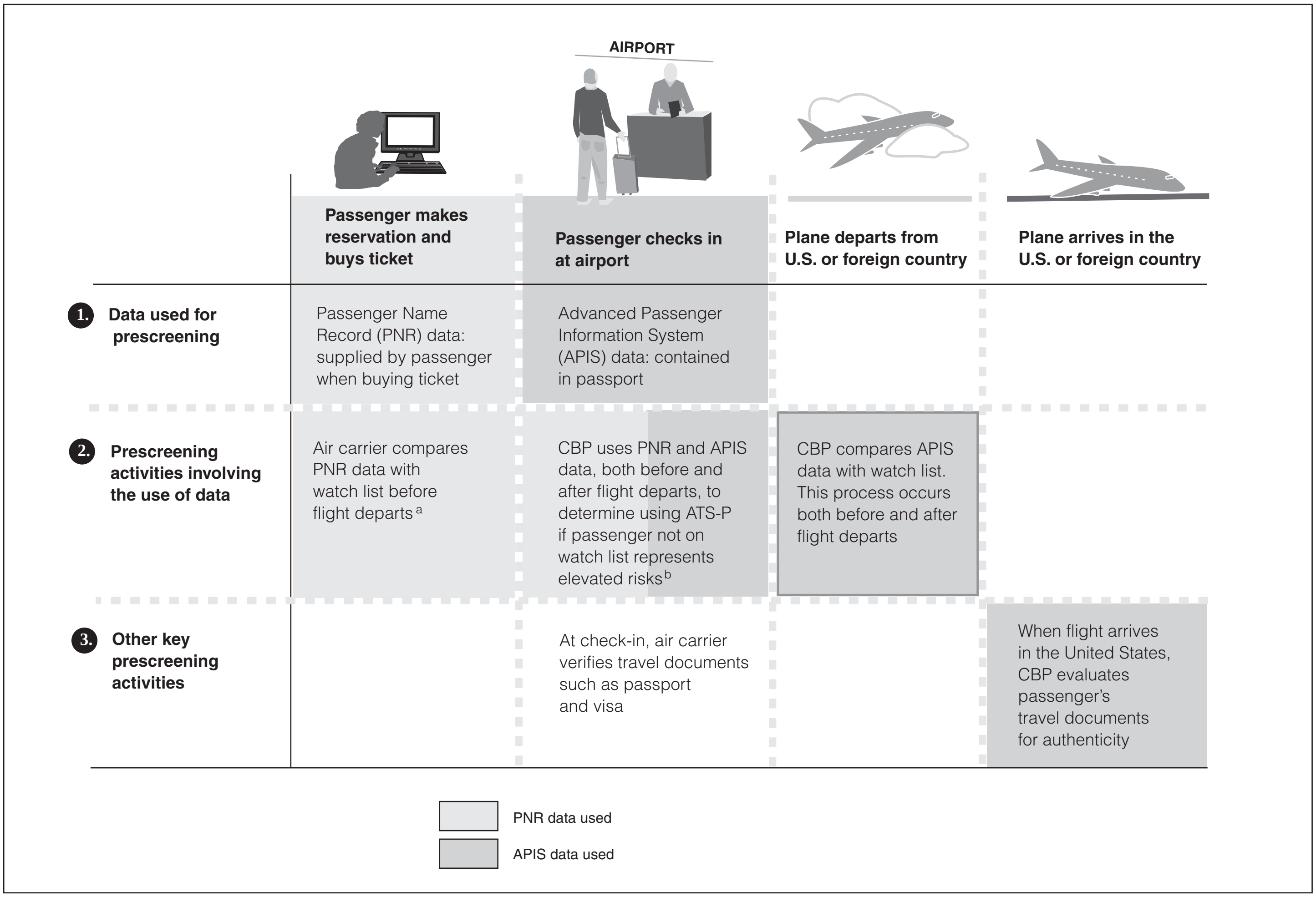
Advance Passenger Information System (APIS) data, such as name, date and location of birth, and country of citizenship, which is derived from passports and other government-issued documents, such as visas, that most passengers must present to air carriers when checking in for international flights.

A central prescreening activity involves matching identifying information about passengers—including name and date of birth—against the No Fly and Selectee Lists that are extracted from the TSC's Terrorist Screening Database (TSDB) to identify potential security threats in a process often called identity matching. The identity matching step is conducted by both air carriers and the U.S. government. Federal requirements state that air carriers must transmit APIS data to CBP no later than 15 minutes before flight departure for international flights originating in the United States and no later than 15 minutes after flight departure for international flights bound for the United States. In addition to these data, CBP occasionally uses commercial data or data from other government databases during this process to help confirm a passenger's identity.

A second prescreening activity, separate from identity matching, involves using risk assessment tools to analyze passenger data to assess the security risk that a passenger might pose. This constitutes an effort to identify high-risk passengers that may not be on the No Fly or Selectee Lists. Specifically, CBP uses an automated system, called the Automated Targeting System-Passenger (ATS-P), that uses available passenger data to apply a set of CBP-generated targeting "rules" that CBP has determined are associated with increased passenger risk. CBP uses both PNR and APIS data to apply the ATS-P rules. This comparison results in a risk assessment for each passenger indicating the passenger's relative security risk.

A third prescreening activity involves the review of passengers' travel documents for evidence of forgery or fraudulent use. Depending on the passenger, this document review can occur at three separate time frames during the process of flying internationally, as follows: (1) the State Department reviews the travel documents in advance of travel for passengers who are required to obtain a visa in advance of their travel, (2) air carrier personnel review passengers' travel documents for authenticity upon check-in for flights, and (3) CBP officers review passenger travel documents either upon the passengers' arrival in the United States or, in some cases, prior to their departure for the United States. Figure 1 provides an overview of the current passenger prescreening activities as set against the basic steps typically taken to fly internationally—including obtaining a flight reservation and ticket, checking in for a flight, departing from one country, and arriving in another.

Figure 1: Overview of Current Prescreening Activities for International Flights



	Passenger makes reservation and buys ticket	Passenger checks in at airport	Plane departs from U.S. or foreign country	Plane arrives in the U.S. or foreign country
1. Data used for prescreening	Passenger Name Record (PNR) data: supplied by passenger when buying ticket	Advanced Passenger Information System (APIS) data: contained in passport		
2. Prescreening activities involving the use of data	Air carrier compares PNR data with watch list before flight departs[a]	CBP uses PNR and APIS data, both before and after flight departs, to determine using ATS-P if passenger not on watch list represents elevated risks[b]	CBP compares APIS data with watch list. This process occurs both before and after flight departs	
3. Other key prescreening activities		At check-in, air carrier verifies travel documents such as passport and visa		When flight arrives in the United States, CBP evaluates passenger's travel documents for authenticity

□ PNR data used

▨ APIS data used

Source: GAO.

[a] An additional prescreening step occurs for those passengers traveling to the United States from non-visa waiver program countries. For these passengers this additional step involves State Department officers reviewing the authenticity of their passports prior to issuing a travel visa.

[b] In several overseas locations, CBP also reviews the travel documents of selected high-risk passengers through a pilot program. See page 14 for more details on the pilot program.

Air Carriers Use Passenger Data Obtained during Reservation Process to Conduct a Comparison against the No Fly and Selectee Lists

Before a passenger receives a boarding pass, the air carriers conduct an initial identity match, which (along with CBP's identity matching process) constitutes the first step of the international passenger prescreening process. To complete this prescreening step, air carriers compare PNR data (information that is self-reported by passengers when they make a flight reservation) against the No Fly and Selectee Lists to determine if there are any identity matches. This prescreening step is required to occur prior to flight departure. The No Fly and Selectee Lists are extracted from the TSC's TSDB, the consolidated federal government terrorist watch list (which contains the names of known or suspected terrorists). Persons on the No Fly List are deemed to be a threat to civil aviation and are therefore to be precluded from boarding an aircraft traveling to, from, or within the United States. Being on the Selectee List does not mean that the person will not be allowed to board an aircraft or enter the United States. Instead, persons on this list receive additional security screening prior to being permitted to board an aircraft—this screening may involve a physical inspection of the person and a hand-search of their luggage.

Examples of PNR data that may be collected at the time a reservation is made include a passenger's name, home address, telephone number, frequent flyer information, and e-mail address. If an air carrier determines that a passenger's identity matches an identity on the No Fly List, TSA requires the carrier to contact the TSA Office of Intelligence so U.S. authorities can further verify whether the passenger's identity matches the watch-listed identity.[6]

[6] For example, in some cases a passenger may have the same name as a person listed on the No Fly or Selectee Lists, and an air carrier may require assistance from TSA to verify whether the person is, in fact, the same person.

CBP Uses Passenger Data Obtained during Passenger Check-in to Conduct an Identity-matching Procedure

CBP also conducts an identity matching process after air carriers conduct their identity matching, but CBP's process utilizes APIS data. These data are generally gathered from the passenger's passport—a document required of almost all passengers flying into and out of the United States.[7] In most instances, these data are recorded electronically from the traveler's machine-readable passport. This process records information from the passport directly into the air carrier's computer systems, thereby avoiding potential errors that could occur by key-stroking the data. CBP uses the APIS data to conduct identity matching using its automated systems including its law enforcement databases and the No Fly and Selectee Lists, which CBP transfers to its Treasury Enforcement Communications System (TECS).[8] If this review produces a positive match to the No Fly List, the TSA Office of Intelligence is contacted to confirm the match.

CBP Identifies Passengers Not on the No Fly and Selectee Lists Who May Present Security Risks

While the above prescreening activities focus on determining whether any passengers are on the No Fly and Selectee Lists, CBP also conducts a second prescreening step to identify other passengers, not on the No Fly and Selectee Lists, but who may nonetheless present a potential security risk. This step is a risk targeting process that occurs for international flights traveling to or from the United States. CBP conducts this risk-targeting using a computer-based system called the Automated Targeting System-Passenger. This system compares passenger data (both PNR and APIS data), along with data from government databases (including the TSDB), against a set of targeting rules. According to CBP officials, this risk-targeting process reflects CBP's experience with indicators of possible illegal or other activities that CBP is responsible for monitoring. This comparison results in a risk assessment for each passenger that CBP uses to determine if the passenger requires additional CBP contact—either

[7] Prior to January 23, 2007, an exception to this rule existed for citizens of the United States, and visiting citizens of Canada, Mexico, and Bermuda when entering the United States from most countries in the Western Hemisphere. However, under a plan required by the Intelligence Reform and Terrorism Prevention Act of 2004, as amended, all U.S. citizens, and citizens of Canada, Bermuda, and Mexico traveling to the United States as nonimmigrant visitors, generally must present a valid passport at air ports-of-entry.

[8] TECS is the principal law enforcement system supporting CBP's counter-terrorism and regulatory compliance missions. TECS consists of multiple databases that maintain investigative case information, border-crossing information, passenger information, and other information provided by other government agencies related to the inspection of persons crossing the border. CBP uses automated systems to screen large amounts of data against information in the TSDB, including names on the No Fly and Selectee Lists.

before the passenger boards a U.S.-bound aircraft or upon the passenger's arrival in the United States. If a passenger's risk assessment indicates an elevated security risk, CBP may decide to take additional security actions to gather more information about the passenger. Additionally, CBP can also decide that a passenger's risk level is sufficiently elevated that the passenger should be prevented from boarding a flight. If the flight is abroad, CBP officials stated that they can coordinate with State Department Officers to contact U.S. Embassy Legal Attaché officials assigned abroad at foreign embassies and consular offices. These Legal Attaché officers coordinate with foreign law enforcement personnel to identify, interview, or inspect the passenger before allowing the passenger to board the flight.

