United States Government Accountability Office

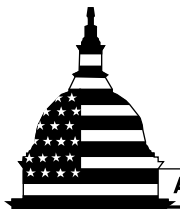
GAO

Report to Congressional Requesters

May 2012

# TERRORIST WATCHLIST

# Routinely Assessing Impacts of Agency Actions since the December 25, 2009, Attempted Attack Could Help Inform Future Efforts



G A O

Accountability * Integrity * Reliability

GAO-12-476

May 2012

# TERRORIST WATCHLIST

## Routinely Assessing Impacts of Agency Actions since the December 25, 2009, Attempted Attack Could Help Inform Future Efforts

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-476, a report to congressional requesters

### Why GAO Did This Study

The December 25, 2009, attempted bombing of Northwest Flight 253 exposed weaknesses in how the federal government nominated individuals to the terrorist watchlist and gaps in how agencies used the list to screen individuals to determine if they posed a security threat. In response, the President tasked agencies to take corrective actions. GAO was asked to assess (1) government actions since the incident to strengthen the nominations process, (2) how the composition of the watchlist has changed based on these actions, and (3) how agencies are addressing gaps in screening processes. GAO analyzed government reports, the guidance used by agencies to nominate individuals to the watchlist, data on the volumes of nominations from January 2009 through May 2011, the composition of the list, and the outcomes of screening agency programs. GAO also interviewed officials from intelligence, law enforcement, and screening agencies to discuss changes to policies, guidance, and processes and related impacts on agency operations and the traveling public, among other things. This report is a public version of the classified report that GAO issued in December 2011 and omits certain information, such as details on the nominations guidance and the specific outcomes of screening processes.

### What GAO Recommends

GAO recommends that the Assistant to the President for Homeland Security and Counterterrorism ensure that the outcomes and impacts of agencies' actions to strengthen nominations and screening processes are routinely assessed. Technical comments were provided and incorporated.

View GAO-12-476. For more information, contact Eileen Larence at (202) 512-6510 or larenceej@gao.gov.

### What GAO Found

In July 2010, the federal government finalized guidance to address weaknesses in the watchlist nominations process that were exposed by the December 2009 attempted attack and to clarify how agencies are to nominate individuals to the watchlist. The nominating agencies GAO contacted expressed concerns about the increasing volumes of information and related challenges in processing this information. Nevertheless, nominating agencies are sending more information for inclusion in the terrorist watchlist after the attempted attack than before the attempted attack. Agencies are also pursuing staffing, technology, and other solutions to address challenges in processing the volumes of information. In 2011, an interagency policy committee began an initiative to assess the initial impacts the guidance has had on nominating agencies, but did not provide details on whether such assessments would be routinely conducted in the future. Routine assessments could help the government determine the extent to which impacts are acceptable and manageable from a policy perspective and inform future efforts to strengthen the nominations process.

After the attempted attack, federal agencies took steps to reassess the threat posed by certain individuals already identified in government databases and either add them to the watchlist or change their watchlist status, which included adding individuals to the watchlist's aviation-related subset lists. For example, the number of U.S. persons (U.S. citizens and lawful permanent residents) on the subset No Fly List the government uses to deny individuals the boarding of aircraft more than doubled after the attempted attack.

Screening agencies are addressing gaps in processes that were exposed by the attempted attack. For example, based on the growth of lists used to screen aviation passengers and continued implementation of Secure Flight—which enabled the Transportation Security Administration to assume direct responsibility for conducting watchlist screening from air carriers—more individuals have been denied boarding aircraft or subjected to additional physical screening before boarding. Secure Flight has also reduced the likelihood of passengers being misidentified as being on the watchlist and has allowed agencies to use a broader set of watchlist records during screening. U.S. Customs and Border Protection has built upon its practice of evaluating individuals before they board flights to the United States, resulting in hundreds more non-U.S. persons on the watchlist being kept off flights because the agency determined they would likely be deemed inadmissible upon arrival at a U.S. airport. The Department of State revoked hundreds of visas shortly after the attempted attack because it determined that the individuals could present an immediate threat to the United States. These actions are intended to enhance homeland security, but have also impacted agency resources and the traveling public. An interagency policy committee is also assessing the outcomes and impacts of these actions, but it did not provide details on this effort. Routine assessments could help decision makers and Congress determine if the watchlist is achieving its intended outcomes and help information future efforts.

# Contents

## Abbreviations

| | |
|---|---|
| CBP | U.S. Customs and Border Protection |
| CIA | Central Intelligence Agency |
| DHS | Department of Homeland Security |
| FBI | Federal Bureau of Investigation |
| NCTC | National Counterterrorism Center |
| State | U.S. Department of State |
| TIDE | Terrorist Identities Datamart Environment |
| TRIP | Traveler Redress Inquiry Program |
| TSA | Transportation Security Administration |
| TSC | Terrorist Screening Center |
| TSDB | Terrorist Screening Database |

GAO
Accountability * Integrity * Reliability

**United States Government Accountability Office**
**Washington, DC 20548**

May 31, 2012

Congressional Requesters

The attempt on December 25, 2009, to detonate a concealed explosive on board a U.S.-bound aircraft raised questions as to why warnings about the attempted bomber did not result in the U.S. government including him on its consolidated terrorist watchlist. The Terrorist Screening Center (TSC)—administered by the Federal Bureau of Investigation (FBI)—is responsible for maintaining this list of known or suspected terrorists and making records from the watchlist database available as appropriate to agencies that screen individuals for possible threats. For instance, subsets of the watchlist are used by the Transportation Security Administration (TSA) to screen individuals before they board an aircraft, by U.S. Customs and Border Protection (CBP) to inspect or vet individuals traveling to and from the United States, and by the Department of State (State) to screen visa applicants.

The Executive Office of the President's review of the attempted attack found that the U.S. government had sufficient information to have uncovered and potentially disrupted the attack, but shortcomings in the watchlisting process prevented the attempted bomber—Umar Farouk Abdulmutallab—from being nominated for inclusion on the watchlist.[1] Thus, screening agencies that could have identified him as a potential threat were unable to identify him and take action. The Executive Office of the President tasked departments and agencies to undertake a number of corrective actions to help ensure that known or suspected terrorists are identified and nominated to the watchlist and that agencies can use the list to screen individuals for potential links to terrorism.[2]

[1]Executive Office of the President, *Summary of the White House Review of the December 25, 2009, Attempted Terrorist Attack* (Washington, D.C.: Jan. 7, 2010).

[2]Executive Office of the President, *Memorandum on Attempted Terrorist Attack on December 25, 2009: Intelligence, Screening, and Watchlisting System Corrective Actions* (Washington, D.C., Jan. 7, 2010). Terrorism and terrorist activities are, in general, acts that (1) involve violent acts or acts dangerous to human life, property, or infrastructure that may be a violation of U.S. law and (2) appear intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of government by mass destruction, assassination, kidnapping, or hostage taking. This includes activities that facilitate or support terrorism and terrorist activities.

We have been monitoring the government's efforts to improve its ability to share terrorism-related information to further homeland security. In January 2005, we designated information sharing a high-risk area because the federal government faced formidable challenges in analyzing and disseminating this information in a timely, accurate, and useful manner. The federal government's sharing of terrorism-related information remained a high-risk area in our biennial update that we issued in February 2011.[3] Also, in October 2007, we reported on how the watchlist is created and maintained and how federal, state, and local security partners use the list to screen individuals for potential threats to the homeland.[4] We identified potential vulnerabilities—including ones created because agencies were not screening against all watchlist records—and concluded that an up-to-date strategy could help the government optimize use of the watchlist. We made recommendations to enhance the effectiveness of the watchlisting and screening processes, which agencies implemented or have actions under way to address. Further, after the attempted attack, we reported that weighing and responding to the potential impacts that changes to the criteria used to nominate individuals to the terrorist watchlist would have on the traveling public will be an important consideration in determining what changes may be needed.[5]

In response to your request, we issued a classified report in December 2011 that addressed the following questions:

- What actions has the federal government taken since the December 25, 2009, attempted attack to strengthen the watchlist nominations process, and to what extent are departments and agencies experiencing challenges implementing these actions and assessing impacts of the actions they have taken?
- How did the composition of the watchlist change as a result of actions taken by departments and agencies after the attempted attack?

[3]GAO, *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 2011).

[4]GAO, *Terrorist Watch List Screening: Opportunities Exist to Enhance Management Oversight, Reduce Vulnerabilities in Agency Screening Processes, and Expand Use of the List*, GAO-08-110 (Washington, D.C.: Oct. 11, 2007).

[5]GAO, *Homeland Security: Better Use of Terrorist Watchlist Information and Improvements in Deployment of Passenger Screening Checkpoint Technologies Could Further Strengthen Security*, GAO-10-401T (Washington, D.C.: Jan. 27, 2010).

- How are screening agencies addressing vulnerabilities exposed by the attempted attack, what have been the outcomes of related screening since the incident, and to what extent are federal agencies assessing the impacts of this screening?

This report is a public version of the classified report that we provided to you. The various departments and agencies we reviewed deemed some of the information in the restricted report as classified or sensitive (e.g., Sensitive Security Information or For Official Use Only), which must be protected from public disclosure. Therefore, this report omits certain information associated with vulnerabilities in watchlisting and screening processes that were exposed by the December 25, 2009, attempted attack and government actions to address these vulnerabilities. This report also omits key details regarding (1) certain policies and procedures associated with the development and use of the terrorist watchlist and (2) specific outcomes of encounters with individuals who were positively matched to the watchlist. Although the information provided in this report is more limited in scope, it addresses the same questions as the restricted report. Also, the overall methodology used for both reports is the same.

To determine federal government actions to strengthen the watchlist nominations process and related challenges, we analyzed postattack government reports issued by the Executive Office of the President and the Senate Select Committee on Intelligence.[6] We also compared the July 2010 Watchlisting Guidance—issued by the TSC to standardize watchlisting policies and processes—to the 2009 watchlisting protocol (the most recent operational policy before the December 2009 attempted attack) to identify changes that were intended to strengthen agencies' abilities to nominate known or suspected terrorist to the watchlist.[7] To help us determine how postattack changes in the watchlisting guidance have affected the volume of nominations and any resulting impacts, we obtained data for the period January 2009 through May 2011 from seven

[6]Senate Select Committee on Intelligence, *Unclassified Summary of the Committee Report on the Attempted Terrorist Attack on Northwest Airlines Flight 253* (Washington, D.C.: May 18, 2010).

[7]TSC issued versions of the watchlisting protocol in 2008 and 2009, and it issued the Watchlisting Guidance in 2010.

federal entities involved in the nominations process.[8] Specifically, we obtained data from five entities that nominate individuals for inclusion on the terrorist watchlist (nominating agencies). We also obtained information from the National Counterterrorism Center (NCTC), an entity that processes these nominations and submits them to TSC, as does the FBI, and TSC.[9] Further, we analyzed documentation on the watchlisting nominations process and interviewed agency officials—including the Director of TSC, NCTC's Deputy Director for Terrorist Identities, and agency watchlisting program officials—to discuss nomination processes, how changes instituted as a result of the July 2010 Watchlisting Guidance have impacted agencies, and related challenges.

To identify how the composition of the watchlist has changed since the December 2009 attempted attack, we analyzed agency documents and TSC data for 2009 and 2010 on the number of individuals on the terrorist watchlist and its subset No Fly and Selectee lists, and on the number of U.S. persons (U.S. citizens and lawful permanent residents) on these lists.[10] We also analyzed the July 2010 Watchlisting Guidance and interviewed the TSC Director and other center officials to obtain their perspectives on the reasons for changes in the size and composition of the watchlist and subset lists.

To identify how screening and law enforcement agencies are addressing vulnerabilities exposed by the attempted attack, the outcomes and impacts of agency actions, and the extent to which agencies are assessing the outcomes and impacts, we focused on screening, inspection, and vetting conducted by the Department of Homeland Security's (DHS) TSA and CBP, and State. These are the primary agencies that use the watchlist to screen and vet individuals traveling to

[8]In general, our work focused on the federal entities that the Executive Office of the President tasked to take corrective actions in response to the December 2009 attempted attack (see app. I).

[9]NCTC—within the Office of the Director of National Intelligence—serves as the primary organization in the U.S. government for, among other things, analyzing and integrating all intelligence pertaining to terrorism and counterterrorism, except for intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism. See 50 U.S.C. § 404o(d)(1).

[10]In general, individuals on the No Fly List are to be precluded from boarding an aircraft and individuals on the Selectee List are to receive additional screening prior to boarding an aircraft.

the United States. We obtained data—generally for 2009 and 2010 but in some cases through May 2011—on how often these agencies have encountered individuals on the watchlist and the outcomes of these encounters to help determine what impact changes in agency screening or vetting procedures have had on the traveling public and agency operations, among other things.[11] We also interviewed officials from each agency to discuss how their screening and vetting procedures have changed since the attempted attack and how they are assessing the impacts of the changes. Further, to better understand the impacts of watchlist screening on the traveling public, we analyzed data for 2009 and 2010 on individuals who had inquiries or sought resolution regarding difficulties they experienced during their travel screening and interviewed DHS officials who are responsible for providing redress for these individuals.

To assess the reliability of data on watchlist nominations, number of watchlist records, and screening outcomes, we questioned knowledgeable officials about the data and the systems that produced the data, reviewed relevant documentation, examined data for obvious errors, and (when possible) corroborated the data among the different agencies. We determined that the data were sufficiently reliable for the purposes of this report. We conducted this performance audit from February 2010 to May 2012 in accordance with generally accepted government auditing standards.[12] Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Appendix I contains more details about our objectives, scope, and methodology.

[11]As used in this report, the term encounter refers to an event in which an individual is identified to be a positive match to an individual on the terrorist watchlist.

[12]We issued a classified report on this work in December 2011.

# Background

## Overview of the Watchlisting and Screening Processes

Pursuant to Homeland Security Presidential Directive 6, TSC was established to create and maintain the U.S. government's consolidated watchlist—the Terrorist Screening Database (TSDB)—and to provide for the use of watchlist records during security-related and other screening processes.[13] The watchlisting and screening processes are intended to support the U.S. government's efforts to combat terrorism by consolidating the terrorist watchlist and providing screening and law enforcement agencies with information to help them respond appropriately during encounters with known or suspected terrorists, among other things.

TSC receives watchlist information for inclusion in the TSDB from two sources: NCTC and the FBI. TSC receives the vast majority of its watchlist information from NCTC, which compiles information on known or suspected international terrorists.[14] NCTC receives this information from executive branch departments and agencies—such as the Central Intelligence Agency (CIA), State, and the FBI—and maintains the information in its Terrorist Identities Datamart Environment (TIDE) database. Agencies that submit nominations to NCTC are to include pertinent derogatory information and any biographic information—such as name and date of birth—needed to establish the identity of individuals on the watchlist.[15] The FBI provides TSC with information about known or

[13]Homeland Security Presidential Directive/HSPD-6, *Integration and Use of Screening Information* (Sept. 16, 2003).

[14]In general, international terrorists engage in terrorist activities that occur primarily outside the territorial jurisdiction of the United States or that transcend national boundaries and include individuals in the United States with connections to terrorist activities outside the United States. See, e.g., 18 U.S.C. § 2331 and 22 U.S.C. § 2656f(d) (defining domestic and international terrorism in a criminal context, and international terrorism in a foreign relations context, respectively).

[15]In general, a nominator is a department or agency that has determined that an individual is a known or suspected terrorist and nominates that individual to TIDE and the TSDB based on information that originated with that agency or another agency. An originator is a department or agency that has appropriate subject matter interest and classification authority, and collects terrorism information and disseminates it to other U.S. government entities.

suspected domestic terrorists.[16] In general, the FBI nominates individuals who are subjects of ongoing FBI counterterrorism investigations to TSC for inclusion in the TSDB, including persons the FBI is preliminarily investigating to determine if they have links to terrorism.

In accordance with Homeland Security Presidential Directive 6—and built upon through Homeland Security Presidential Directives 11 and 24—the TSDB is to contain information about individuals known or suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism and terrorist activities.[17] Nominating agencies, NCTC, and the FBI apply a reasonable-suspicion standard to determine which individuals are appropriate for inclusion in the TSDB.[18] NCTC and the FBI are to consider information from all available sources to determine if there is a reasonable suspicion of links to terrorism that warrants a nomination. Once NCTC and the FBI determine that an individual meets the reasonable-suspicion standard and that minimum biographic information exists, they extract sensitive but unclassified information on the individual's identity—such as name and date of birth—from their classified databases and send the information to TSC. TSC reviews these nominations—evaluating the derogatory and biographic information—to decide whether to add nominated individuals to the TSDB. Appendix II contains additional information on the watchlist nominations process.

To support agency screening processes, TSC sends applicable records from the TSDB to screening and law enforcement agency systems based

[16]According to the FBI's Domestic Terrorist Operations Unit, domestic terrorists engage in activities that (1) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any state; (2) appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by mass destruction, assassination, or kidnapping; and (3) occur primarily within the territorial jurisdiction of the United States. See 18 U.S.C. § 2331(5).

[17]See Homeland Security Presidential Directive 11, *Comprehensive Terrorist-Related Screening Procedures* (Aug. 27, 2004); and Homeland Security Presidential Directive 24, *Biometrics for Identification and Screening to Enhance National Security* (June 5, 2008).

[18]In general, to meet the reasonable-suspicion standard, the nominator shall consider the totality of information available that, taken together with rational inferences from that information, reasonably warrants a determination that an individual is known or suspected to be or have been knowingly engaged in conduct constituting, in preparation for, in aid of, or related to terrorism or terrorist activities.

on the agency's mission responsibilities and other factors. For instance, applicable TSC records are provided to TSA for use in screening airline passengers, to CBP for use in inspecting and vetting persons traveling to and from the United States, and to State for use in screening visa applicants. Regarding individuals who are not citizens or nationals of the United States seeking to travel to and lawfully enter the United States, screening and law enforcement agencies rely on immigration laws that specify criteria for determining whether to issue visas to individuals and whether to admit them into the country.[19] In many instances, individuals who are not citizens or nationals of the United States who have engaged in or are likely to engage in terrorist-related activities may be ineligible to receive visas or inadmissible for entry to the United States, or both.[20] U.S. citizens returning to the United States from abroad are not subject to the admissibility requirements of the Immigration and Nationality Act, regardless of whether they are subjects of watchlist records. In general, these individuals only need to establish their U.S. citizenship to the satisfaction of the examining officer—by, for example, presenting a U.S. passport—to obtain entry into the United States.[21] U.S. citizens are subjected to inspection by CBP before being permitted to enter and additional actions may be taken, as appropriate.

## Weaknesses Exposed by the December 2009 Attempted Attack

On December 25, 2009, Umar Farouk Abdulmutallab, a 23-year old Nigerian man, attempted to detonate a concealed explosive device on Northwest Airlines Flight 253 en route from Amsterdam to Detroit as the plane descended into the Detroit Metropolitan Wayne County Airport.

[19]See, e.g., 8 U.S.C. § 1182 (codifying § 212 of the Immigration and Nationality Act, as amended, which articulates many of the grounds upon which an alien—any person not a citizen or national of the United States—may be determined to be ineligible for a visa or inadmissible to the United States). Before traveling to the United States, an alien who is not a lawful permanent resident must generally obtain a State-issued nonimmigrant visa for temporary stay (such as for business, tourism, or other reasons) or immigrant visa for permanent residence. See 8 U.S.C. § 1101(a)(15) (defining "immigrant").

[20]See 8 U.S.C. § 1182(a)(3).

[21]See 8 C.F.R. § 235.1(b) and 8 U.S.C. § 1185(b). Lawful permanent residents generally are not regarded as seeking admission to the United States and are not subject to the grounds for inadmissibility unless they fall within certain criteria listed at 8 U.S.C. § 1101(a)(13)(C) that describe the circumstances under which an alien lawfully admitted for permanent residence would be regarded as seeking admission. However, lawful permanent residents may be subject to the grounds of removability under 8 U.S.C. § 1227(a) after admission.

According to the Executive Office of the President's and Senate Select Committee on Intelligence's inquiries into events that led to the attempted attack, failures across the intelligence community—including human errors, technical problems, and analytic misjudgments—contributed to the government's failure to identify the subject as a threat that would qualify him for inclusion on the terrorist watchlist. The inquiries concluded that the intelligence community held information on Mr. Abdulmutallab—he was included in TIDE at the time of the attempted attack—but that it was fragmentary and ultimately not pieced together to form a coherent picture of the threat he posed (see fig. 1).

**Figure 1: Summary of Information on Mr. Abdulmutallab Contained in U.S. Government Holdings before the December 2009 Attempted Attack**

- Mr. Abdulmutallab held an active U.S. visa, issued on June 16, 2008.
- U.S. Embassy officers in Abuja, Nigeria, met with Mr. Abdulmutallab's father on November 18, 2009, to discuss his concerns that his son may have come under the influence of "Yemeni-based extremists" and had planned to travel to Yemen.
- State sent a cable on November 20, 2009, to intelligence and law enforcement officials stating concerns about Mr. Abdulmutallab's potential involvement with Yemeni-based extremists, but did not include the source of the information.
- Mr. Abdulmutallab was entered into NCTC's TIDE database on November 23, 2009.
- The intelligence community had reports related to Mr. Abdulmutallab, but agencies did not search other databases that would have identified additional relevant information and intelligence that when pieced together, might have warranted his nomination to the terrorist watchlist.

Source: GAO analysis of published government reports and testimonies.

The government inquiries also raised issues regarding how agencies used and interpreted the 2009 watchlisting protocol for nominating individuals to the watchlist. For example, according to the Executive Office of the President's review, although Mr. Abdulmutallab was entered into TIDE in November 2009, NCTC determined that the associated derogatory information did not meet the criteria for nominating him to the terrorist watchlist. Therefore, NCTC did not send the nomination to TSC. Also, according to the Senate Select Committee on Intelligence report, agencies may have interpreted the 2009 watchlisting protocol's standards for placing individuals on the watchlist too rigidly, thereby preventing Mr. Abdulmutallab from being nominated for inclusion on the watchlist.