Air Carriers and CBP Evaluate the Authenticity of Passenger Travel Documents

A third prescreening step involves air carriers and CBP determining the authenticity of passenger travel documents. Before issuing boarding passes on flights departing from or arriving in the United States, air carriers are required to review each passenger's travel documents, including passports and visas, to verify that the passenger is properly documented for the intended destination. For U.S.-bound passengers, air carriers are also required to validate that the passenger's passport information matches the APIS data that the air carriers electronically submit to CBP. CBP provides periodic training to air carrier personnel to help them determine the authenticity and completeness of passenger travel documents. CBP's review of passenger documentation can occur in multiple locations. For example, CBP is always required to inspect travel documents for passengers on international flights arriving in the United States. However, in some overseas locations, CBP officials also review passenger documents prior to the passenger boarding a U.S.-bound international flight.

Federal Law Mandated That CBP Publish a Plan to Alter Its Prescreening Process

The current prescreening process is under revision and under a proposed plan, the U.S. government will take over the process of identity matching passengers against the No Fly and Selectee Lists from the air carriers prior to flight departures. As part of the Intelligence Reform and Terrorism Prevention Act of 2004,[9] Congress mandated that DHS issue a notice of proposed rulemaking (NPRM) by February 16, 2005, that would allow CBP

[9] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638, Section 4012.

to conduct its comparison of passenger information against the No Fly and Selectee Lists before the departure of all international flights traveling to or from the United States. CBP issued its NPRM on July 14, 2006, and provided for a public comment period.[10]

Prescreening Passengers on Domestic Flights Involves a Different Process

Concurrent to the changes that are being considered for conducting international passenger prescreening, TSA, the agency charged with ensuring the security of all modes of transportation, is in the process of modifying domestic passenger prescreening procedures. TSA is required, by the Intelligence Reform and Terrorism Prevention Act of 2004, to develop a prescreening program through which TSA would assume the domestic watch list matching function currently conducted by air carriers prior to domestic flight departures. TSA has named this prospective prescreening program Secure Flight.

As we have reported in our prior work on Secure Flight, currently only air carriers—and not the U.S. government—match passenger information against the No Fly and Selectee Lists to prescreen passengers on domestic flights. [11] We have also reported that TSA has faced significant management challenges in the past in developing the Secure Flight program, and that key policy decisions that would affect the effectiveness of the program had not yet been made. In 2006, TSA announced that it was delaying the development of Secure Flight in order to reassess the program's goals, requirements, and capabilities. The current domestic prescreening process also requires that air carriers operate the Computer-Assisted Passenger Prescreening System (CAPPS), which identifies passengers for secondary screening based on certain travel behaviors reflected in their reservation information that are associated with threats to aviation security, as well as through a random selection of passengers.[12]

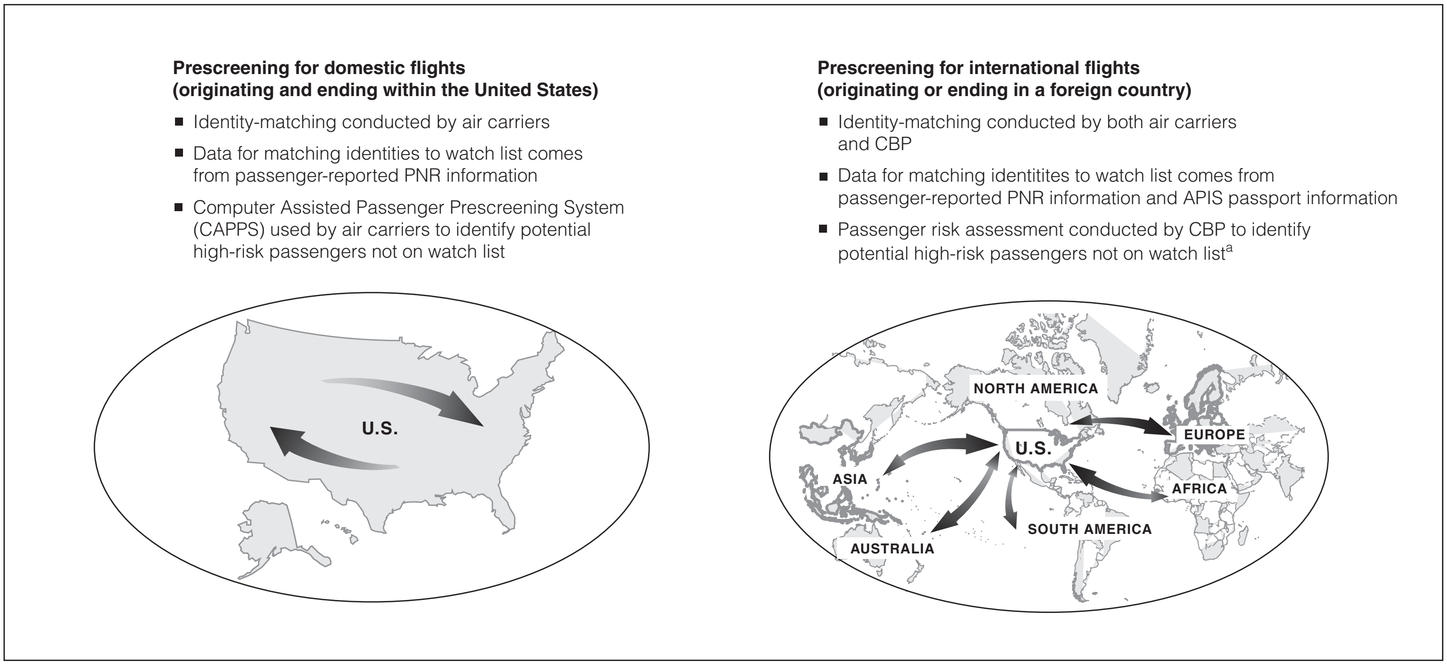
[10] 71 Fed. Reg. 40035, July 14, 2006. CBP granted an extension to the comment period in response to a request by the aviation industry. As a result of the extension, comments on the proposed rule were due by October 12, 2006.

[11] GAO, *Aviation Security: Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program*, GAO-06-374T (Washington, D.C.: Feb. 9, 2006). GAO, *Aviation Security: Secure Flight Development and Testing Under Way, but Risk Should Be Managed as System Is Further Developed*, GAO-05-356 (Washington, D.C.: Mar. 28, 2005).

[12] Although the air carriers currently conduct the watch list matching and CAPPS prescreening functions, these processes are required and overseen by TSA.

Figure 2 highlights the main steps of, and differences between, the prescreening of passengers on domestic and international flights.

Figure 2: Overview of Current Differences between the Domestic and International Prescreening Process



Prescreening for domestic flights (originating and ending within the United States)

- Identity-matching conducted by air carriers
- Data for matching identities to watch list comes from passenger-reported PNR information
- Computer Assisted Passenger Prescreening System (CAPPS) used by air carriers to identify potential high-risk passengers not on watch list

Prescreening for international flights (originating or ending in a foreign country)

- Identity-matching conducted by both air carriers and CBP
- Data for matching identitites to watch list comes from passenger-reported PNR information and APIS passport information
- Passenger risk assessment conducted by CBP to identify potential high-risk passengers not on watch list[a]

Source: GAO, MapArt (map).

[a] International flights departing from the United States that are operated by U.S. air carriers are required to also operate CAPPS to identify passengers for secondary screening. This occurs in addition to the risk assessments being conducted by CBP.

DHS is Taking Steps to Strengthen the Current International Passenger Prescreening Process

CBP has several efforts under way to strengthen certain international passenger prescreening processes. One such effort involves the placement of CBP personnel overseas to interview some high-risk passengers and inspect their travel documents in advance of their departure to the United States. This program also incorporates a mechanism to provide air carrier personnel with additional training on identifying fraudulent travel documents. As it revises the international passenger prescreening process, CBP is also attempting to align its process with the prospective program to prescreen passengers on domestic flights, which will be administered by the TSA.

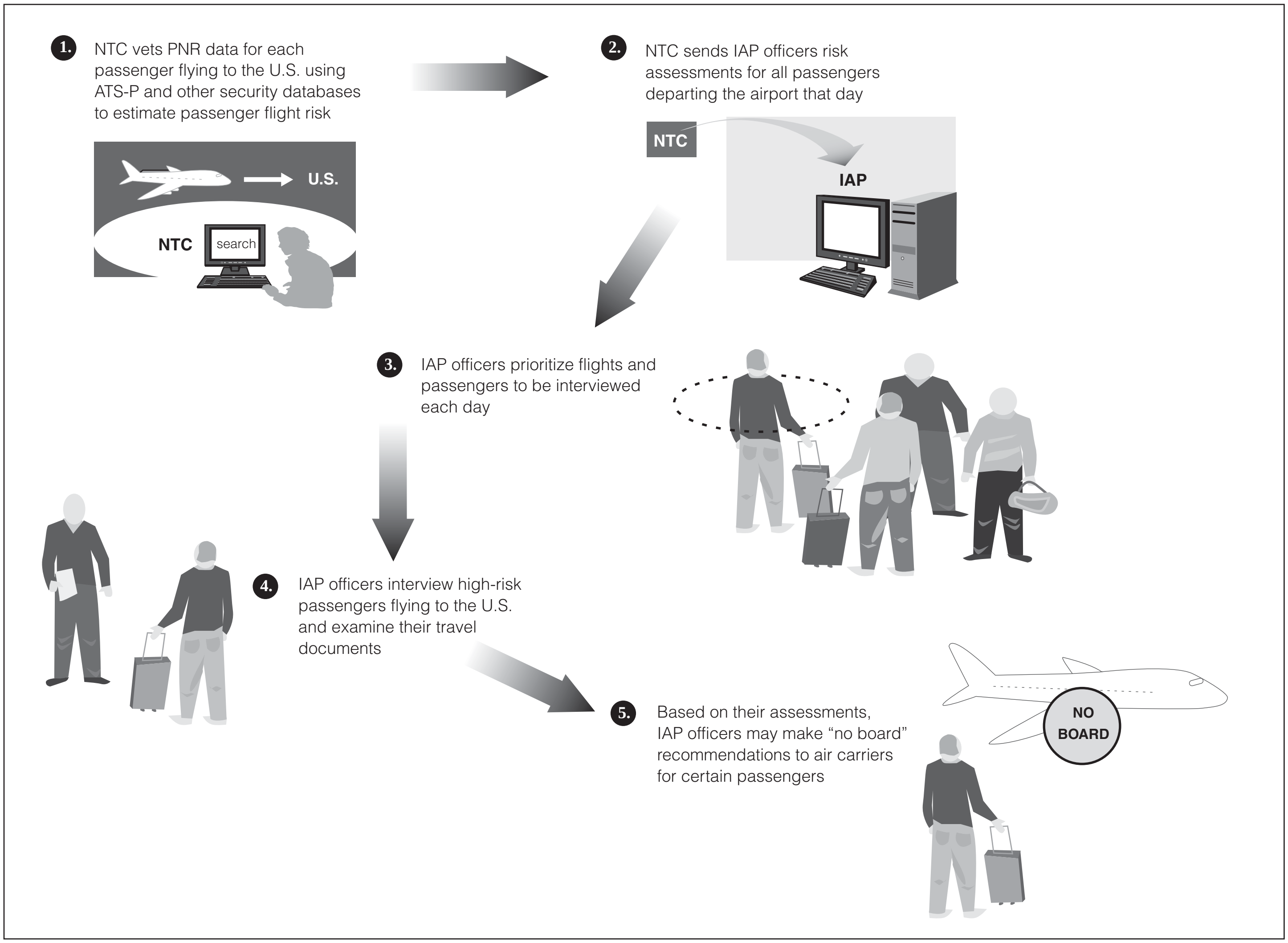
Immigration Advisory Program Developed to Increase Review of Travel Documents for Some High-Risk Passengers at Foreign Airports

One program, currently in place but supplemental to the primary international passenger prescreening processes, is a program that provides additional scrutiny to passengers and their travel documents at foreign airports prior to their departure for the United States. This program, called the IAP,[13] is a pilot program that began in 2004 and was designed to identify and target potential high-risk passengers. Under the IAP pilot, CBP has assigned trained officers to foreign airports where they personally interview pre-identified high-risk passengers, conduct behavioral assessments, and evaluate the authenticity of travel documents prior to the passenger's departure to the United States. The pilot program has been tested in several foreign airports, and CBP is negotiating with other countries to expand it elsewhere and to make certain IAP sites permanent.

The IAP pilot serves both national security and immigration functions. According to CBP, the purpose of the IAP is to (1) prevent passengers identified as security threats from boarding international flights bound for the United States, (2) provide no board recommendations to the air carriers for passengers who are not properly documented for entry into the United States, (3) provide training to air carrier personnel on how to detect fraudulent travel documents, (4) provide advance notice to U.S. authorities of passengers that warrant closer inspection upon their arrival in the United States, (5) collect law enforcement information on known or suspected criminal aliens and smugglers, and (6) share information with foreign government and law enforcement officials regarding trends in illegal travel. CBP officials and others have also stated that a secondary benefit of the IAP pilot is to help facilitate the legitimate travel of passengers, particularly U.S. citizens. Figure 3 depicts how the IAP works at international airports.

[13] IAP, or the Immigration Advisory Program, was initially referred to as the Immigration Security Initiative (ISI). Prior to the development of IAP, the legacy Immigration and Naturalization Service operated the Immigration Control Officers program, which was similar to IAP in that it stationed U.S. immigration officers abroad to screen U.S.-bound passengers in order to validate travel documents.

Figure 3: Immigration Advisory Program Process


1. NTC vets PNR data for each passenger flying to the U.S. using ATS-P and other security databases to estimate passenger flight risk
U.S.
NTC
search
2. NTC sends IAP officers risk assessments for all passengers departing the airport that day
NTC
IAP
3. IAP officers prioritize flights and passengers to be interviewed each day
4. IAP officers interview high-risk passengers flying to the U.S. and examine their travel documents
5. Based on their assessments, IAP officers may make “no board” recommendations to air carriers for certain passengers
NO
BOARD

Source: GAO.

Perceived Successes of IAP Led CBP to Expand the Program

The IAP pilot began at several sites in 2004. Each site consists of a group of IAP officers and a team leader. Team leaders are typically assigned to longer posts as compared to other IAP officers. Expansion of the pilot program to other locations has already begun. The Intelligence Reform and Terrorism Prevention Act of 2004 requires that CBP identify 50 foreign airports for further expansion of the IAP, and CBP has subsequently completed this list.[14]

CBP has reported several successes through the IAP pilot. According to CBP documents, from the start of the IAP pilot in June 2004 through February 2006, IAP teams made more than 700 no-board recommendations for inadmissible passengers and intercepted approximately 70 fraudulent travel documents. CBP estimated that these accomplishments equate to about $1.1 million in cost avoidance for the U.S. government associated with detaining and removing passengers who would have been turned away after their flights landed, and $1.5 million in air carrier savings in avoided fines and passenger return costs.[15] According to CBP, these monetary savings have defrayed the costs of implementing the program. However, it is not yet clear whether CBP anticipates, or expects, that the IAP will pay for itself through its government and air carrier cost savings, as it previously asserted.[16]

CBP officials said that they have also expanded a related program for training air carrier staff to better identify fraudulent identity documents and placed this program within IAP. This program, known as the Carrier Liaison Program, officially began in February 2006. According to CBP officials, CLP's purpose is to enhance border security by providing technical assistance and training to air carrier staff on the identification of improperly documented passengers destined for the United States.

To continue to strengthen and successfully expand the IAP, CBP is faced with concerns expressed by host government and IAP officials about the duration of its IAP officer rotations. CBP officials said that they were aware of these concerns and are taking steps to address the matter.

CBP's IAP Is Similar to Programs in Other Countries

Several other countries, such as the United Kingdom, Canada, Australia, and New Zealand, also operate programs similar to IAP. Known as airline liaison officer (ALO) programs, these programs have in some cases been

[14] CBP was directed in the Conference Report accompanying its FY 2007 Appropriations Act to report to the Congress on the performance of the IAP no later than January 23, 2007. According to CBP, they submitted the report to Congress prior to this deadline.

[15] We did not independently assess these costs estimates or other reported program benefits.

[16] IAP cost savings are derived from a CBP estimate based on the average costs to detain and remove an individual from the United States who is found not eligible to be admitted.

operating since the late 1980s. Like IAP, these countries also generally post officers overseas at airports in an attempt to intercept improperly documented passengers from traveling to their country. CBP officials are aware of these programs but believe that the IAP is different in some key respects. Most notably, CBP officials stated that IAP's focus is on terrorism, while ALO programs focus primarily on illegal immigration. However, valuable lessons can be gained from the experiences of these other countries in implementing similar programs as CBP continues to develop its IAP pilot. For example, officials from one ALO program stated that their country incorporated a Web-based system that allows its ALO officers to record improperly documented and other suspect travelers. These data can then be instantly accessed and analyzed at headquarters so that the information can be used to make changes to improve all of the country's ALO locations. Another ALO program utilizes PNR data to identify trends in document fraud, allowing its ALO network to quickly transmit alert information into its passenger screening system so that identified passengers can be screened further at check in prior to boarding an aircraft. CBP, however, relies upon each IAP site to send aggregate reporting statistics to CBP headquarters—potentially limiting the program's ability to rapidly analyze and act on trends in document fraud since there is a time delay in CBP headquarters receiving the data. Additionally, a United Kingdom official stated that their ALO program benefited from expanding the program slowly during the initial stages of the program to allow the United Kingdom government to learn important lessons from its early ALO sites. Appendix II contains a summary of information and potential lessons to be learned from the ALO programs of other countries.

CBP Could More Fully Incorporate Risk Management Principles in the IAP Pilot

CBP has not taken all of the steps necessary to fully learn from its pilot sites in order to determine whether the program should be made permanent and the number of sites that should exist. These steps are part of a risk management approach to developing and evaluating homeland security programs. Risk management is a continuous process of assessing risks, determining the best available actions to mitigate these risks, implementing actions to reduce risks, and evaluating these actions to determine their level of benefit. Managing homeland security efforts on the basis of risk has received widespread support from Congress, the President, and others as a way to help set priorities effectively and to allocate limited resources. A risk management framework includes such elements as formally outlining the goals of the program, setting measurable performance measures, and evaluating program effectiveness.[17]

Although CBP is currently taking steps to make its IAP sites permanent and to expand the program to other foreign locations, CBP has not finalized a strategic plan for the program that delineates program goals, objectives, constraints, and evaluative criteria. We have reported in the past that high-performing organizations have a focus on achieving results and outcomes and foster a results-oriented organizational culture to reinforce this focus. Key to developing this focus is strategic planning, which involves having a mission that employees, clients, customers, partners, and other stakeholders understand and find compelling; setting goals to achieve the mission; and aligning the organization's activities, core processes, and resources with those goals.[18] CBP officials told us that they have drafted a strategic plan for the IAP, which contains program goals and performance measures, but CBP stated that the plan has not yet been finalized.

DHS Intends to Align International and Domestic Prescreening Programs, but DHS Has Not Yet Made All Key Policy Decisions

A second effort that CBP has under way to strengthen the international passenger prescreening process involves the alignment of the U.S. government's international and domestic aviation prescreening programs, which are being developed separately by CBP and TSA, respectively. Aligning these two programs is particularly important because many passengers in the United States who are traveling to or from foreign destinations have a domestic flight in addition to their international flight. Passengers traveling on these types of flights are currently subjected to two different prescreening processes.

[17] These steps are part of an overall risk management framework for developing and evaluating homeland security programs. In 2004, we developed a risk management framework that brought together recognized risk management practices from public and private sector reports, as well as through interviews with terrorism experts. This framework was reviewed by academic experts in risk management, field-tested on several GAO reviews, and applied in analyzing a variety of homeland security applications. For further discussion of this risk management framework, see GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, GAO-06-91 (Washington, D.C.: Dec. 15, 2005).

[18] GAO, *Forum on High Performing Organizations: Metrics, Means, and Mechanisms for Achieving High Performance in the 21st Century Public Management Environment*, GAO-04-343SP (Washington, D.C.: Feb. 13, 2004).

The air carrier community has asked CBP and TSA to coordinate their efforts to ensure that the programs are compatible and are developed as a single approach to avoid the need for air carriers to implement two separate screening systems to meet CBP and TSA requirements. Without such coordination, air carriers might have to implement different information connections, communications, and programming for each prescreening program, as well as ensure that their data are compatible with each program. In a joint letter to the Secretary of DHS, the Air Transport Association of America (ATA) and the Association of European Airlines (AEA) urged DHS to coordinate international and domestic aviation passenger prescreening programs so that air carriers are not unduly burdened by the costs and inefficiencies posed by working with two different prescreening programs. The letter also stated that ATA and AEA believed that there had been a lack of full coordination between CBP and TSA in aligning their respective passenger prescreening programs. Further, as we have previously reported, since both agencies are developing and implementing passenger prescreening programs, CBP and TSA could mutually benefit from the sharing of technical testing results and the coordination of other developmental efforts.[19] Coordination and planning in the development of these two programs would also enhance program integration and interoperability and potentially limit redundancies.

In 2004, CBP and TSA officials stated that they recognized the similarities between the international passenger prescreening and the proposed domestic prescreening programs, and acknowledged the need to coordinate the two programs. According to CBP officials, DHS has expressed its intention to align international and domestic passenger prescreening efforts, and decided to develop one "portal" through which carriers will transmit passenger data to the government for domestic and international flights. CBP officials further stated that interagency discussions with TSA have resulted in a decision to create a single communication point for the submission of the passenger data for both domestic and international flights, one of the main concerns of air carriers.

Despite these coordination efforts and DHS's commitment to align the processes, CBP and TSA have not yet made all of the policy decisions to complete the alignment between the CBP international prescreening program and the prospective Secure Flight program, including the use of

[19] GAO-06-374T and GAO-05-356.

different data elements, documentation, and identity matching technologies to conduct prescreening.[20] CBP officials stated that many of these policy and technical decisions have not been made because TSA is in a process of "rebaselining" its Secure Flight program, which involves TSA reassessing program goals, requirements, and capabilities. In discussions with us, CBP and TSA officials stated that these coordination efforts were continuing, but they did not provide any documentation of how such matters were being resolved or when they planned for the programs to be aligned.

CBP Has Not Fully Disclosed its Use of Personal Information during the Prescreening Process

One additional issue requires consideration, as well, in the context of DHS's efforts to strengthen the passenger prescreening process. Despite recent efforts by CBP to provide more detailed information to the public about its use of passenger data during the international passenger prescreening process, CBP has not fully disclosed or assessed the privacy impacts of its use of personal information during international passenger prescreening as required by law. The Privacy Act of 1974 and the E-Government Act of 2002 require federal agencies to protect personal privacy by, among other things, limiting the disclosure of personal information and informing the public about how personal data are being used and protected. Federal agencies inform the public of their use of personal information by issuing two types of documents:

System of records notices: The Privacy Act requires that agencies publish a notification in the *Federal Register* that informs the public when they establish or make changes to a system of records.