Under the auspices of the Information Sharing and Access Interagency Policy Committee, TSC—in coordination with watchlisting and screening agencies—reviewed the 2009 watchlisting protocol and made

recommendations regarding whether adjustments to the protocol were warranted.[22] The Deputies Committee—a senior interagency forum that considers policy issues affecting national security—initially approved new watchlisting guidance for issuance to the watchlisting and screening communities in May 2010. After a multiagency classification review was completed, the Deputies Committee approved a final version of the Watchlisting Guidance in July 2010, which TSC issued to the watchlisting and screening communities.[23]

## 2010 Guidance Addresses Weaknesses in Nominations Process, but Agencies Face Challenges in Managing Increased Volumes of Information

### Changes to Watchlisting Guidance and Impacts on Agencies

The July 2010 Watchlisting Guidance includes changes that were intended to address weaknesses in the nominations process that were exposed by the December 2009 attempted attack and to clarify how agencies are to nominate individuals to the watchlist.[24] Since the guidance was approved, nominating agencies have expressed concerns

[22]The Interagency Policy Committees are the main day-to-day forums for interagency coordination of national security policy, providing policy analysis and ensuring timely responses to decisions made by the President. See Presidential Policy Directive 1, *Organization of the National Security Council System* (Feb. 13, 2009).

[23]According to the TSC Director's memorandum that was released with the revised guidance, although the Deputies Committee officially approved the guidance in May 2010, agencies had been implementing certain modifications prior to this date.

[24]Details regarding information contained in the July 2010 Watchlisting Guidance were deleted from this report because agencies considered them to be Sensitive Security Information.

about the increasing volumes of information and related challenges in processing this information and noted that the long-term impacts of the revisions may not be known for some time. For example, the watchlisting unit director from one agency reported that the agency is experiencing an increasing intake of information from its sources, which has impacted its analysts' reviews of this information. Also, officials from some agencies reported that at times they have had to temporarily add personnel to review and process the large volumes of information.

Data from the nominating agencies we contacted show that the agencies sent more nominations-related information to NCTC after the attempted attack than before the attack. According to NCTC officials, the center experienced receiving an increase in nominations beginning in February 2010. The officials noted that in May 2010, the volume of incoming nominations exceeded NCTC's ability to process it, resulting in a backlog. NCTC has applied additional resources—both staffing and technological—to address its backlog. As a result, in October 2011, NCTC officials noted that the center had virtually eliminated its backlog. Moreover, unless TSC has the ability to process the information it receives, it cannot add information to the TSDB for use by screening and law enforcement agencies.[25] Overall, the volume of nominations TSC is receiving from the FBI and NCTC has generally increased since the attempted attack. According to TSC officials, the center has avoided backlogs by employing a variety of strategies to address its workload, including management of personnel resources and use of more advanced technology.

Since the December 25, 2009, attempted attack, agencies involved in the watchlist nominations process have pursued staffing, technology, working groups, and other solutions to strengthen the process and manage increasing volumes of information. Specifically, officials from four of the seven agencies we contacted reported that they are in the process of developing and implementing certain technological solutions to address watchlisting issues. For example, NCTC, in consultation with other members of the intelligence community, reported that it is developing information technology tools to strengthen analysts' abilities to identify potential links to terrorism. The government has also created interagency

[25]We discuss the impacts that increasing nominations could have on screening agencies later in this report.

working groups to address watchlist-related issues. Further, NCTC reported that training programs have been developed and administered to its watchlisting analysts, as well as nominating and screening agency personnel.

Our review of the July 2010 Watchlisting Guidance and discussions with relevant agency officials indicated that in drafting the guidance, the watchlist community emphasized quality-assurance mechanisms as well as civil rights and civil liberties protections that should be considered when nominating individuals.

## Assessing Impacts of Guidance Could Help Ensure That Challenges Are Resolved and Inform Future Efforts to Strengthen the Watchlisting Process

While agencies are pursuing actions to strengthen the watchlisting process, no single entity is accountable for routinely assessing the overall impacts the July 2010 Watchlisting Guidance is having on the watchlisting community, the extent to which these impacts are acceptable and manageable from a policy perspective, and if the impacts indicate the need for any adjustments. Further, no entity is routinely collecting and analyzing data needed to conduct such governmentwide assessments over time. In general, officials from the nominating agencies we contacted and from NCTC and TSC said that they participated in developing the July 2010 Watchlisting Guidance and agreed with the changes, but noted that they did not know at the time how changes implemented through the 2010 guidance would impact them. Routinely assessing these impacts could help agencies address any challenges they are having in implementing the watchlisting guidance.

Agencies involved in the nominations process are taking actions to address challenges related to implementing the 2010 guidance. For example, officials from the Information Sharing and Access Interagency Policy Committee's Subcommittee on Watchlisting noted that departments and agencies within the watchlisting community are responsible for assessing the impacts of their individual watchlisting efforts and for bringing issues, as needed, to the subcommittee.[26] They explained that agencies react to and address issues and challenges as they arise. However, this approach has not allowed them to proactively and systematically assess the watchlisting process and identify emerging

[26]The Subcommittee on Watchlisting is attended by members of the watchlist community and provides an interagency forum to which agencies can bring watchlist-related issues for discussion and resolution.

issues; achieve consensus on solutions to potential challenges before they manifest themselves; and determine if adjustments to the watchlisting guidance are needed.

Because of the collaborative nature of the watchlisting process, any assessment of impacts must be an interagency effort. However, none of the interagency entities we contacted were routinely performing these assessment functions. In February 2011, officials from the Subcommittee on Watchlisting noted that the subcommittee was preparing a report on watchlisting efforts since the December 2009 attempted attack and had requested that subcommittee members provide input. At that time, the subcommittee officials noted that the Information Sharing and Access Interagency Policy Committee did not plan to conduct routine assessments of the watchlisting processes. In August 2011, a representative of the National Security Staff informed us that the Information Sharing and Access Interagency Policy Committee recently began performing an assessment function related to the July 2010 Watchlisting Guidance. The representative noted that the depth and frequency of specific reviews will vary as necessary and appropriate. The staff did not provide us details on these efforts, so we could not determine to what extent the assessments will be routine or involve collecting and analyzing data needed to conduct such assessments over time.

Since we found no single entity that is responsible and accountable for routinely assessing the overall impacts the 2010 guidance is having on the watchlisting community—and collecting the data needed to conduct such assessments—the Assistant to the President for Homeland Security and Counterterrorism may be best positioned to ensure that governmentwide assessments are conducted. The President tasked this individual to be responsible and accountable for ensuring that agencies carry out actions to strengthen the watchlisting process after the December 2009 attempted attack. Thus, it likewise follows that this individual could be responsible and accountable for ensuring that the impacts from these actions are routinely assessed and that the results of the assessments are used to inform future watchlisting changes.

According to Standards for Internal Control in the Federal Government, ongoing monitoring of programs and activities should occur during the

course of normal operations.[27] Working collaboratively to ensure that appropriate agencies routinely evaluate or assess the impact of the 2010 guidance on the watchlisting community could help decision makers determine if the guidance is achieving its intended outcomes or needs any adjustments, and help inform future efforts to strengthen the watchlisting process. Such assessments could also help the Information Sharing and Access Interagency Policy Committee and the watchlisting community understand longer-term impacts of changes to the watchlisting guidance, such as how increasing volumes of information are creating resource demands. Finally, such assessments could help to improve transparency and provide an accurate accounting to the Executive Office of the President and other stakeholders, including Congress, for the resources invested in the watchlisting process.

## The Number of Individuals on the Watchlist and Aviation-Related Subsets Increased after the Attempted Attack

Immediately after the December 2009 attempted attack, federal agencies took steps that resulted in an increase in the number of individuals in the TSDB and its aviation-related subsets—the No Fly and Selectee lists—based on new intelligence and threat information. Specifically, in the months following the attempted attack, agencies added these individuals to the TSDB from TIDE or from the TSDB to the No Fly or Selectee lists. Also, upon completion of this initiative, the number of U.S. persons on the No Fly List more than doubled and the number of U.S. persons on the Selectee List increased by about 10 percent. According to TSC data, the number of individuals on the No Fly List generally continued to increase during the remainder of 2010, while the number of individuals on the Selectee List remained relatively constant.

To carry out these upgrades, TSC and NCTC—at the direction of the Deputies Committee and in consultation with other intelligence agencies—reviewed available intelligence and threat information that existed on certain individuals. At the same time, TSC worked with NCTC and intelligence community agencies to ensure that (1) the information that supported changing the watchlist status of the individuals was as complete and accurate as possible and (2) the individuals were placed in

[27]GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

the TSDB and, when applicable, on the No Fly or Selectee lists, in accordance with standards and criteria for inclusion on these lists.[28]

## Screening Agencies Are Addressing Vulnerabilities Exposed by the Attempted Attack, but Assessing Their Impacts Could Help Inform Future Efforts

Agencies that screen individuals against TSDB records are addressing vulnerabilities and gaps in processes that were exposed by the December 2009 attempted attack to enhance homeland security. For example, TSA actions have resulted in more individuals being denied boarding aircraft or subjected to enhanced screening before boarding. The number of U.S. persons (U.S. citizens and lawful permanent residents) denied boarding has also increased and, for such persons abroad, required the government to develop procedures to facilitate their return. TSA is also screening airline passengers against additional TSDB records to mitigate risks. CBP has implemented a program to build upon its practice of evaluating the risk posed by individuals attempting to enter the United States before they board flights bound for the United States. As a result, air carriers have permitted fewer individuals in the TSDB to board such flights, particularly nonimmigrant aliens. State took actions to revoke hundreds of U.S. visas immediately after the attempted attack because it determined that the individuals could present an immediate threat. These and other agency actions are intended to enhance homeland security, but no entity is routinely assessing governmentwide issues, such as how the changes have impacted agency resources and the traveling public, whether watchlist screening is achieving intended results, or if adjustments to agency programs or the watchlisting guidance are needed.

### TSA Has Encountered More Individuals on the No Fly and Selectee Lists and Is Screening against More Watchlist Records

#### No Fly and Selectee List Encounters

After the attempted attack, TSA continued implementation of the Secure Flight program, which enabled TSA to assume direct responsibility for

[28]Certain details regarding government actions to add individuals to the TSDB and its aviation-related subsets after the December 2009 attempted attack and the number of individuals added were deleted from this report because they are considered to be Sensitive Security Information.

determining if individuals are matches to the No Fly or Selectee lists from air carriers. Secure Flight requires that air carriers collect—and that passengers provide—full name and date-of-birth and gender information, thereby improving TSA's ability to correctly determine whether individuals are on these lists.[29] Before Secure Flight, air carriers were not required to collect date-of-birth and gender information, and each airline conducted watchlist matching differently with varying effectiveness.[30] According to TSA, the increase in individuals added to the No Fly and Selectee lists, combined with the implementation of Secure Flight, resulted in an increase in the number of times airlines encountered individuals on these lists. TSA data show that the encounters involved both domestic flights (flights to and from locations within the United States) and international flights (flights to or from the United States or over U.S. air space).