Privacy impact assessment: The E-Government Act requires that agencies analyze how information is handled to (1) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) examine and evaluate protections

[20] GAO-06-374T.

and alternative processes for handling information to mitigate potential privacy risks.[21]

Although CBP has taken certain actions to meet the requirements of the Privacy and E-Government Acts, including the recent publication of additional privacy disclosures, these actions have not fully informed the public about how personal information is being used, as required by law. Specifically, CBP has published public notices and reports that describe certain elements of its international prescreening process, but these documents do not fully or accurately describe CBP's use of personal data throughout the passenger prescreening process. It is important for CBP's documentation to describe all of the steps of the prescreening process because the interrelationship of various steps of the process allows data to be transferred and used in ways that have not been fully disclosed.

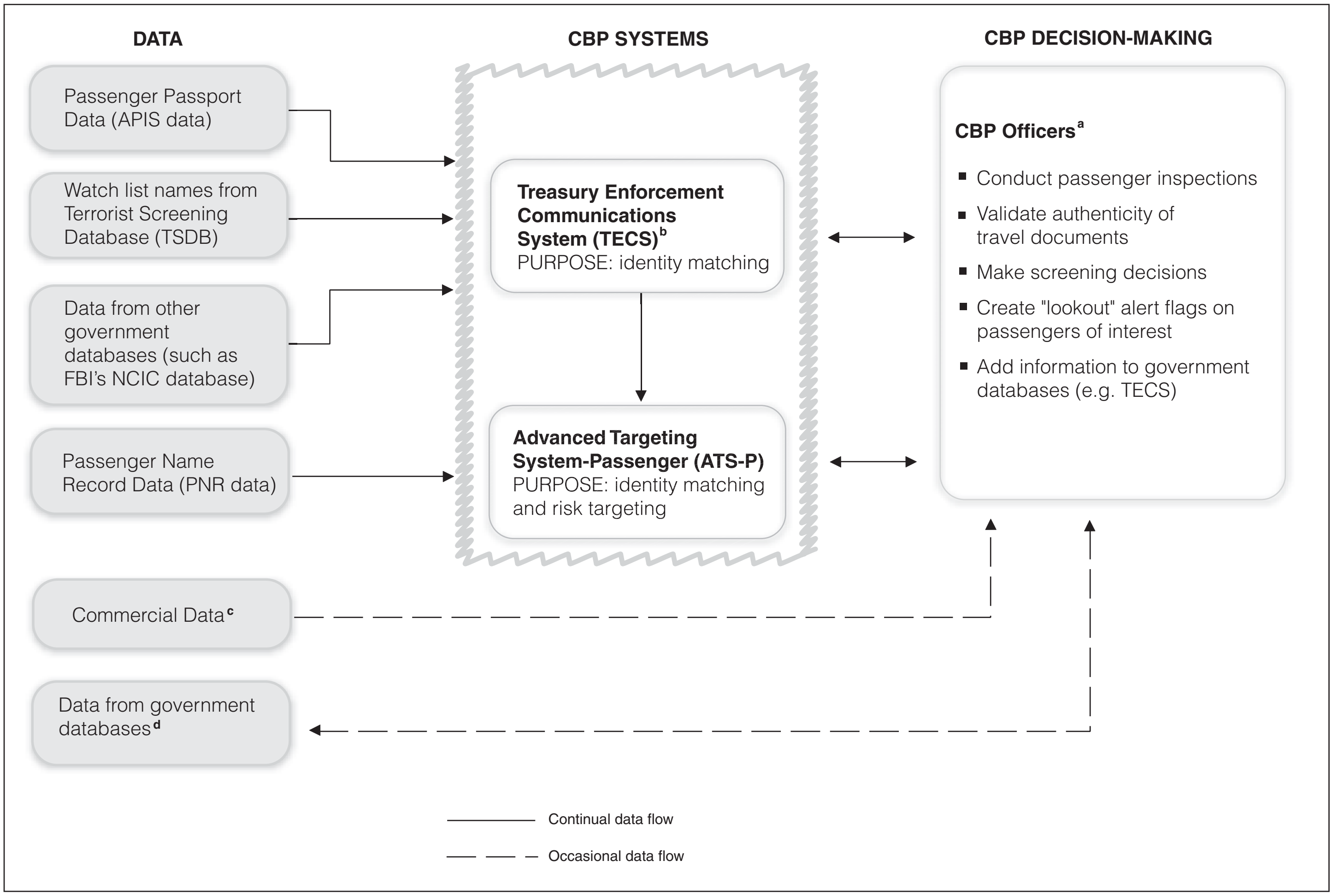
CBP's international prescreening process involves a wide range of procedures and data sources that CBP utilizes to determine passenger risk levels. According to a CBP official, to help make these prescreening decisions, CBP collects personal data from multiple sources (including passengers and government databases), and uses the data for several purposes, including identity matching against the government watch list, risk targeting, and passenger document validation. According to CBP, its officers also use commercial data, to a limited degree, to assist them in confirming a passenger's identity when needed. CBP's public disclosures about APIS and ATS do not describe all of the data inputs or the extent to which the data are combined and used in making prescreening decisions.[22]

[21] The Privacy Act places limitations on agencies' collection, use, and disclosure of personal information maintained in systems of records, which are groups of personal information that are maintained by an agency from which personal information is retrieved by an individual's name or identifier. Among the act's provisions are requirements for agencies to give notice to the public about the use of their personal information. Also, when agencies establish or make changes to a system of records, they must notify the public by a notice in the *Federal Register* about the type of data collected; the types of individuals about whom information is collected; the intended "routine" uses of the data; the policies and practices regarding data storage, retrievability, access controls, retention, and disposal; and procedures that individuals can use to review and correct personal information. The E-Government Act of 2002 requires agencies to conduct a privacy impact assessment when using information technology to process personal information.

[22] The degree to which an agency must disclose its use of personal information may be limited by exemptions permitted by the Privacy Act. To claim such exemptions, an agency must issue a rule, with an opportunity for public comment, identifying their exemptions and the reasons for taking the exemptions. 69 Fed. Reg. 41543, July 9, 2004 and 68 Fed. Reg. 69412, 69413, Dec. 12, 2003.

As shown in Figure 4, CBP's passenger prescreening involves more data inputs and uses of data than are described in CBP's current privacy disclosures.

Figure 4: The interaction between CBP Prescreening Systems and Data Usage


DATA
CBP SYSTEMS
CBP DECISION-MAKING
Passenger Passport Data (APIS data)
Watch list names from Terrorist Screening Database (TSDB)
Data from other government databases (such as FBI's NCIC database)
Passenger Name Record Data (PNR data)
Commercial Data[c]
Data from government databases[d]
Treasury Enforcement Communications System (TECS)[b]
PURPOSE: identity matching
Advanced Targeting System-Passenger (ATS-P)
PURPOSE: identity matching and risk targeting
CBP Officers[a]
Conduct passenger inspections
Validate authenticity of travel documents
Make screening decisions
Create "lookout" alert flags on passengers of interest
Add information to government databases (e.g. TECS)
Continual data flow
Occasional data flow

Source: GAO.

[a] CBP officers can utilize TECS and ATS-P databases to enter "lookout" alert flags. Not all CBP officers have access to all of the databases listed.

[b] In the APIS privacy impact assessment, CBP defined APIS as a system. However, CBP officials later stated that APIS is not a system but rather data that are sent to the TECS to conduct identity matching.

[c] CBP officials stated that commercial data are only used in rare situations when a passenger's identity cannot be verified against other information.

[d] CBP officers use data from the TSC as needed to help confirm a passenger's identity.

CBP has stated that its public reporting on its use of APIS data complies with the Privacy Act through references to previously published Privacy Act notices about systems used during the prescreening process. However, these references are not sufficient because they do not fully disclose CBP's use of personal information during the prescreening process. Specifically, CBP stated that because APIS is a system within the Treasury Enforcement Communications System, it is described in the TECS system of records notice, which was published in October 2001. CBP also referenced a 2003 system of records notice for the DHS Arrival and Departure Information System (ADIS), which interfaces with TECS, but which CBP officials stated separately is not used by CBP in the passenger prescreening process. However, neither of these notices specifically describes CBP's passenger prescreening or the use of APIS or PNR data.

Although CBP has stated that its previous privacy disclosures sufficiently complied with federal privacy law, on November 2, 2006, DHS published a Privacy Act system of records notice for ATS. In addition, on November 22, 2006, DHS published a privacy impact assessment for ATS. Both of these documents refer to the ATS-P system used in CBP's aviation passenger prescreening process. These disclosures —released after CBP received an earlier version of this report—provide much more detailed information on ATS-P as compared with prior privacy disclosures. Nevertheless, CBP has still not published a system of records notice or a privacy impact assessment that comprehensively describes the entire prescreening process. For example, although CBP has published a privacy impact assessment for APIS and ATS, neither disclosure describes the combined use of APIS and PNR data in passenger prescreening decision-making. The disclosures also do not describe that during the prescreening process CBP officers are able to access personal data obtained from commercial providers.

Because CBP's development and operation of its international passenger prescreening process has not been accompanied by the publication of Privacy Act notices or E-Government Act privacy impact assessments that fully describe the use of personal data and the steps taken to protect privacy, the public may not be aware of the different ways that their information is being used or protected, as required by law. Although maintaining that their prior privacy disclosures were fully compliant with federal privacy law, CBP stated in May 2006, and DHS reiterated in its official comments to this report in January 2007, that CBP plans to revise the APIS privacy impact assessment and issue a system of records notice for APIS. However, no deadline has been given for when these steps will be completed. As CBP moves forward with future modifications to its prescreening process, it will be important for CBP to fully assess and disclose data privacy protections used in these prescreening programs as well.

Conclusions

Since the terrorist hijackings of aircraft on September 11, the United States and the rest of the world have uncovered new attempts to threaten the security of the commercial aviation system. These threats underscore the importance of continually reassessing the numerous security measures put into place to secure commercial aviation. One key security measure is the prescreening of passengers on international flights—an important step to ensure that high-risk passengers do not board international flights traveling to or from the United States. Another important effort involves ensuring that international and domestic prescreening programs are fully aligned to maximize their effectiveness and cost efficiency for the government, airline industry and passengers. In conjunction with conducting these important prescreening activities, DHS must also be vigilant about ensuring that it is in full compliance with public privacy requirements.

CBP is currently taking various and important steps to strengthen the international aviation passenger prescreening process. CBP's recent publication of a proposed rule for changing the procedures and timing for conducting passenger identity matching is an important step. Another important effort to strengthen the international aviation passenger prescreening process is aligning the process with TSA's new domestic prescreening program. Efforts to significantly expand the IAP may also strengthen the prescreening process, although CBP will need to ensure that sufficient data are collected to allow for appropriate risk assessments and evaluations.

While CBP recognizes and is taking steps to address many of the challenges it faces in implementing its various planned prescreening programs, there are three areas, in particular, that require further planning and monitoring. These areas include:

- **More fully incorporating risk management principles in the IAP pilot.** CBP is not benefiting from all of the information that could be learned from the pilot program and remains at risk of expanding the program or making IAP sites permanent without establishing a clear vision of what the program is intended to accomplish and how its success will be evaluated and measured. Without completing a strategic plan for the IAP, the program may not realize its full potential security benefits and could require substantial revisions after implementation.

- **Aligning international and domestic passenger prescreening programs.** If these two prescreening efforts are not effectively coordinated with each other, air carriers and other stakeholders could be unnecessarily inconvenienced and experience potentially avoidable costs. The U.S. government could incur avoidable costs as well, if the programs are not properly coordinated and aligned. So far, CBP and TSA have taken some steps to coordinate their efforts—for example, they have announced their intention to develop a single portal for prescreening passengers on domestic and international flights. However, CBP and TSA have not yet made all of the key decisions necessary to align the two processes nor have they completed a timetable for completing this process.