Since the December 2009 attempted attack and subsequent increase in the number of U.S. persons nominated to and placed on the No Fly List, there have been instances when U.S. persons abroad have been unable to board an aircraft bound for the United States. Any individual—regardless of nationality—can be prohibited from boarding an aircraft if the threat represented by the individual meets the criteria for inclusion on the No Fly List. In general, however, U.S. citizens are permitted to enter the United States at a U.S. port of entry if they prove to the satisfaction of a CBP officer that they are in fact U.S. citizens.[31] Lawful permanent residents, who in limited circumstances independent of the No Fly List may be rendered an applicant for admission, are usually entitled to removal proceedings prior to having their status as a lawful permanent resident terminated for immigration purposes.[32]

[29]Air carriers must also request that passengers provide a redress number, if available, though passengers are not required to provide this information. See 49 C.F.R. § 1560.101. In general, the term redress refers to an agency's complaint resolution process whereby individuals may seek resolution of their concerns about an agency action.

[30]See GAO, *Aviation Security: TSA Is Enhancing Its Oversight of Air Carrier Efforts to Identify Passengers on the No Fly and Selectee Lists, but Expects Ultimate Solution to Be Implementation of Secure Flight*, GAO-08-992 (Washington, D.C.: Sept. 9, 2008).

[31]See 8 U.S.C. § 1185(b); 8 C.F.R. § 235.1(b).

[32]See 8 U.S.C. §§ 1101(a)(13)(C), 1229a.

## TSA Is Screening Airline Passengers against Additional Watchlist Records

In our October 2007 watchlist report, we recommended that DHS assess to what extent security risks exist by not screening against more watchlist records and what actions, if any, should be taken in response.[33] DHS generally agreed with our recommendation but noted that increasing the number of records that air carriers used to screen passengers would expand the number of misidentifications to unjustifiable proportions without a measurable increase in security. In general, misidentifications occur when a passenger's name is identical or similar to a name in the TSDB but the passenger is not the individual on the watchlist. Since then, TSA assumed direct responsibility for this screening function through implementation of the Secure Flight program for all flights traveling to, from, or within the United States.[34] According to TSA, Secure Flight's full assumption of this function from air carriers and its use of more biographic data for screening have improved watchlist matching. This includes TSA's ability to correctly match passenger data against TSDB records to confirm if individuals match someone on the watchlist and reduce the number of misidentifications.[35] Appendix III contains additional information on how Secure Flight has reduced the likelihood of passengers being misidentified as being on the watchlist and related inconveniences.

TSA's actions discussed below fully respond to the recommendation we made in our October 2007 report. Specifically, TSA has implemented Secure Flight such that as circumstances warrant, it may expand the scope of its screening beyond the No Fly and Selectee lists to the entire TSDB.[36] According to the program's final rule, in general, Secure Flight is to compare passenger information only to the No Fly and Selectee lists because, during normal security circumstances, screening against these components of the TSDB will be satisfactory to counter the security threat. However, the rule also provides that TSA may use the larger set of

[33]GAO-08-110.

[34]Secure Flight also performs this screening function for covered airline flights that travel over the United States and "point-to-point" international flights operated by covered U.S.-based airlines.

[35]See GAO, *Aviation Security: TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks,* GAO-09-292 (Washington, D.C.: May 13, 2009).

[36]See generally Secure Flight Program; Final Rule, 73 Fed. Reg. 64,018 (Oct. 28, 2008) (codified at 49 C.F.R. pt. 1560).

"watch lists" maintained by the federal government when warranted by security considerations, such as if TSA learns that flights on a particular route may be subject to increased security risk.

Also, after the attempted bombing in December 2009, DHS proposed and the Deputies Committee approved the Secure Flight program's expanded use of TSDB records on a routine basis to screen passengers before they board flights. In April 2011, TSA completed the transition of the Secure Flight program to conduct watchlist matching against this greater subset of TSDB records and notify air carriers that those passengers who are determined to be a match should be designated for enhanced screening prior to boarding a flight. According to TSA, the impact on screening operations has been minimal given the relatively low volume of matches against these additional records each day.

TSA noted that the entire TSDB is not used for screening since matching passenger data against TSDB records that contain only partial data could result in a significant increase in the number of passengers who are misidentified as being on the watchlist and potentially cause unwarranted delay or inconvenience to travelers. TSA also noted that as with potential misidentifications to the No Fly and Selectee lists, passengers who feel that they have been incorrectly delayed or inconvenienced can apply for redress through the DHS Traveler Redress Inquiry Program (DHS TRIP).[37] DHS noted that TSA regularly monitors the Secure Flight program and processes and makes adjustments as needed.

In fiscal year 2011, TSA reprogrammed $15.9 million into Secure Flight to begin screening against the additional TSDB records. TSA's fiscal year 2012 budget request proposed funding to make screening against the additional records permanent. According to TSA, for fiscal year 2012, Secure Flight requested an increase of $8.9 million and 38 full-time personnel to continue supporting this expanded screening effort. According to TSA, the funding will be used for information technology enhancements that will be required to implement this expanded screening and will allow TSA to handle the increased workload.

[37]DHS TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening. Additional information on DHS TRIP is discussed in app. VI.

## CBP Expansion of PreDeparture Vetting Has Kept Hundreds More Aliens in the TSDB off Airplanes Bound for the United States

For individuals traveling by air to the United States, CBP has established programs whereby it assesses individuals before they board an aircraft to determine whether it is likely they will be found inadmissible at a port of entry. The following sections discuss how CBP's Pre-Departure Targeting Program and Immigration Advisory Program handle the subset of travelers who are in the TSDB.[38] Other high-risk and improperly documented passengers handled by these programs include passengers who have criminal histories; have had their visas revoked; are in possession of fraudulent, lost, or stolen passports; or otherwise appear to be inadmissible.

### Pre-Departure Program Expanded CBP Vetting to Cover All Airports with Direct Flights to the United States

In response to the attempted attack in December 2009, and as part of its border and immigration security mission, CBP implemented the Pre-Departure Targeting Program in January 2010 to build upon its process of assessing if individuals would likely be found inadmissible at a port of entry before they board an aircraft to cover all airports worldwide with direct flights to the United States. Before the attempted attack, CBP assessed individuals who were departing from airports that had CBP Immigration Advisory Program officers on site. At airports without such a program, passengers in the TSDB but not on the No Fly List generally were allowed to board flights and travel to U.S. airports. Upon arrival at a U.S. port of entry, CBP would inspect the passengers and determine their admissibility. CBP continues to assess passengers through the Immigration Advisory Program for flights departing from airports that have a program presence.

For both the Pre-Departure Targeting Program and the Immigration Advisory Program, if CBP determines that a passenger would likely be deemed inadmissible upon arrival at a U.S. airport, it recommends that the air carrier not board that passenger (that is, it makes a no board recommendation). CBP generally makes these no board recommendations based on provisions for admissibility found in the Immigration and Nationality Act.[39] U.S. citizens are generally not subject

[38]CBP's Pre-Departure Targeting Program was designed specifically for vetting aviation passengers. The Immigration Advisory Program was established in 2004 to place trained CBP officers at certain foreign airports to assist with passenger vetting, such as interviewing high-risk or improperly documented passengers and evaluating the authenticity of travel documents prior to a passenger's departure.

[39]See, e.g., 8 U.S.C. § 1182 (codifying section 212 of the Immigration and Nationality Act, as amended, and establishing conditions under which an alien—any person not a citizen or national of the United States—may be deemed inadmissible to the United States).

to these recommendations since they are generally permitted to enter the United States at a U.S. port of entry if they prove to the satisfaction of a CBP officer that they are in fact U.S. citizens. CBP may also decide to not issue such recommendations for aliens in the TSDB if, for example (1) CBP officers determine that, based on a review of all available information, the individual is not likely to be denied admission to the United States, or (2) the individual was granted a waiver of inadmissibility by DHS, if such a waiver is available.[40]

For flights departing from airports without an Immigration Advisory Program officer on site, CBP is leveraging the capabilities of its officers within its Regional Carrier Liaison Groups to issue no board recommendations to air carriers. These groups were established in 2006 to assist air carriers with U.S. entry-related matters—with a primary focus on verifying the authenticity of travel documents—and to work directly with commercial air carriers on security-related matters. Regional Carrier Liaison Group staff who are located in the United States handle Pre-Departure Targeting Program no board recommendations to air carriers remotely by delivering the recommendations via phone, fax, or e-mail.[41] CBP policy instructs staff to give no board recommendations priority over other duties, given the time and security sensitivities involved.

Upon receiving a no board recommendation from CBP for a passenger, air carriers make the ultimate decision whether to deny boarding or to transport the individual to the United States. According to CBP officials, air carriers almost always follow no board recommendations because (1) they do not want to transport high-risk individuals and (2) such alien passengers will almost always be found inadmissible at the U.S. port of entry. In this case, the air carrier is responsible for ensuring space for such an individual on the next available flight to the originating airport.[42] In addition, the air carrier could be fined for transporting an alien to the

[40]See 8 U.S.C. § 1182(d) (governing the temporary admission of aliens otherwise deemed inadmissible). See also 8 C.F.R. §§ 212.4, 212.7.

[41]There are three Regional Carrier Liaison Groups, which are located in Honolulu, Hawaii; Miami, Florida; and New York City, New York. Each of the three locations has authority over a region of the world, with the Honolulu location covering U.S.-bound flights from Asia and the Pacific; the New York City location covering flights from Africa, Europe, and the Middle East; and the Miami location covering flights from Latin America and the Caribbean.

[42]See 8 U.S.C. § 1231(c), (d).

United States who does not have a valid passport and visa, if a visa is required.[43] When CBP does not recommend that an individual in the TSDB be denied boarding and the passenger boards a flight bound for the United States, CBP inspects the passenger upon arrival at a U.S. airport. For aliens seeking admission to the United States, determinations on admissibility are generally made by CBP officers during this inspection in accordance with applicable provisions of the Immigration and Nationality Act. In general, aliens who are deemed inadmissible are detained by DHS until the individual can board a return flight home.

## CBP Made Hundreds More No Board Recommendations after the Attempted Attack

Since the attempted attack, CBP predeparture vetting programs—the Pre-Departure Targeting Program and the Immigration Advisory Program—have resulted in hundreds more aliens being kept off flights bound for the United States because CBP determined that they likely would be deemed inadmissible upon arrival at a U.S. airport and made corresponding no board recommendations to air carriers. In addition to the increase in no board recommendations that resulted from implementing the Pre-Departure Targeting Program in January 2010, the increase during 2010 was in response to the new threats made evident by the attempted attack, according to CBP officials. CBP data also show that there have been instances when individuals have boarded flights bound for the United States and arrived at U.S. airports. According to CBP officials, the vast majority of these cases involved either (1) U.S. citizens and lawful permanent residents who generally may enter the United States, and therefore, CBP generally does not recommend that air carriers not board these passengers, or (2) aliens in the TSDB who were deemed inadmissible but were granted temporary admission into the United States under certain circumstances, such as DHS granting a waiver of inadmissibility.[44]

At the time of our review, CBP did not have readily available data on how often aliens in the TSDB boarded flights bound for the United States—

[43]See 8 U.S.C. § 1323; 8 C.F.R. pt. 273.

[44]See, e.g., 8 U.S.C. § 1182(d)(3)(B) (authorizing the Secretary of Homeland Security, in certain circumstances, and after consultation with the Attorney General and Secretary of State, to grant temporary admission to an alien otherwise deemed inadmissible thereby, in effect, waiving a determination of inadmissibility). See also, e.g., 8 U.S.C. § 1182(d)(5) (authorizing the Attorney General to parole—that is, grant temporary permission to enter and be present in the United States—any alien into the United States on a case-by-case basis for urgent humanitarian reasons or significant public benefit).

information that could help CBP assess how its predeparture programs are working and provide transparency over program results, among other things. According to CBP officials, the agency was working on adding data fields to CBP systems to capture more information related to these programs. The officials noted that these changes will allow CBP to break down and retrieve data by U.S. citizens, lawful permanent residents, and aliens, and that related reports will be produced. At our request, CBP conducted a manual review of data it compiled on the results of its processing of passengers at U.S. airports from April 2010 through September 2010.[45] During this period, CBP data show that there were instances when aliens in the TSDB boarded flights bound for the United States and were admitted into the country. These occurrences are in addition to instances where aliens in the TSDB were able to board flights bound for and enter the United States because they had been granted admission to the country on a temporary basis under certain circumstances, such as by DHS granting a waiver of inadmissibility. According to CBP officials, for each of these occurrences, CBP officers determined—based on a review of all available and relevant information—that the derogatory information on the individual was not sufficient to render that person inadmissible under the Immigration and Nationality Act.

CBP officials stated that the Pre-Departure Targeting Program increased the workload for Regional Carrier Liaison Group staff and that two of the three groups increased the number of CBP officers assigned to handle this workload.[46] In addition, CBP officials noted that personnel at its facility that supports these programs experienced increased workloads, which they handled through additional hiring, overtime hours, and assignment of temporary duty personnel.

In cases where an individual expresses concern about not being able to board a flight to the United States, CBP Immigration Advisory Program officers or air carrier personnel are instructed not to reveal to the

[45]CBP compiles reports on these data twice each fiscal year, and at the time we requested the information, the April 2010 through September 2010 report was the most recently compiled. We did not request that CBP conduct manual reviews of other reports because of the labor intensive nature of the reviews.

[46]Regional Carrier Liaison Group positions are not specifically funded but are staffed from existing CBP port personnel, with CBP port management determining the staffing levels required at each location.

individual any law enforcement sensitive information. Rather, the CBP officers or air carrier personnel are to advise the individual to go to the U.S. consulate or the person's home country passport office, as appropriate, to address the issue. CBP officials also noted that individuals who have travel-related concerns are advised to file an inquiry through DHS TRIP. According to DHS TRIP officials, about 20 percent of all requests for redress that it receives involve CBP inspections conducted at land, sea, or air ports of entry.

## State Revoked Hundreds of Visas Held by Individuals on the Watchlist after the Attempted Attack

### State Revoked Hundreds of Visas after Attempted Attack

After the December 2009 attempted attack, the Executive Office of the President directed TSC to determine the visa status of all known or suspected terrorists in the TSDB. TSC then worked with State to determine whether individuals who held U.S. visas should continue holding them in light of new threats made evident by the incident. Specifically, in January 2010, State revoked hundreds of visas because it determined that the individuals could present an immediate threat to the United States. State officials noted that these revocations were largely related to individuals who were added to the TSDB—or moved to the No Fly or Selectee lists—after the attempted attack based on new intelligence and threat information.

In March 2010, TSC and State initiated another review and identified hundreds of cases in which individuals in the TSDB held U.S. visas. These cases included individuals who were in the TSDB at the time of the December 2009 attempted attack but did not have their visas revoked during the January 2010 review. According to State officials, all individuals who could present an immediate threat to the United States had their visas revoked within 24 hours. In cases involving a less clear nexus to terrorism, the officials noted that visas were not immediately revoked. The officials explained that investigating these cases can take several months and involve extensive coordination with law enforcement and intelligence officials. According to State officials, of these remaining cases, the department revoked a number of visas based on intelligence community recommendations and determined that other visas had been issued properly following the completion of an interagency review process and, in applicable cases, ineligibility waivers provided by DHS.

Regarding the cases in which State determined that individuals could continue to hold visas, State officials noted that an individual's presence in the TSDB does not itself render that person ineligible for a visa. For example, State will issue a visa if it determines that the available information supporting the TSDB record does not meet the statutory conditions under which an individual may be deemed ineligible for a visa to the United States, and the individual is not otherwise ineligible for a visa.[47] The officials added that in those instances where State finds that an individual is ineligible for a visa—based on provisions in the Immigration and Nationality Act that define terrorist activities—the department may still, in certain circumstances, issue a visa if DHS agrees to grant a waiver of inadmissibility, if such a waiver is available.[48] According to State officials, reasons an individual found ineligible for a visa may receive a waiver include significant or compelling U.S. government interests or humanitarian concerns. According to State officials, while the department consulted with law enforcement and intelligence community officials regarding whether to revoke the visas, State has final authority over all visa decisions.

In addition to the hundreds of visa revocations involving individuals in the TSDB that were related to the reviews directed by the Executive Office of the President, State data show that the department revoked hundreds more visas based on terrorism-related grounds during 2010. The total number of visas State revoked during 2010 was more than double the number of visas the department revoked based on terrorism-related grounds during 2009. According to State, as of May 2011, a number of individuals in the TSDB continued to hold U.S. visas because the department found that (1) they were ineligible to hold a visa under the

[47]See 8 U.S.C. § 1182(a)(3) (codifying § 212(a)(3) of the Immigration and Nationality Act, which identifies terrorist activities as one of the grounds for finding an alien ineligible for a visa or admission to the United States, and describes in broad terms the types of activities or circumstances that could lead to such a finding on terrorism grounds). Section 1182 identifies other security and nonsecurity grounds on which an individual may be deemed ineligible for a visa.

[48]See 8 U.S.C. § 1182(d)(3)(B) (authorizing the Secretary of State, in certain circumstances and after consultation with the Attorney General and Secretary of Homeland Security, to grant temporary admission to an alien otherwise deemed inadmissible thereby, in effect, waiving a determination of inadmissibility). A decision by the Secretary of State to issue a visa to an otherwise ineligible applicant would not, however, overcome DHS authority to determine admissibility at a port of entry into the United States.

terrorism-related provisions of the Immigration and Nationality Act but received waivers of that ineligibility or (2) they were not ineligible to hold visas under the terrorism-related provisions of the act following standard interagency processing of the visa applications.

## Outcomes of Visa Screening and Status of New State Efforts to Screen Visa Applicants

Under current procedures, State screens visa applicant data against sensitive but unclassified extracts of biographical information drawn from TSDB records as part of its evaluation process for issuing U.S. visas. If an applicant for a visa is identified as a possible match with a TSDB record, consular officers are to initiate a process to obtain additional information on the individual's links to terrorism, including information maintained by law enforcement and intelligence agencies. State data show that the department denied about 55 percent more nonimmigrant visas based on terrorism-related grounds during 2010 than it did during 2009, which includes denials involving individuals in the TSDB. Further, State found that in cases where individuals were ineligible to hold nonimmigrant visas based on terrorism-related grounds—but evinced significant or compelling U.S. government interest or humanitarian concern—the department recommended, and DHS granted, waivers of ineligibility.

According to State officials, the department's automated systems do not capture data on the number of individuals in the TSDB who applied for visas—or the related outcomes of these applications (e.g., issued or denied)—because this information is not needed to support the department's mission. State officials noted that it would be costly to change department databases to collect information specific to individuals applying for visas who are in the TSDB, but the department is working with TSC on a process to make these data more readily available through other means. State is also partnering with other agencies to develop a new, more automated process for reviewing visa applications that is intended to be more efficient than the current process. The new process is also intended to help minimize the inconvenience of protracted visa processing times for applicants incorrectly matched to TSDB records, among other things.

## Assessing Outcomes and Impacts of Screening and Vetting Agency Programs Could Help Ensure That the Watchlist Is Achieving Intended Results

Since the December 2009 attempted attack, agencies have taken actions to strengthen their respective processes for screening and vetting individuals against TSDB records. However, no entity has acknowledged that it is responsible and accountable for routinely conducting governmentwide assessments of how agencies are using the watchlist to make screening or vetting decisions and related outcomes or the overall impact screening or vetting programs are having on agency resources and the traveling public. Also, no entity is assessing whether watchlist-related screening or vetting is achieving intended results from a policy perspective, or if adjustments to agency programs or the watchlisting guidance are needed. Further, no entity is routinely collecting and analyzing data needed to conduct such governmentwide assessments over time. According to the TSC Director, conducting such assessments and developing related metrics will be important in the future.

The actions screening and law enforcement agencies have taken since the attempted attack have resulted in more individuals in the TSDB being denied boarding flights, being deemed inadmissible to enter the United States, and having their U.S. visas revoked, among other things. These outcomes demonstrate the homeland security benefits of watchlist-related screening or vetting, but such screening or vetting and related actions have also had impacts on agency resources and the traveling public. For example, new or expanded screening and vetting programs have required agencies to dedicate more staff to check traveler information against TSDB records and take related law enforcement actions. Also, any new or future uses of the watchlist for screening or vetting may result in more individuals being misidentified as the subject of a TSDB record, which can cause traveler delays and other inconveniences. Agencies are independently taking actions to collect information and data on the outcomes of their screening or vetting programs that check against TSDB records, but no entity is routinely assessing governmentwide issues, such as how U.S. citizens and lawful permanent residents are being affected by screening or the overall levels of misidentifications that are occurring. Routinely assessing these outcomes and impacts governmentwide could help decision makers determine if the watchlist is achieving its intended results without having unintended consequences or needs further revisions.

Because watchlist-related screening or vetting is a governmentwide function, any effort to assess the overall outcomes and impacts must be an interagency effort. The federal government has established interagency working groups to address screening and related issues. However, according to agency officials we contacted, these groups have

not conducted governmentwide assessments because they have been focused on implementing new or expanding screening or vetting programs and revising related policies and procedures, among other things.

Similar to watchlisting issues, in August 2011, a representative of the National Security Staff informed us that the Information Sharing and Access Interagency Policy Committee recently began performing an assessment to support its oversight of new screening processes. The representative noted that the depth and frequency of specific reviews will vary as necessary and appropriate. The staff did not provide us details on these efforts, so we could not determine to what extent the assessments will be routine or involve collecting and analyzing data needed to conduct such governmentwide assessments over time. As discussed previously, the President tasked the Assistant to the President for Homeland Security and Counterterrorism to be responsible and accountable for ensuring that agencies carry out actions to strengthen the watchlisting process after the December 2009 attempted attack. As such, the Assistant to the President may be best positioned to ensure that governmentwide assessments of the outcomes and impacts of agency screening programs are conducted.

According to Standards for Internal Control in the Federal Government, ongoing monitoring of programs and activities should occur during the course of normal operations. These standards also note that performance data on agency programs be available as a means to hold public service organizations accountable for their decisions and actions, including stewardship of public funds, fairness, and all aspects of performance.[49] Routine, governmentwide assessments of screening agency programs could help the government determine if the watchlist is achieving its intended results, identify broader issues that require attention, and improve transparency and provide an accurate accounting to the Executive Office of the President and other stakeholders, including Congress, for the resources invested in screening processes.