- **Attaining full compliance with privacy laws.** It is important that CBP completes reports that fully describe the agency's use and protection of personal data during the international passenger prescreening process to ensure that it is complying with all applicable privacy laws. CBP's current disclosures do not fully inform the public about all of its systems for prescreening aviation passenger information nor do they explain how CBP combines data in the prescreening process, as required by law. As a result, passengers are not assured that their privacy is protected during the international passenger prescreening process.

Recommendations for Executive Action

To strengthen CBP's international aviation passenger prescreening process, in our November 2006 report we recommended that the Secretary of the Department of Homeland Security take or direct the Commissioner of Customs and Border Protection to take the following three actions:

- To more fully incorporate risk management principles into the planning, implementation, and evaluation of the IAP pilot, CBP should (1) prepare a strategic plan that identifies the risks, goals, objectives, and performance measures for the IAP pilot, and (2) conduct program evaluations that measure the performance of the pilot IAP sites against predetermined goals and performance measures.

- To more fully align CBP's international aviation passenger prescreening program with TSA's prospective domestic aviation passenger prescreening program, take additional steps necessary to identify the remaining impediments to alignment, make the key policy and technical decisions needed to more fully coordinate these programs (including a determination of the data and identity matching technologies that will be used), and set time frames for when these efforts will be completed.

- To fully inform the public of possible uses of their personal information, ensure that all required public data privacy disclosures, including system of record notices and privacy impact assessments, are completed to adequately cover each element of the international passenger prescreening process. The privacy disclosures should fully describe the use and handling of personal information within the prescreening process and all of CBP's systems for conducting international passenger prescreening.

Agency Comments and Our Evaluation

We provided a draft of the security sensitive version of this report, and related updates, to DHS and DOJ. On January 31, 2007, we received written comments from DHS which are reproduced in full in Appendix IV. DHS generally concurred with the three report recommendations and provided technical comments, which we incorporated where appropriate. DOJ also provided technical comments, which we incorporated where appropriate.

Regarding the actions DHS reported taking to address the recommendations, DHS stated that it has completed an IAP Strategic Plan and that the plan has been sent for Departmental review. DHS provided a copy of the draft IAP Strategic Plan to GAO. While DHS stated that the draft strategic plan outlines the measures that CBP intends to use to assess the IAP's performance, it is not yet clear from the draft strategic plan how challenges as well as successes of the program will be measured at each IAP site. This appears to be the case since all of the performance measures outlined in the draft strategic plan are likely to improve following the deployment of IAP officers, without addressing program impediments. DHS also noted that CBP is developing system enhancements that will permit simple input, extraction, and analysis of empirical data necessary for baseline and current data. We are encouraged by these efforts and believe that they will help CBP to better evaluate the effectiveness of this pilot program. Moreover, given CBP's intention to transition this pilot program into a permanent one and expand the program to additional locations, it is important that IAP officers and those managing the IAP have the sufficient data necessary to make sound decisions.

Regarding the recommendation that steps be taken to more fully align CBP's international passenger prescreening program with TSA's domestic passenger prescreening program, DHS stated that its Screening Coordination Office has directed CBP and TSA to align these programs. DHS further stated that CBP has been working with TSA to align procedures and systems and functional requirements, and that both CBP and TSA will work with the Centers for Disease Control and Prevention to harmonize data requirements and present a single face to the travel industry. DHS also noted that CBP recognizes that air carriers have invested significant resources to reprogram systems to comply with CBP's regulations, and that CBP will continue to work to allow for the submission of various passenger data through one transmission process. Given the potential costs to air carriers and the government of having prescreening procedures and requirements that are not aligned, we encourage DHS to complete these efforts and make associated policy decisions in a timely manner.

Regarding the recommendation that the public be fully informed of the possible uses of its personal information and that all required public data privacy disclosures are completed to adequately address each element of the international passenger prescreening process, DHS responded with several statements. CBP stated in its comments on the draft report that it is and has been in compliance with both the Privacy Act regarding System of Records Notices (SORNs) and section 208 of the E-Government Act of 2002 regarding Privacy Impact Assessments (PIAs). CBP bases its compliance with the Privacy Act on the 2001 publication of a SORN for the Treasury Enforcement Communications System (TECS). To the extent that all uses of personal information in CBP international passenger prescreening can be associated with the statements made in that notice, we would agree that CBP is in compliance with the law. That notice, however, states that TECS contains "[e]very possible type of information from a variety of Federal, state, and local sources, which contribute to effective law enforcement." This statement does not identify the categories of records maintained in the system, as required by the Act, let alone APIS and ATS, which CBP now describes as separate systems. It also does not disclose that the system includes personal information collected directly from individuals (i.e., passport data) and indirectly through air carriers (i.e., PNR data). The TECS SORN does not "facilitate the exercise of the rights of individuals" under the Act, as required by OMB's Privacy Act guidance.[23] While OMB guidance states that agencies are granted considerable discretion in preparing SORNS, the guidance stresses the importance of appropriately identifying the purpose(s) of a system and ensuring that any associated notices have "information value to the public." According to OMB, a major purpose of the Act is "the publicizing of what those systems are and how they are used." The TECS SORN has virtually no information value to the public and cannot be said to meet the requirements of the Act.

CBP also stated in its comments that no PIA is required for its prescreening process because the March 2005 APIS PIA addressed changes to APIS, and there have been no changes to ATS since the E-Government Act went into effect.[24] This is incorrect for at least two reasons. First, CBP's handling of personal information was significantly altered on the basis of its July 2004 agreement with the EU regarding handling PNR data from flights between the US and EU member countries.[25] The DHS Privacy Office's September 2005 report on the handling of EU PNR describes a number of changes made to CBP systems and processes to better safeguard such data. These changes are not addressed in any new or revised PIA or SORN. Second, the privacy documents that CBP has published do not fully describe the use of personal information in the CBP international passenger prescreening

[23] 40 Fed. Reg. 28948, 28952, July 9, 1975.

[24] CBP states that the ATS PIA was conducted merely to satisfy a DHS requirement that new SORNs be accompanied by PIAs, again, not because of any change to ATS that would require a PIA under the terms of the E-Gov Act.

[25] 69 Fed. Reg. 41543, July 9, 2004.

process, even accepting CBP's statutory authority to limit public disclosures under certain circumstances.[26] Contrary to CBP's characterization of CBP officers as merely conducting an "act of physical inspection," the CBP international passenger prescreening process involves decisions made by CBP officers on the basis of information obtained from multiple sources. As described in our report, CBP officers can retrieve identity matching information conducted with APIS data, identity matching and risk targeting information performed by ATS with PNR and APIS data, as well as information from other government databases. They can also access commercial data sources, although reportedly on a limited basis for confirming passenger identities. Finally, they can also enter information about individuals back into a number of government systems.[27] These multiple uses of information are not described in any CBP privacy documents. Despite CBP's statement to the contrary, there are no legal limitations to the Privacy Act or the E-Government Act that constrain the agency's ability to provide the public with meaningful notice on the use and protection of personal information.[28] Furthermore, given that the handling of personal information in the CBP prescreening process has been significantly changed multiple times in the last several years, including changes to address the EU PNR agreement and changes to the collection of passenger manifest information via APIS, the separate publication of APIS and ATS privacy documents satisfy the requirements of neither the Privacy Act nor the E-Government Act.

Upon its issuance, we will provide copies of this report to the Secretary of the Department of Homeland Security, the Commissioner of Customs and Border Protection, the Administrator of the Transportation Security Administration, and interested congressional committees.

[26] The extent of an agency's public description of a system of records can be limited by exemptions permitted by the Privacy Act, e.g., an agency can claim an exemption from the requirement to describe the categories of sources of records for investigative material compiled for law enforcement purposes. 5 U.S.C. § 552a(k).

[27] As noted in DHS Privacy Office's PIA guidance, privacy concerns can be raised where technology may only collect personal information for a moment.

[28] For example, under these laws and their implementing guidance, CBP's modification of its systems and processes to comply with the 2004 EU agreement on the use of European PNR data should have led CBP to issue a revised SORN and conduct a PIA.

If you have any questions about this report, please contact me at BerrickC@gao.gov or (202) 512-3404. Key contributors to this report are listed in appendix V.

Cathleen A. Berrick

Cathleen A. Berrick
Director, Homeland Security and Justice Issues

Appendix I: Objectives, Scope, and Methodology

The information contained in this public report is narrower in scope and detail than the original report and examines only limited aspects of international passenger prescreening procedures. It focuses on only certain elements of the current international aviation passenger prescreening process as well as only some of the actions that DHS is taking or has planned to strengthen prescreening procedures. More specifically the report's content is limited to certain issues related to:

- the implementation of the Immigration Advisory Program (IAP), a CBP program that assesses risk levels for certain passengers in overseas locations;
- aligning international and domestic passenger prescreening programs;
- ensuring that compliance with privacy laws is fully achieved with respect to information collected to conduct international passenger prescreening.

Although the information provided in this report is more limited in scope, the overall methodology used for our initial report is relevant to this report as well because the information contained in this report was derived from the initial sensitive report. We addressed the following objectives in our initial November 2006 report:

- the main factors affecting the international passenger prescreening process, and the potential impact of these factors, and
- the status of efforts to address these factors, and the issues, if any, that could affect efforts to strengthen the international prescreening process.

To address our first objective from the November 2006 report—the factors that affect the international passenger prescreening process and their potential impacts—we interviewed officials from Customs and Border Protection (CBP), including staff at CBP's National Targeting Center (NTC); the Terrorist Screening Center (TSC); and the Transportation Security Administration (TSA) to understand the current international passenger prescreening process and the data that are used during this process. We obtained and analyzed relevant documents from these agencies including statistics from the Immigration Advisory Program pilot, documentation on CBP's use of data systems to conduct international passenger prescreening, and a CBP summary memorandum documenting the agency's decision not to pursue the Advanced Passenger Prescreening

(APP) system that currently operates in other countries such as Australia and New Zealand. To obtain a cross section of air carriers' views about the process, we selected air carriers that fly large, medium, and small numbers of passengers annually into the United States. For the purposes of this review, we defined the transport of a large number of passengers as more than 1 million passengers annually, we defined a medium number as between 500,000 and 1 million passengers annually, and a small number as less than 500,000 passengers annually. These criteria generally reflect the distribution of the incoming passenger volume being flown into the United States between 2000 and 2004 as shown in Department of Transportation statistical reports. Using these criteria, we interviewed officials from seven large air carriers, four medium air carriers, and two small air carriers, both domestic and foreign, that conduct international flights into and out of the United States to discuss the impact of current U.S. international passenger prescreening requirements on their operations. We also spoke with officials from two domestic air carrier and passenger travel associations and three international air carrier associations to discuss the impact on their members of current international passenger prescreening requirements. We also reviewed documents from an international aviation association that evaluated the potential impact on its membership of CBP's proposed passenger prescreening reforms. To determine the number of No Fly and improperly prescreened Selectee passengers who traveled on flights to or from the United States during 2005, we obtained and analyzed TSA security incident reports from January 1, 2005 to December 31, 2005.[1]

To address our second objective from the November 2006 report— the status of CBP's efforts to address these factors and the issues, if any, that could affect efforts to strengthen the prescreening process—we interviewed officials from CBP and reviewed relevant documents. We also interviewed officials from the seven large air carriers, three medium air carriers, and two small air carriers, both domestic and foreign, that conduct international flights into and out of the United States to obtain their views on the potential impact of future U.S. international prescreening requirements. We also spoke with officials from two domestic air carrier and passenger travel associations, three international air carrier associations, and a travel association that represent the interests of air carriers and travelers to obtain their views on the potential