## Conclusions

The attempt on December 25, 2009, to detonate a concealed explosive on board a U.S.-bound aircraft highlights the importance of the U.S. government placing individuals with known or suspected ties to terrorism

[49]GAO/AIMD-00-21.3.1.

on its watchlist. The Executive Office of the President's review of the attempted attack found that the U.S. government had sufficient information to have uncovered and potentially disrupted the attempted attack, but shortcomings in the watchlisting process prevented the attempted bomber from being nominated for inclusion on the watchlist. The July 2010 Watchlisting Guidance includes changes that were intended to address weaknesses in the nominations process. Since the guidance was approved, agencies have expressed concerns about the increasing volumes of information and related challenges in processing this information. The federal entities involved in the nominations process are taking actions to address challenges related to implementing the guidance. However, no single entity is routinely assessing the overall impacts of the watchlisting guidance or the steps taken to strengthen the nominations process. Working collaboratively to ensure that the watchlisting community periodically evaluates or assesses the impacts of the revised guidance on the watchlisting community could (1) help decision makers determine if the guidance is achieving its intended outcomes or needs any adjustments, (2) inform future efforts to strengthen the watchlisting process, (3) help the watchlisting community understand longer-term impacts of changes to the watchlisting guidance, and (4) improve transparency and provide an accurate accounting to the Executive Office of the President and other stakeholders, including Congress, for the resources invested in the watchlisting process.

Just as agencies are not routinely assessing the impacts of the revisions made to the watchlisting guidance or the steps taken to strengthen the nominations process, no single entity is routinely assessing information or data on the collective outcomes or impacts of agencies' watchlist screening operations to determine the effectiveness of changes made to strengthen screening since the attempted attack or how changes to the watchlisting guidance have affected screening operations. Routine, governmentwide assessments of the outcomes and impacts of agencies' watchlist screening or vetting programs could help ensure that these programs are achieving their intended results or identify if revisions are needed. Such assessments could also help identify broader issues that require attention, determine if impacts on agency resources and the traveling public are acceptable, and communicate to key stakeholders how the nation's investment in the watchlist screening or vetting processes is enhancing security of the nation's borders, commercial aviation, and other security-related activities.

## Recommendations for Executive Action

To help inform future efforts to strengthen watchlisting and screening processes, we recommend that the Assistant to the President for Homeland Security and Counterterrorism establish mechanisms or use existing interagency bodies to routinely assess

- how the watchlisting guidance has impacted the watchlisting community—including its capacity to submit and process nominations in accordance with provisions in the guidance—and whether any adjustments to agency programs or the guidance are needed, and
- whether use of the watchlist during agency screening processes is achieving intended results, including whether the overall outcomes and impacts of screening on agency resources and the traveling public are acceptable and manageable or if adjustments to agency programs or the watchlisting guidance are needed.

## Agency Comments

We provided a draft of the classified version of this report for comment to the National Security Staff; the Office of the Director of National Intelligence; the Departments of Defense, Homeland Security, Justice, and State; and the CIA. In its written comments, DHS noted that it appreciated the report's identification of enhancements the department has made to several screening programs to address vulnerabilities exposed by the December 25, 2009, attempted attack, including actions taken by CBP and TSA. DHS also noted that it is committed to working with interagency stakeholders, including the Interagency Policy Committee, to ensure that its use of the watchlist in its screening programs is achieving intended results.[50] DHS also provided technical comments, in addition to its written comments. National Security Staff; the Office of the Director of National Intelligence; and the Departments of Defense, Justice, and State did not provide written comments to include in this report, but provided technical comments, which we have incorporated in this report where appropriate. The CIA did not provide any comments.

We are sending copies of this report to National Security Staff; the Attorney General; the Secretaries of the Departments of Defense, Homeland Security, and State; the Directors of National Intelligence and

[50]DHS's written comments are not included in this report because the department considered them to be Sensitive Security Information.

Central Intelligence; and appropriate congressional committees. This report is also available at no charge on the GAO website at http://www.gao.gov.

Should you or your staff have any questions about this report, please contact Eileen R. Larence at (202) 512-6510 or larencee@gao.gov. Key contributors to this report are acknowledged in appendix V. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report.

Eileen R. Larence
Director
Homeland Security and Justice Issues

*List of Requesters*

The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

The Honorable John F. Tierney
Ranking Member
Subcommittee on National Security, Homeland Defense and Foreign Operations
Committee on Oversight and Government Reform
House of Representatives

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

The Honorable Brian Higgins
Ranking Member
Subcommittee on Counterterrorism and Intelligence
Committee on Homeland Security
House of Representatives

The Honorable Sheila Jackson Lee
Ranking Member
Subcommittee on Transportation Security
Committee on Homeland Security
House of Representatives

# Appendix I: Objectives, Scope, and Methodology

## Objectives

Our reporting objectives were to determine (1) the actions the federal government has taken since the December 25, 2009, attempted attack to strengthen the watchlist nominations process, the extent to which departments and agencies are experiencing challenges in implementing revised watchlisting guidance, and the extent to which agencies are assessing impacts of the actions they have taken; (2) how the composition of the watchlist has changed as a result of actions taken by departments and agencies after the attempted attack; and (3) how screening and law enforcement agencies are addressing vulnerabilities exposed by the attempted attack as well as the outcomes of related screening, and to what extent federal agencies are assessing the impacts of this screening.

## Scope and Methodology

In general, we focused on the federal entities that were tasked by the Executive Office of the President to take corrective actions after the attempted attack:[1] the Department of Homeland Security (DHS); Department of Justice's Federal Bureau of Investigation (FBI) and Terrorist Screening Center (TSC); Department of State (State); Department of Defense; Office of the Director of National Intelligence's National Counterterrorism Center (NCTC); Central Intelligence Agency (CIA); and Executive Office of the President's National Security Staff.[2]

### Watchlist Nominations Process

To determine actions the federal government has taken to strengthen the watchlist nominations process, we analyzed postattack government reports, including reports issued by the Executive Office of the President and the Senate Select Committee on Intelligence.[3] We analyzed the

[1]Executive Office of the President, *Memorandum on Attempted Terrorist Attack on December 25, 2009: Intelligence, Screening, and Watchlisting System Corrective Actions* (Washington, D.C.: Jan. 7, 2010).

[2]NCTC—within the Office of the Director of National Intelligence—serves as the primary organization in the U.S. government for, among other things, analyzing and integrating all intelligence pertaining to terrorism and counterterrorism, except for intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism. See 50 U.S.C. § 404o(d)(1).

[3]Executive Office of the President, *Summary of the White House Review of the December 25, 2009, Attempted Terrorist Attack* (Washington, D.C.: Jan. 7, 2010), and Senate Select Committee on Intelligence, *Unclassified Summary of the Committee Report on the Attempted Terrorist Attack on Northwest Airlines Flight 253* (Washington, D.C.: May 18, 2010).

Watchlisting Guidance that was approved in July 2010 and compared it to the February 2009 watchlisting protocol—the last version that was published before the attempted attack—to identify changes that were intended to strengthen agencies' abilities to nominate known or suspected terrorist to the watchlist. We interviewed officials from five entities that nominate individuals for inclusion on the terrorist watchlist, as well as NCTC's Deputy Director for the Terrorist Identities and TSC's Director.[4] We also met with officials from the Executive Office of the President's Information Sharing and Access Interagency Policy Committee and its Subcommittee on Watchlisting, which provides an interagency forum to which agencies can bring watchlist-related issues for discussion and resolution.[5]

To identify to what extent agencies are experiencing challenges implementing changes to the watchlisting guidance, we analyzed data and documentation provided by seven federal entities involved in the nominations process—such as nominations data for the period January 2009 through May 2011—as well as the congressional testimony of NCTC, TSC, and FBI leadership and program directors.[6] We also interviewed the watchlisting unit directors and program staff at each of the five nominating agencies, NCTC's Deputy Director for the Terrorist Identities, and the TSC Director to discuss their nominations processes, the number of nominations they send to NCTC, and how, if at all, the changes to the nominations process have created challenges for each agency.

To determine to what extent agencies are assessing for the impacts of the actions they have taken, we interviewed officials from five federal entities who participate in the Information Sharing and Access

[4]In general, a nominating agency is any federal department or agency that has determined that an individual is a known or suspected terrorist and nominates that individual for inclusion in Terrorist Identities Datamart Environment (TIDE) database and the Terrorist Screening Database (TSDB).

[5]The Interagency Policy Committees are the main day-to-day forums for interagency coordination of national security policy, providing policy analysis and ensuring timely responses to decisions made by the President. See, Presidential Policy Directive 1, *Organization of the National Security Council System* (Feb. 13, 2009).

[6]Regarding nominations data, we did not review or assess the derogatory information available on individuals nominated to the terrorist watchlist, partly because such information involved ongoing counterterrorism or counterintelligence investigations.

Interagency Policy Committee's Subcommittee on Watchlisting and related working groups.

## Composition of the Watchlist

To identify how the composition of the watchlist has changed since the attempted attack, we reviewed TSC data from late December 2009 through March 2010 on the number of individuals who were added to TSC's Terrorist Screening Database and its subset No Fly and Selectee lists that are used to screen airline passengers before boarding, and related efforts to determine whether the individuals should remain on these lists.[7] To identify broader trends in the size and composition of the watchlist and subset lists, we reviewed TSC monthly data for 2009 and 2010 on the number of individuals on these lists, including U.S. citizens and lawful permanent residents. We also determined how the revised watchlisting guidance has impacted the size of these lists. Further, we interviewed senior-level officials from TSC and NCTC to identify factors that contributed to trends in the size of the lists during 2009 and 2010, and to obtain their perspectives on how changes in the watchlist guidance had impacted growth in the lists.

## Screening and Law Enforcement Agency Actions

To identify how screening and law enforcement agencies have addressed vulnerabilities exposed by the attempted attack and how they are assessing the outcomes and impacts of screening or vetting, we focused on the departments and agencies that use the watchlist to screen individuals traveling to the United States—the Transportation Security Administration (TSA), which screens passengers before they board aircraft; U.S. Customs and Border Protection (CBP), which inspects travelers to determine their admissibility into the United States; and State, which screens individuals who apply for U.S. visas.