[1] We did not report on the details of this passenger information as it is sensitive security information.

impact of future U.S. international prescreening requirements including APIS- 60 and AQQ. We visited two Immigration Advisory Program (IAP) pilot sites and met with the IAP teams to discuss the current status of the program and observe the prescreening process at their respective locations. We discussed potential benefits and challenges of the program with the IAP teams. We also reviewed and assessed CBP's evaluations of IAP pilot sites. Furthermore, we met with government officials from the United Kingdom and Canada to learn details about their respective airline liaison officer (ALO) programs and to obtain their views on how the IAP pilot compares with their ALO programs. One foreign government provided documents that summarize the functions of its ALO program. We also met with foreign government officials in the Netherlands, Poland, the United Kingdom, Australia, and New Zealand to discuss U.S. efforts to strengthen international passenger prescreening and the potential impact of these programs. Officials from Australia and New Zealand also provided documents related to their respective APP prescreening systems. We met with officials from the European Union to discuss the impact of U.S. international prescreening requirements (including the advanced transmission of passenger name record data) on air carriers originating from Europe. Additionally, we interviewed and obtained documents from private companies that facilitate the electronic transmission of passenger data between air carriers and government agencies, including CBP, to determine their role, if any, in future international aviation passenger prescreening initiatives. To assess CBP's July 2006 Notice of Proposed Rulemaking (NPRM), we obtained and analyzed documents associated with the NPRM, including CBP's regulatory assessment for the rulemaking. To assess whether CBP disclosed, as required by law, its use of passenger information during the prescreening process, we reviewed CBP's published privacy impact assessments and system of records notices. We also met with CBP and DHS officials regarding their current and draft privacy documents related to passenger prescreening. To determine the extent to which CBP has utilized risk management principles to guide decisions on passenger prescreening, we used a risk management framework developed and tested by GAO over several years.[2] The risk management framework was developed by GAO after a review of

[2] GAO, *Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection*, GAO-04-557T (Washington, D.C.: Mar. 31, 2004).

GAO, *Risk Management: Further Refinements Needed to Asses Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, GAO-06-91 (Washington, D.C.: Dec. 15, 2005).

government and private sector documents on risk management and interviews with recognized experts in risk management and terrorism prevention. We used elements of the risk management framework as criteria to analyze CBP's actions in developing and implementing its existing international passenger prescreening process, as well as CBP's proposed and planned actions to modify the international passenger prescreening process. We conducted our work, which included updates to our version of the report that contains sensitive security information, from April 2005 through November 2006 in accordance with generally accepted government auditing standards.

Appendix II: Airline Liaison Officer Programs Implemented In Other Countries

Several countries have created airline liaison officer (ALO) programs and placed officers in foreign countries to reduce the number of improperly documented passengers traveling into their respective countries. These officers also assist air carrier staff in establishing whether individual passengers who may appear to be improperly documented are actually eligible to fly without resulting in fines to the air carrier. According to the International Air Transport Association Code of Conduct for Immigration Liaison Officers, the liaison officers' primary responsibilities include:

- Establishing and maintaining a good working relationship with the airlines, local immigration, police, other appropriate authorities, and other liaison officers posted to that country and with consular staff of other missions. Additionally, liaison officers assist local immigration and police authorities in gathering and sharing information related to the movement of improperly documented passengers.

- Training airline staff in the general principles of passport and visa requirements, passenger assessment, and awareness of fraud and forgery, and advising airline staff on whether travel documents and visas are genuine, forged or fraudulently obtained.

Table 1 shows a side-by-side comparison of the characteristics of ALO programs from four countries.

Table 1: The Characteristics of Selected ALO Programs

Characteristics	U.K. Airline Liaison Officer Program	Canadian Migration Integrity Program	Australian Airline Liaison Officer Program	New Zealand Airline Liaison Officer Program
Initiation date	1993	1989	1989	1991
Number of locations	32	39	14	9
Approximate number of staff	34	45	20	9
Number of officers at each location	1-2	1-2	1-2	1
Physical location of staff	At nearest embassy	At nearest embassy	At airport	At nearest embassy or with an air carrier
Mission	Reduce travel document fraud	Reduce travel document fraud	Reduce travel document fraud	Reduce number of refugee cases

Source: GAO analysis of ALO programs.

These ALO programs have incorporated various approaches regarding data collection, program expansion, and staffing to allow for continuous improvement and measurement of their liaison programs. For example, the Canadian Migration Integrity Officers (MIO) program developed a system that regularly collects data on improperly documented arrivals in Canada and other suspect travelers and records this information in a Web database to develop trend and other analyses. These data are also used to measure the success of the Canadian MIO program. Canadian officials stated that this web-based database allows Canada to immediately inform air carriers of violations, has assisted in reducing the number of violations and fines, and has allowed air carriers to take corrective action in a timely manner. Similarly, officials from the United Kingdom ALO program stated that they also collect statistics and intelligence to develop profiles and trends on particular flights for use in their program. The New Zealand ALO program utilizes passenger name record (PNR) data to identify the trends of travelers utilizing fraudulent passports to travel to their country. New Zealand officials stated that accessing and using PNR data in real time has allowed their ALO network to immediately load alert or referral information into its passenger-screening system so that identified passengers can be screened further at check-in prior to boarding. New Zealand officials also stated that they utilize data to conduct assessments and intensive reviews of the highest risk countries and passengers, which they then use to determine the location of airline liaison sites. Some New Zealand ALO sites also have direct access to the immigration application system, which allows their liaison officers to directly input alerts as necessary. The New Zealand government is also currently considering providing ALO officers with handheld computers to facilitate more efficient communications. Australian officials stated that at several of their ALO sites the liaison officers work under a particular air carrier versus going through the typical approval process needed to establish an overseas program, which may take a long time to complete. According to these officials, this type of arrangement provides them with the advantage of being able to quickly move liaison officers from location to location when needed to keep up with trends in illegal passenger travel. Both the United Kingdom and the Canadian ALO programs expanded gradually. A United Kingdom ALO program official validated this approach by suggesting that limited growth of ALO programs during the initial stages allowed countries to fully learn from the pilot program before expanding to other countries.

Appendix III: APIS Quick Query (AQQ) and APIS Minus 60 Minutes (APIS-60)

In July 2006, CBP released a notice of proposed rulemaking that would require air carriers to transmit APIS data to CBP prior to the departure of all international flights departing from or bound for the United States. The notice of proposed rulemaking provided air carriers with two main options for prescreening passengers on international flights prior to departure. One option under the proposed rule would require air carriers to send APIS data on all passengers to CBP 60 minutes before a flight's departure. The other option would allow air carriers to transmit APIS data on a passenger-by-passenger basis, up to 15 minutes prior to a flight's departure. The two options are designed to accommodate air carriers with different types of operations.[1]

Under both options, CBP has broadly outlined the procedures for air carriers to receive a "not-cleared" response which would identify that a passenger is prohibited from boarding an aircraft. CBP would provide this response to the air carrier prior to the passenger boarding the aircraft. In addition to satisfying requirements under the Intelligence Reform and Terrorism Prevention Act, both options would strengthen the prescreening process.

First Prescreening Option: Transmitting APIS Data 60 Minutes Prior to Departure

The first option under the proposed rule would require air carriers to transmit APIS data to CBP for all passengers on a flight 60 minutes prior to the flight's departure. This approach is known as APIS-60. The APIS-60 option will require an air carrier to transmit a manifest to CBP with APIS information for all passengers on the flight 60 minutes before the flight departs. This option gives CBP staff approximately 60 minutes before flight departures to match the APIS information against the lists and notify the carrier if any passengers should not be allowed to travel. Under this option, a passenger would be issued a boarding pass, but if a "not cleared" response is later received from CBP, the air carrier would be responsible for denying boarding, or for removing the passenger and his or her

[1] Under the current international passenger prescreening process, CBP has identified some air carriers whose reservation systems do not allow them to send passenger APIS data to CBP through a batched electronic transmission. These air carriers include seasonal charters, air taxis, and air ambulances. CBP allows these air carriers to transmit passenger data through other means, such as through e-mail, in a program called eAPIS. In its NPRM, CBP noted that such air carriers are not likely to be able to adopt either the APIS-60 or AQQ prescreening options. Consequently, these air carriers will be permitted to continue to send passenger data through eAPIS, but they will still be bound by the requirement to transmit APIS data 60 minutes prior to departure and they must be able to receive CBP's identity matching results through e-mail or telephone.

baggage from the aircraft, if the passenger had already boarded the aircraft. This option, according to CBP officials, is likely to be preferred by smaller air carriers that are not dependent on having passengers transfer from connecting flights (and therefore whose passengers would not likely have difficulty checking in at least 60 minutes before flight departure). According to CBP officials, these air carriers might prefer APIS-60 because it would not require technical changes in how they transmit APIS data to CBP, although it would require that carriers develop the technical means to receive a screening response from CBP. In the fall of 2004, CBP initially proposed APIS-60 as the sole approach for conducting international prescreening. However, the International Air Transport Association (IATA), the Air Transport Association of America (ATA),[2] and individual air carriers raised concerns about the economic impacts they believed would be associated with implementing APIS-60 across the industry. For example, they told CBP that network flight schedules would have to change to expand the minimum connection times between flights because all passengers would be required to check in at the airport at least 1 hour in advance of the flight so that information could be collected and sent to CBP on time. Air carriers that carry passengers arriving on connecting flights, which are known to operate on “hub-and spoke” networks,[3] said that they would be particularly affected because their passengers could arrive on a variety of connecting flights from many other airports, and some would not arrive 60 minutes in advance of their connecting flight, making them ineligible to board their scheduled flights. In addition, according to some air carriers, the trend in the air carrier industry of moving toward self-service check-in by some passengers has shortened the time between check-in and scheduled flight departure times, further exacerbating the impact of this type of approach. In response to industry concerns that the APIS-60 approach would create serious problems for some carriers’ operations, CBP offered a second option for air carriers to

[2] IATA represents the airline industry and comprises 260 passenger and cargo air carriers, representing 94 percent of international scheduled air traffic. ATA is the nation’s largest airline trade association and its stated purpose is to foster a business and regulatory environment that ensures safe and secure air transportation.

[3] With a hub-and-spoke network, air carriers can combine local passengers (those passengers originating at or destined for the hub), with connecting passengers (those not originating at or destined for the hub but traveling via the hub) on the same flight. In this manner, carriers can serve more cities and offer greater frequency of service with their fleet of aircraft than is possible with point-to-point service, which is service from one city to another without this connecting network.

consider adopting to conduct passenger prescreening in advance of flight departures.

Second Prescreening Option: Transmitting APIS Data as Each Passenger Checks In for a Flight

The second option under the proposed rule would require air carriers to send APIS data to CBP as each passenger checks in for a flight. CBP would then complete its identity match against the No Fly and Selectee Lists and send a response to the air carrier—generally within 4 seconds—identifying that the passenger is either cleared or not-cleared for boarding. Since this approach would utilize a nearly instantaneous data transmission between air carriers and CBP, it is known as a real-time prescreening option.[4] For those passengers found to be eligible to board, the response message from CBP would identify that the air carrier is permitted to issue a boarding pass and receive checked-in luggage from the passenger.[5] Known as APIS Quick Query (AQQ), this approach would represent a significant change to the current prescreening process in that CBP would complete its identity matching for each passenger separately, instead of conducting identity matching for all passengers on a flight at the same time.

CBP officials believe that larger carriers with hub-and-spoke operations are the most likely to choose the AQQ option, in part because larger carriers are more likely to have the communications infrastructure needed to develop and install the new interactive system. Some air carriers have expressed the desirability of receiving a real-time cleared/not cleared response from CBP earlier in the prescreening process such as what AQQ would provide. This timing would allow them to know almost immediately if an identified passenger represents a potential security risk.

CBP officials are already in the process of developing the AQQ system. Under this approach, the federal government would bear the costs associated with the actual prescreening of passengers. However, air carriers would be responsible for any changes needed to their internal information technology systems and the transmission of APIS data. This type of real-time interactive prescreening approach is currently in use in

[4] It is also known as an interactive approach, because CBP transmits a response message back to air carriers informing them whether a passenger can board or not board.

[5] Passengers whose identities matched the No Fly List from this initial screening would not be issued a boarding pass by the air carrier until CBP and other agencies completed their identity vetting procedures and returned a message to the air carrier identifying that it was okay to board the passenger. If this identity verification process is not completed prior to the flight's departure, the passenger would not be permitted to travel on the flight.

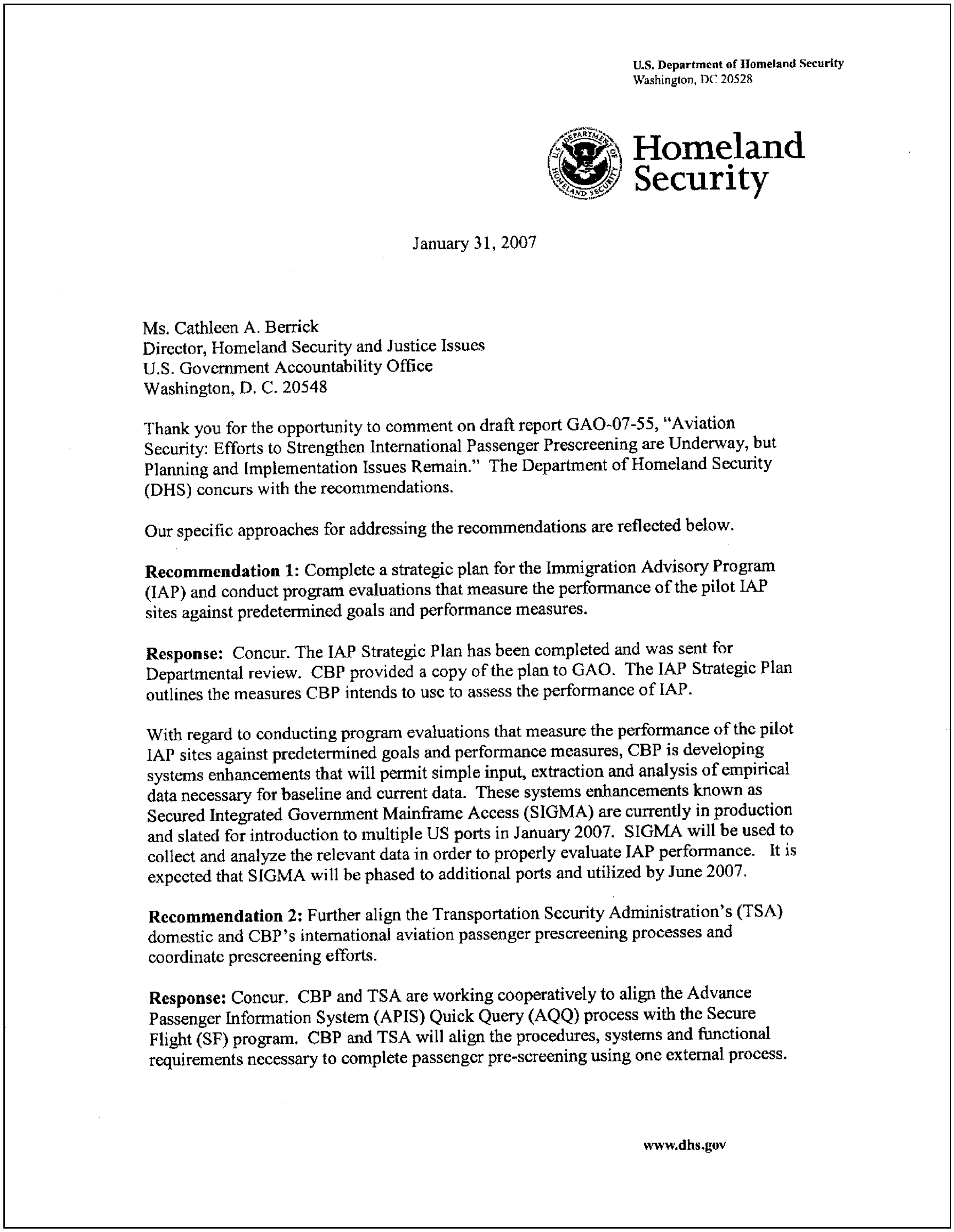
several countries, including Australia, New Zealand, and Bahrain, through a system called Advance Passenger Processing (APP). The APP system was initially used by Australia's Customs Service and Department of Immigration and Multicultural and Indigenous Affairs, and was first implemented in 1995.

AQQ and APP are both real-time interactive concepts but are different systems. CBP officials stated that they considered APP when determining which prescreening options to pursue but, in an August 2005 memorandum, identified a number of reasons for not adopting it.[6] Nonetheless, the experience of these other countries with APP may be of value to CBP as it continues to develop the AQQ program. For example, Australian government officials told us that the successful deployment of the APP program was dependent upon working closely with air carriers to ensure system functionality upon implementation. This will be particularly important with regard to the AQQ given that almost 200 air carriers fly international routes into and out of the United States, assuming that a number of these air carriers decide to participate in AQQ.[7] Officials from Australia and New Zealand said that they were willing to continue to share relevant lessons learned as CBP works to develop its AQQ program.

[6] Some of the reasons CBP cited for not adopting APP included high infrastructure and transaction costs to both air carriers and government, and the system's inability to adjudicate possible matches and allow for human intervention and response. Although CBP's memo refers to an evaluation of APP conducted by its Office of Field Operations and Office of Information Technology, CBP did not provide us with the supporting documentation of this evaluation despite a request for relevant documentation in its considerations of implementing APP.

[7] CBP estimated that 1,280 foreign and domestic air carriers will be affected by its proposed rulemaking related to AQQ and APIS-60.

Appendix IV: Comments from the Department of Homeland Security



U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

January 31, 2007

Ms. Cathleen A. Berrick
Director, Homeland Security and Justice Issues
U.S. Government Accountability Office
Washington, D. C. 20548

Thank you for the opportunity to comment on draft report GAO-07-55, "Aviation Security: Efforts to Strengthen International Passenger Prescreening are Underway, but Planning and Implementation Issues Remain." The Department of Homeland Security (DHS) concurs with the recommendations.

Our specific approaches for addressing the recommendations are reflected below.

Recommendation 1: Complete a strategic plan for the Immigration Advisory Program (IAP) and conduct program evaluations that measure the performance of the pilot IAP sites against predetermined goals and performance measures.

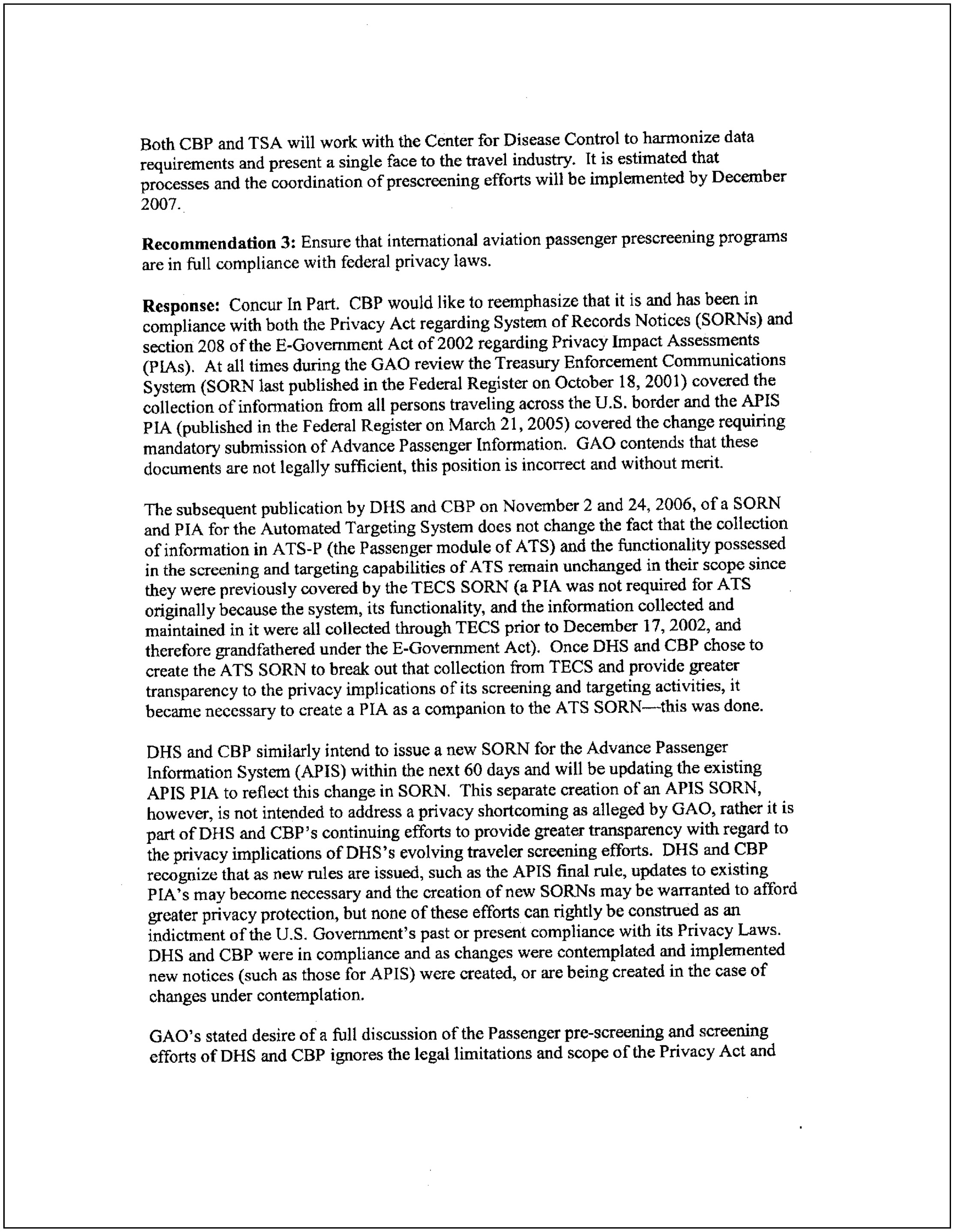
Response: Concur. The IAP Strategic Plan has been completed and was sent for Departmental review. CBP provided a copy of the plan to GAO. The IAP Strategic Plan outlines the measures CBP intends to use to assess the performance of IAP.

With regard to conducting program evaluations that measure the performance of the pilot IAP sites against predetermined goals and performance measures, CBP is developing systems enhancements that will permit simple input, extraction and analysis of empirical data necessary for baseline and current data. These systems enhancements known as Secured Integrated Government Mainframe Access (SIGMA) are currently in production and slated for introduction to multiple US ports in January 2007. SIGMA will be used to collect and analyze the relevant data in order to properly evaluate IAP performance. It is expected that SIGMA will be phased to additional ports and utilized by June 2007.

Recommendation 2: Further align the Transportation Security Administration's (TSA) domestic and CBP's international aviation passenger prescreening processes and coordinate prescreening efforts.