To determine agency actions to address vulnerabilities in screening or vetting and related outcomes, we analyzed TSA, CBP, and State documentation—such as documents that discuss new or expanded screening programs—as well as testimonies and inspector general reports. We obtained data—generally for 2009 and 2010 but in some cases through May 2011—on how often these agencies have

[7]In general, individuals on the No Fly List are to be precluded from boarding an aircraft, and individuals on the Selectee List are to receive additional screening prior to boarding an aircraft.

encountered individuals on the watchlist and the outcomes of these encounters to help determine what impact changes in agency screening or vetting procedures has had on operations and the traveling public, among other things. We also interviewed senior-level officials from these agencies; these interviews included discussions about how agencies' screening or vetting procedures have changed since the attempted attack and how they are assessing the impacts of the changes. Further, to better understand the impacts of watchlist screening or vetting on the traveling public, we analyzed data for 2009 and 2010 on individuals who had inquiries or sought resolution regarding difficulties they experienced during their travel-related screening or inspection and interviewed DHS officials who are responsible for providing redress for these individuals. Regarding federal government efforts to assess the outcomes and impacts of actions agencies have taken to strengthen screening or vetting processes since the December 2009 attempted attack, we obtained information on the extent to which federal monitoring activities and practices are consistent with GAO's Standards for Internal Control in the Federal Government.[8]

To assess the reliability of data on watchlist nominations, number of watchlist records in databases, and screening outcomes, we interviewed knowledgeable officials about the data and the systems that produced the data, reviewed relevant documentation, examined data for obvious errors, and (when possible) corroborated the data among the different agencies. We determined that the data were sufficiently reliable for the purposes of this report. We conducted this performance audit from February 2010 to May 2012 in accordance with generally accepted government auditing standards. [9] Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[8]GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

[9]We issued a classified report on this work in December 2011.

# Appendix II: Overview of the Watchlist Nominations Process

Pursuant to Homeland Security Presidential Directive 6, the Terrorist Screening Center (TSC) was established to develop and maintain the U.S. government's consolidated watchlist—the Terrorist Screening Database (TSDB)—and to provide for the use of watchlist records during security-related screening processes.[1] The watchlisting and screening processes are intended to support the U.S. government's efforts to combat terrorism by consolidating the terrorist watchlist and providing screening and law enforcement agencies with information to help them respond appropriately during encounters with known or suspected terrorists, among other things.

TSC receives watchlist information for inclusion in the TSDB from two sources: the National Counterterrorism Center (NCTC) and the Federal Bureau of Investigation (FBI). TSC receives the vast majority of its watchlist information from NCTC, which compiles information on known or suspected international terrorists from executive branch departments and agencies—such as the Central Intelligence Agency (CIA), Department of State (State), and the FBI—and maintains the information in its Terrorist Identities Datamart Environment (TIDE) database.[2] According to NCTC, the TIDE database includes, to the extent permitted by law, all information the U.S. government possesses related to the identities of individuals known or suspected to be or have been involved in activities constituting, in preparation for, in aid of, or related to terrorism, with the exception of purely domestic terrorism information. Examples of conduct that will warrant an entry into TIDE include persons who

- engage in international terrorist activity;
- prepare or plan international terrorist activity;
- gather information on potential targets for international terrorist activity;
- solicit funds or other things of value for international terrorist activity or a terrorist organization;
- solicit membership in an international terrorist organization;
- provide material support, such as a safe house, transportation, communications, funds, transfer of funds or other material financial

[1]Homeland Security Presidential Directive 6: *Integration and Use of Screening Information* (Sept. 16, 2003).

[2]TIDE is the U.S. government's central repository of information on known or suspected international terrorists and is maintained by NCTC.

benefit, false documentation or identification, weapons, explosives, or training; or
- are members of or represent a foreign terrorist organization.[3]

In general, nominating agencies submit terrorism-related information to NCTC to add information to existing records in TIDE as well as to nominate new individuals to be included in TIDE, with the additional purpose of nominating known or suspected terrorists to the TSDB. Nominations are to include pertinent derogatory information and any biographic information—such as name and date of birth—needed to establish the identity of individuals on the watchlist.

The FBI provides TSC with information about known or suspected domestic terrorists. According to the FBI's Domestic Terrorist Operations Unit, domestic terrorists engage in activities that (1) involve acts dangerous to human life that are a violation of the criminal laws of the United States or any state; (2) appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by mass destruction, assassination, or kidnapping; and (3) occur primarily within the jurisdiction of the United States.[4]

In general, the FBI nominates individuals who are subjects of ongoing FBI counterterrorism investigations to TSC for inclusion in the TSDB, including persons the FBI is preliminarily investigating to determine if they have links to terrorism. In determining whether to open an investigation, the FBI uses guidelines established by the Attorney General, which contain specific standards for opening investigations. The FBI also has a process for submitting requests to NCTC to nominate known or suspected international terrorists who are not subjects of FBI investigations.

In accordance with Homeland Security Presidential Directive 6—and built upon through Homeland Security Presidential Directives 11 and 24—the TSDB is to contain information about individuals known or suspected to

[3]In general, these types of conduct are related to provisions in the Immigration and Nationality Act that establishes grounds for alien admissibility on terrorist-related grounds. See, e.g., 8 U.S.C. § 1182(a)(3) (codifying section 212(a)(3) of the Immigration and Nationality Act, as amended).

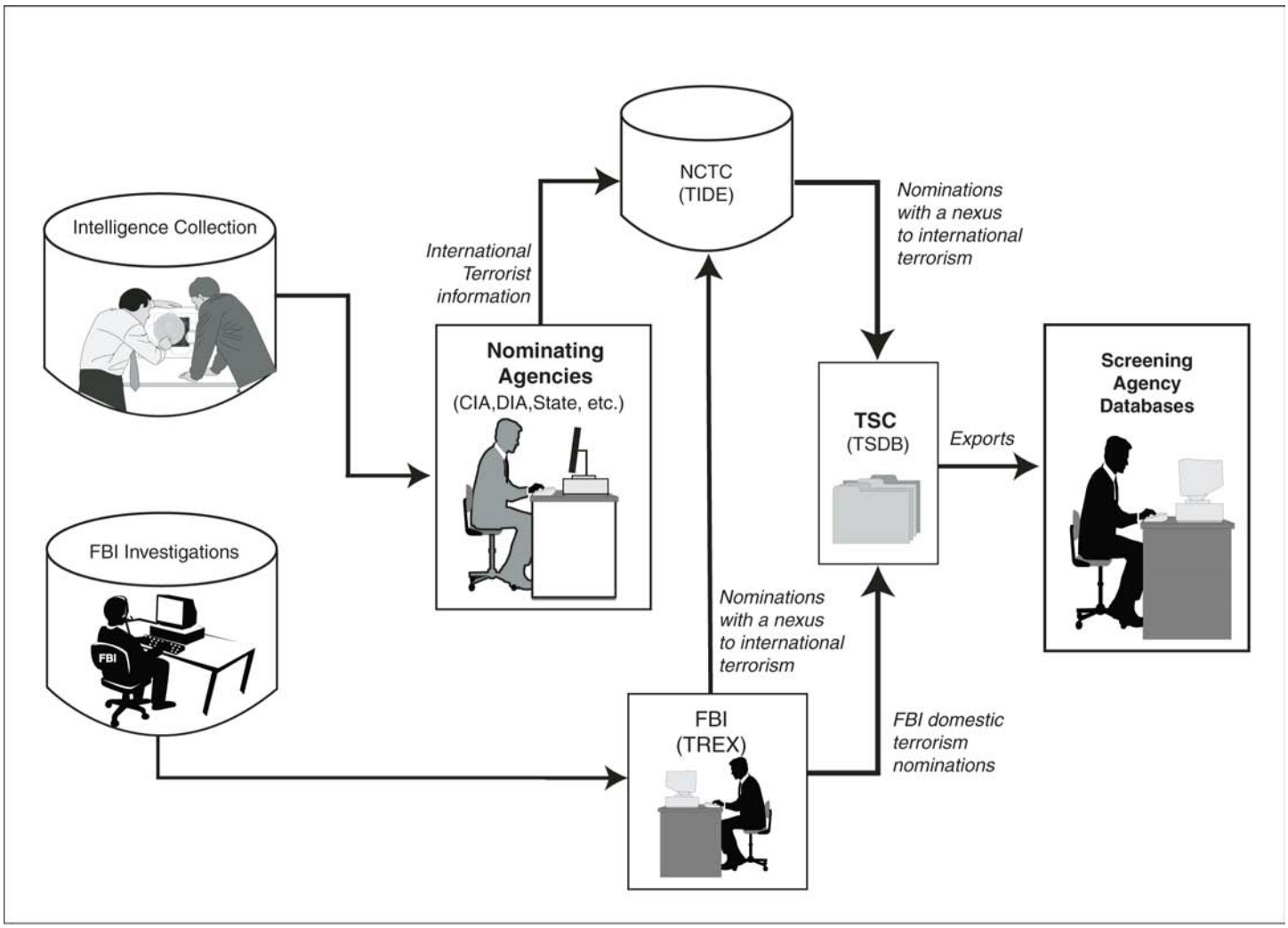
[4]See 18 U.S.C. § 2331(5).

be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism and terrorist activities.[5] NCTC and the FBI apply a reasonable-suspicion standard to determine which individuals are appropriate for inclusion in the TSDB. Determining whether individuals meet this standard, however, can involve some level of subjectivity. NCTC and the FBI are to consider information from all available sources and databases—including information forwarded by nominating agencies as well as information in their own holdings—to determine if there is a reasonable suspicion of links to terrorism that warrants a nomination.

Once NCTC and the FBI determine that an individual meets the reasonable-suspicion standard and that minimum biographic information exists, they extract sensitive but unclassified information on the individual's identity—such as name and date of birth—from their classified databases and send the information to TSC. TSC reviews these nominations—evaluating the derogatory and biographic information, in accordance with the watchlisting guidance—to determine whether to add nominated individuals to the TSDB. As TSC adds individuals to the watchlist, the list may include persons with possible ties to terrorism in addition to people with known links, thereby establishing a broad spectrum of individuals who are considered known or suspected terrorists. Figure 2 provides an overview of the process used to nominate individuals for inclusion in the TSDB.

[5]See, Homeland Security Presidential Directive 11: *Comprehensive Terrorist-Related Screening Procedures* (Aug. 27, 2004) and Homeland Security Presidential Directive 24*: Biometrics for Identification and Screening to Enhance National Security* (June 5, 2008).

**Figure 2: Overview of the Watchlist Nominations Process**




Source: GAO analysis of TSC information.

Consistent with Homeland Security Presidential Directive 6, to ensure that watchlist information is current, accurate, and complete, nominating agencies generally are to provide information to remove an individual from the watchlist when it is determined that no nexus to terrorism exists.

To support agency screening or law enforcement processes, TSC sends applicable records from the TSDB to screening or law enforcement agency systems for use in efforts to deter or detect the movement of

known or suspected terrorists. For instance, applicable TSC records are provided to TSA for use in screening airline passengers, to U.S. Customs and Border Protection (CBP) for use in vetting and inspecting persons traveling to and from the United States, and to State for use in screening visa applicants. Regarding individuals who are not citizens or nationals of the United States seeking travel to and entry into the United States, screening and law enforcement agencies rely on immigration laws that specify criteria and rules for deciding whether to issue visas to individuals or to admit them into the country.[6] In many instances, individuals who are not citizens or nationals of the United States who have engaged in or are likely to engage in terrorist-related activities may be ineligible to receive visas or inadmissible for entry to the United States, or both. If a foreign citizen is lawfully admitted into the United States—either permanently or temporarily—and subsequently engages in or is likely to engage in a terrorist activity, the individual, in certain circumstances, may be removed to his or her country of citizenship. U.S. citizens returning to the United States from abroad are not subject to the admissibility requirements of the Immigration and Nationality Act, regardless of whether they are subjects of watchlist records. In general, these individuals only need to establish their U.S. citizenship to the satisfaction of the examining officer—by, for example, presenting a U.S. passport—to obtain entry into the United States.[7] U.S. Citizens are subject to inspection by CBP before being permitted to enter, and additional actions may be taken, as appropriate.