Response: Concur. CBP and TSA are working cooperatively to align the Advance Passenger Information System (APIS) Quick Query (AQQ) process with the Secure Flight (SF) program. CBP and TSA will align the procedures, systems and functional requirements necessary to complete passenger pre-screening using one external process.

www.dhs.gov



Both CBP and TSA will work with the Center for Disease Control to harmonize data requirements and present a single face to the travel industry. It is estimated that processes and the coordination of prescreening efforts will be implemented by December 2007.

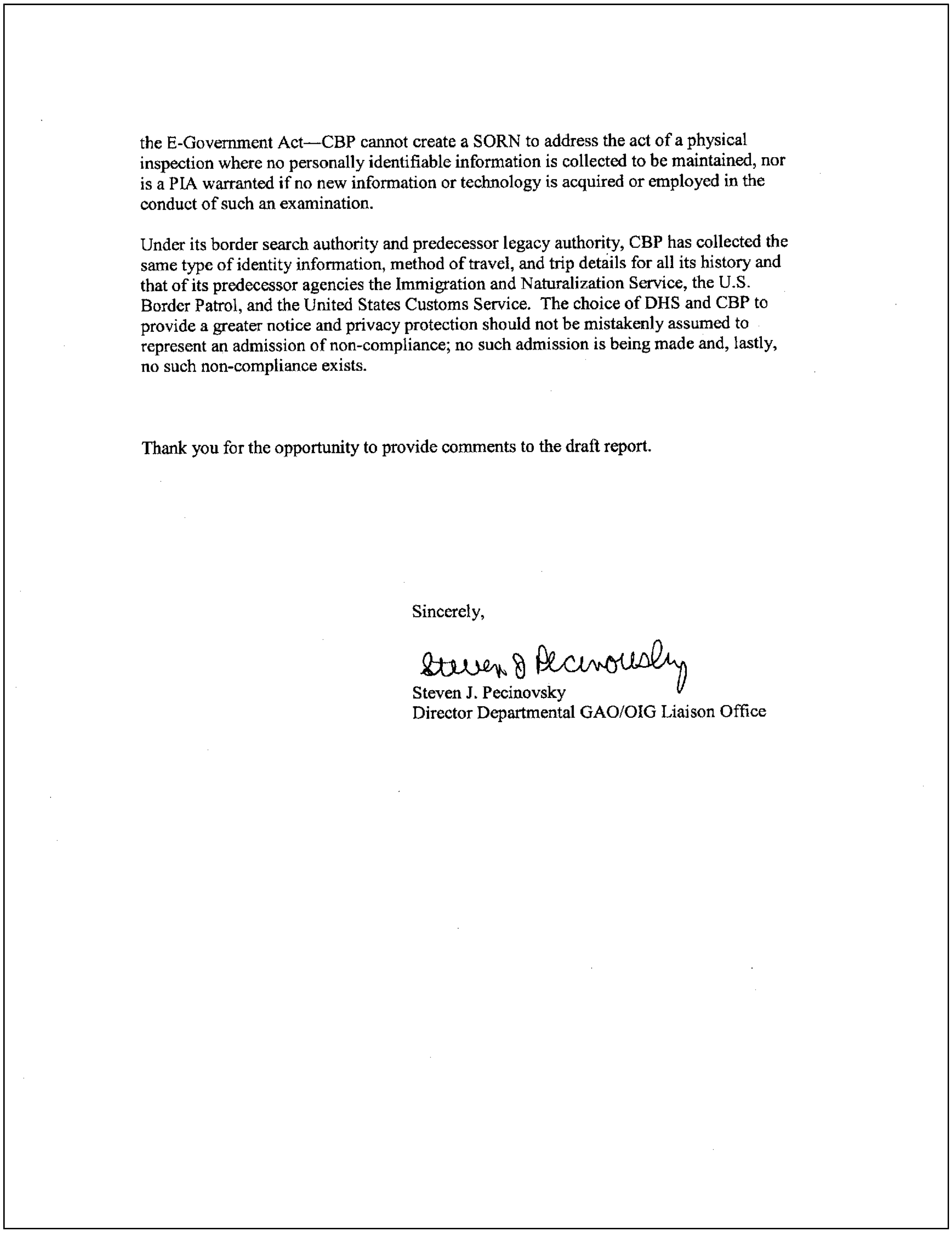
Recommendation 3: Ensure that international aviation passenger prescreening programs are in full compliance with federal privacy laws.

Response: Concur In Part. CBP would like to reemphasize that it is and has been in compliance with both the Privacy Act regarding System of Records Notices (SORNs) and section 208 of the E-Government Act of 2002 regarding Privacy Impact Assessments (PIAs). At all times during the GAO review the Treasury Enforcement Communications System (SORN last published in the Federal Register on October 18, 2001) covered the collection of information from all persons traveling across the U.S. border and the APIS PIA (published in the Federal Register on March 21, 2005) covered the change requiring mandatory submission of Advance Passenger Information. GAO contends that these documents are not legally sufficient, this position is incorrect and without merit.

The subsequent publication by DHS and CBP on November 2 and 24, 2006, of a SORN and PIA for the Automated Targeting System does not change the fact that the collection of information in ATS-P (the Passenger module of ATS) and the functionality possessed in the screening and targeting capabilities of ATS remain unchanged in their scope since they were previously covered by the TECS SORN (a PIA was not required for ATS originally because the system, its functionality, and the information collected and maintained in it were all collected through TECS prior to December 17, 2002, and therefore grandfathered under the E-Government Act). Once DHS and CBP chose to create the ATS SORN to break out that collection from TECS and provide greater transparency to the privacy implications of its screening and targeting activities, it became necessary to create a PIA as a companion to the ATS SORN—this was done.

DHS and CBP similarly intend to issue a new SORN for the Advance Passenger Information System (APIS) within the next 60 days and will be updating the existing APIS PIA to reflect this change in SORN. This separate creation of an APIS SORN, however, is not intended to address a privacy shortcoming as alleged by GAO, rather it is part of DHS and CBP's continuing efforts to provide greater transparency with regard to the privacy implications of DHS's evolving traveler screening efforts. DHS and CBP recognize that as new rules are issued, such as the APIS final rule, updates to existing PIA's may become necessary and the creation of new SORNs may be warranted to afford greater privacy protection, but none of these efforts can rightly be construed as an indictment of the U.S. Government's past or present compliance with its Privacy Laws. DHS and CBP were in compliance and as changes were contemplated and implemented new notices (such as those for APIS) were created, or are being created in the case of changes under contemplation.

GAO's stated desire of a full discussion of the Passenger pre-screening and screening efforts of DHS and CBP ignores the legal limitations and scope of the Privacy Act and



the E-Government Act—CBP cannot create a SORN to address the act of a physical inspection where no personally identifiable information is collected to be maintained, nor is a PIA warranted if no new information or technology is acquired or employed in the conduct of such an examination.

Under its border search authority and predecessor legacy authority, CBP has collected the same type of identity information, method of travel, and trip details for all its history and that of its predecessor agencies the Immigration and Naturalization Service, the U.S. Border Patrol, and the United States Customs Service. The choice of DHS and CBP to provide a greater notice and privacy protection should not be mistakenly assumed to represent an admission of non-compliance; no such admission is being made and, lastly, no such non-compliance exists.

Thank you for the opportunity to provide comments to the draft report.

Sincerely,

Steven J Pecinovsky

Steven J. Pecinovsky
Director Departmental GAO/OIG Liaison Office

Appendix V: GAO Contacts and Staff Acknowledgments

GAO Contacts

Cathleen A. Berrick, Director, Homeland Security and Justice Issues, (202) 512-3404

Staff Acknowledgments

In addition to the individual named above, key contributors to the report include Mark Abraham, Charles Bausell, Dawn Hoff, David Hooper, Michele Fejfar, James Madar, Jan Montgomery, Hugh Paquette, David Plocher, Neetha Rao, Brian Sklar, and Stan Stenersen.

GAO Related Products

Aviation Security: Progress Made in Systematic Planning to Guide Key Investment Decisions, but More Work Remains. GAO-07-448T. Washington, D.C.: February 13, 2007.

Homeland Security: Progress Has Been Made to Address the Vulnerabilities Exposed by 9/11, but Continued Federal Action Is Needed to Further Mitigate Security Risks. GAO-07-375. Washington, D.C.: January 2007.

Transportation Security Administration's Office of Intelligence: Responses to Post Hearing Questions on Secure Flight. GAO-06-1051R. Washington D.C.: August 4, 2006.

Terrorist Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public. GAO-06-1031. Washington, D.C.: Sept. 29, 2006.

Border Security: Stronger Actions Needed to Assess and Mitigate Risks of the Visa Waiver Program. GAO-06-1090T. Washington, D.C.: September 7, 2006.

Border Security: Stronger Actions Needed to Assess and Mitigate Risks of the Visa Waiver Program. GAO-06-084. Washington, D.C.: July 2006.

Process for Admitting Additional Countries into the Visa Waiver Program. GAO-06-835R Washington, D.C.: July 2006.

Aviation Security: TSA Oversight of Checked Baggage Screening Procedures Could Be Strengthened. GAO-06-869.Washington, D.C.: July 28, 2006.

Aviation Security: Management Challenges Remain for the Transportation Security Administration's Secure Flight Program. GAO-06-864T. Washington D.C.: June 14, 2006.

Aviation Security: Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program. GAO-06-374T. Washington, D.C.: Feb. 9, 2006.

Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information During Secure Flight Program Testing in Initial Privacy Notes, but Has Recently Taken Steps to More Fully Inform the Public. GAO-05-864R. Washington, D.C.: July 22, 2005.

Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed. GAO-05-356. Washington, D.C.: March 28, 2005.

Aviation Security: Measures for Testing the Effect of Using Commercial Data for the Secure Flight Program. GAO-05-324. Washington, D.C.: Feb. 23, 2005.

Transportation Security: Systematic Planning Needed to Prioritize Resources. GAO-05-357T. Washington, D.C.: February 15, 2005.

General Aviation Security: Increased Federal Oversight is Needed, but Continued Partnership with the Private Sector is Critical to Long-Term Success. GAO-05-144. Washington, D.C.: November 10, 2004.

Aviation Security: Challenges in Using Biometric Technologies. GAO-04-785T. Washington, D.C.: May 19, 2004.

Aviation Security: Improvement Still Needed in Federal Aviation Security Efforts. GAO-04-592T. Washington, D.C.: March 30, 2004.

Aviation Security: Challenges Delay Implementation of Computer-Assisted Passenger Prescreening System. GAO-04-504T. Washington, D.C.: March 17, 2004.

Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges. GAO-04-385. Washington, D.C.: Feb. 13, 2004.

Forum on High Performing Organizations: Metrics, Means, and Mechanisms for Achieving High Performance in the 21st Century Public Management Environment, GAO-04-343SP. Washington, D.C.: Feb. 13, 2004.

Aviation Security: Efforts to Measure Effectiveness and Strengthen Security Programs. GAO-04-285T. Washington, D.C.: Nov. 20, 2003.

Aviation Security: Efforts to Measure Effectiveness and Address Challenges. GAO-04-232T. Washington, D.C.: Nov. 5, 2003.

Aviation Security: Progress Since September 11, 2001, and the Challenges Ahead. GAO-03-1150T. Washington, D.C.: Sept. 9, 2003.

Airport Finance: Past Funding Levels May Not Be Sufficient to Cover Airports' Planned Capital Development. GAO-03-497T. Washington, D.C.: Feb. 25, 2003.

Commercial Aviation: Financial Condition and Industry Responses Affect Competition. GAO-03-171T. Washington, D.C.: Oct. 2, 2002.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:	Voice:	(202) 512-6000
	TDD:	(202) 512-2537
	Fax:	(202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON ♻ RECYCLED PAPER