[6]See, e.g., 8 U.S.C. § 1182 (codifying § 212 of the Immigration and Nationality Act, as amended, and establishing conditions under which an alien—any person not a citizen or national of the United States—may be deemed ineligible for a visa or inadmissible to the United States).

[7]See 8 C.F.R. § 235.1. Similarly, lawful permanent residents generally are not regarded as seeking admission to the United States and are not subject to the grounds for inadmissibility unless they fall within certain criteria listed at 8 U.S.C. § 1101(a)(13)(C) that describe why an alien lawfully admitted for permanent residence would be regarded as seeking admission. Lawful permanent residents, however, may be subject to the grounds of removability under 8 U.S.C. § 1227(a) after admission.

# Appendix III: Transportation Security Administration's Secure Flight Program and Related Activities

This appendix presents an overview of the Transportation Security Administration's (TSA) Secure Flight program, which began implementation before the December 25, 2009, attempted attack and is a key part of TSA's efforts to address vulnerabilities that were exposed by the incident. This appendix also discusses how the program has reduced the likelihood of passengers misidentified as being on the watchlist and provides an update on the status of TSA efforts to validate the information that passengers report when making a reservation that is used in the watchlist-matching process.

## Secure Flight Overview

The matching of airline passenger information against terrorist watchlist records is a frontline defense against acts of terrorism that target the nation's civil aviation system. In general, passengers identified by the TSA as a match to the No Fly List are prohibited from boarding flights to, from, and within the United States, while those matched to the Selectee List are required to undergo additional screening prior to boarding such flights.[1] Historically, airline passenger prescreening was performed by air carriers pursuant to federal requirements. However, in accordance with the Intelligence Reform and Terrorism Prevention Act of 2004, TSA developed an advanced passenger prescreening program known as Secure Flight that enabled TSA to assume from air carriers the function of watchlist matching.[2] Secure Flight is intended to

- eliminate inconsistencies in passenger watchlist matching procedures conducted by air carriers and use a larger set of watchlist records when warranted,
- reduce the number of individuals who are misidentified as being on the No Fly or Selectee lists,
- reduce the risk of unauthorized disclosure of sensitive watchlist information, and

[1]The No Fly and Selectee lists are subsets of the consolidated terrorist watchlist that is maintained by the Federal Bureau of Investigation's Terrorist Screening Center.

[2]See Pub. L. No. 108-458, § 4012(a), 118 Stat. 3638, 3714-18 (2004) (codified at 49 U.S.C. § 44903(j)(2)(C)). See also Secure Flight Program; Final Rule, 73 Fed. Reg. 64,018 (Oct. 28, 2008).

- integrate information from DHS's redress process into watchlist matching so that individuals are less likely to be improperly or unfairly delayed or prohibited from boarding an aircraft.[3]

In January 2009, the Secure Flight program began initial operations—assuming the watchlist-matching function for a limited number of domestic flights for one airline—and subsequently phased in additional flights and airlines. TSA completed assumption of this function for all domestic and international flights operated by U.S. air carriers in June 2010 and completed assumption of this function for covered foreign air carriers flying to and from the United States in November 2010.[4]

## Secure Flight Has Reduced Misidentifications

Since the December 2009 attempted attack, TSA has completed its assumption of the watchlist-matching function from air carriers—under the Secure Flight program—which has reduced the likelihood of passengers misidentified as being on the watchlist. According to TSA data, Secure Flight is consistently clearing over 99 percent of passengers automatically (less than 1 percent of passengers are being misidentified as being on the No Fly List or Selectee List). When misidentifications occur, a passenger may not be able to print a boarding pass from a computer or an airport kiosk. Rather, the individual may have to go to the airline ticket counter to provide identifying information that is used to determine if the person is a positive match to the No Fly List or Selectee List. Before Secure Flight, more passengers had to go through this process to verify their identities, since each airline conducted watchlist matching differently with varying effectiveness.

The Secure Flight program increases the effectiveness of watchlist matching, applying an enhanced watchlist-matching system and process consistently across the airline industry. Under Secure Flight, air carriers are required to (1) collect full name and date-of-birth and gender information from airline passengers and (2) be capable of collecting

[3]See GAO, *Aviation Security: TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks,* GAO-09-292 (Washington, D.C.: May 13, 2009). In general, the term redress refers to an agency's complaint resolution process whereby individuals may seek resolution of their concerns about an agency action.

[4]Secure Flight also performs this screening function for covered airline flights that travel over the continental United States and "point-to-point" international flights operated by covered U.S.-based airlines.

redress control numbers from passengers.[5] Collecting such information helps reduce misidentifications. According to TSA, Secure Flight is required to submit an annual report to the Office of Management and Budget certifying that the program has met its baseline goal for reducing misidentifications.

Further, people who have been denied or delayed airline boarding, have been denied or delayed entry into or exit from the United States at a port of entry or border crossing; or have been repeatedly referred to additional (secondary) inspection can file an inquiry to seek redress. After completing the redress process—which includes submitting all applicable documents—an individual will receive a redress control number that may facilitate future travel. For example, airline passengers who have completed the redress process and are determined by DHS as not being the subject of a watchlist record are put on the department's list of individuals who are "cleared" to travel. Using the redress control number when making reservations for future travel may help to prevent misidentifications.

To mitigate future risks of performance shortfalls and strengthen management of the Secure Flight program moving forward, in May 2009, we recommended that TSA periodically assess the performance of the Secure Flight system's matching capabilities and results to determine whether the system is accurately matching watchlisted individuals while minimizing the number of false positives, consistent with the goals of the program; document how this assessment will be conducted and how its results will be measured; and use these results to determine whether the system settings should be modified.[6] TSA's actions discussed below fully respond to the recommendation we made in our May 2009 report.

TSA has developed performance measures to report on and monitor Secure Flight's name matching capabilities. According to TSA, Secure Flight leadership reviews the daily reports, which reflect quality, match rate, false positive rates, and other metrics. Reviews are to include analysis, discussion with program leadership, and identification of

[5]The Secure Flight Final Rule provides that air carriers must request a passenger's full name, gender, date of birth, and Redress or Known Traveler Number (if available), but it only requires that passengers provide their full name, gender, and date of birth.

[6]GAO-09-292.

process and data quality improvements to increase efficiency and reduce possible false positive matches to the watchlist. In addition, DHS established a multidepartmental Match Review Board Working Group and a Match Review Board to, among other things, review the performance measures and recommend changes to improve system performance. According to TSA, the working group meets on a biweekly basis and the board meets monthly, or as required, to review working group findings and to make system change recommendations. For example, the board has recommended changes in the threshold used for determining whether an individual is a match to a watchlist record and has decided to implement additional search tools to enhance Secure Flight's automated name-matching capabilities. Furthermore, TSA plans to periodically assess the extent to which the Secure Flight program fails to identify individuals who are actual matches to the watchlist.

# Appendix IV: Redress Process for Individuals Experiencing Difficulties during Travel-Related Screening and Inspection

The DHS Traveler Redress Inquiry Program (DHS TRIP) is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs—like airports and train stations—or crossing U.S. borders, including

- watchlist issues;
- inspection problems at ports of entry; and
- situations where travelers believe they have been unfairly or incorrectly delayed, denied boarding, or identified for additional screening or inspection at our nation's transportation hubs.

While serving as the point of contact for the receipt, tracking, and response to redress applications, DHS TRIP generally refers cases to the appropriate screening agency for review and adjudication.

## Changes to DHS TRIP Watchlist-Related Procedures since the Attempted Attack

According to DHS TRIP officials, since the December 2009 attempted attack, the office implemented a new procedure to ensure that (1) the office is promptly notified when an individual who is determined by DHS TRIP as not being the subject a watchlist record—and, therefore, has been put on the department's list of individuals who are "cleared" to travel—is subsequently added to the watchlist and (2) redress applicants are provided additional information regarding the resolution of their cases. Prior to the attempted attack, DHS TRIP would conduct electronic comparisons once each day to ensure that someone who had been cleared as a result of the redress process had not subsequently been added to the watchlist. Since the attempted attack, DHS TRIP now conducts continuous checks (on a 24/7 basis) of cleared individuals against the watchlist every time the watchlist is updated. According to DHS TRIP officials, this change provides the office immediate notification if an individual who is cleared through the redress process is subsequently added to the watchlist. In turn, DHS TRIP officials can alert screening agencies more quickly that an individual should not be cleared if encountered during screening.

Separately, DHS TRIP—at the direction of the Secretary of Homeland Security and in partnership with the Terrorist Screening Center (TSC), Departments of Justice and State, Federal Bureau of Investigation (FBI), and other members of the interagency redress community—has taken steps intended to help provide transparency to redress applicants regarding the resolution of their cases.

## DHS TRIP Redress Data and Related Information

According to DHS TRIP data, individuals submitted approximately 32,000 applications for redress during 2009 and 36,000 applications during 2010.[1] The DHS TRIP redress application asks travelers to identify their areas of concern, but the information collected generally does not allow DHS TRIP officials to determine if individuals were misidentified as being on the watchlist. DHS TRIP officials explained that since the application allows travelers to list multiple reasons for applying—and the individuals generally do not know why they were subject to additional screening, inspection, or delay—the office cannot conclude with certainty that being misidentified as being on the watchlist was the cause of an applicant's inconvenience. In late 2009, as part of the rollout of TSA's Secure Flight program, several air carriers instituted a public awareness campaign encouraging travelers to submit redress inquiries if they believed that they have been misidentified in the past. Finally, DHS TRIP officials noted that individual screening and law enforcement agencies are in the best position to understand if their screening and law enforcement systems and procedures incorrectly identify individuals as matches with watchlist records. The officials explained that these agencies have access to more detailed records that would identify reasons for a delay or inconvenience, including a misidentification to the watchlist.

According to DHS TRIP, less than 1 percent of individuals who apply for redress have been confirmed matches to the watchlist or have identifying information (e.g., name and date of birth) that closely matches someone on the watchlist. In such cases, DHS TRIP forwards the inquiry to TSC for resolution. TSC data show that the government has procedures in place to review the information that supports a watchlist record upon receipt of a redress inquiry and has revised the watchlist status of individuals based on these reviews. We did not review the effectiveness of these procedures.

[1]According to DHS TRIP officials, these numbers could include multiple inquiries from individuals providing additional supporting documentation, reapplying regarding the same issue, or reporting other travel-related difficulties. In addition, the officials said that a small number of inquiries are related to misdirected communications sent to DHS TRIP from outside parties, including law offices.

# Appendix V: GAO Contact and Staff Acknowledgments

## GAO Contact

Eileen R. Larence, (202) 512-6510 or larencee@gao.gov

## Staff Acknowledgments

In addition to the contact named above, Eric Erdman, Assistant Director; Mona Blake; Jeffrey DeMarco; Michele Fejfar; Lisa Humphrey; Richard Hung; Thomas Lombardi; Linda Miller; Victoria Miller; Jan Montgomery; Timothy Persons; and Michelle Woods made key contributions to this report.