

October 2007

TERRORIST WATCH LIST SCREENING

Opportunities Exist to
Enhance Management
Oversight, Reduce
Vulnerabilities in
Agency Screening
Processes, and
Expand Use of the List





Highlights of [GAO-08-110](#), a report to congressional requesters

Why GAO Did This Study

The Federal Bureau of Investigation's (FBI) Terrorist Screening Center (TSC) maintains a consolidated watch list of known or appropriately suspected terrorists and sends records from the list to agencies to support terrorism-related screening. Because the list is an important tool for combating terrorism, GAO examined (1) standards for including individuals on the list, (2) the outcomes of encounters with individuals on the list, (3) potential vulnerabilities and efforts to address them, and (4) actions taken to promote effective terrorism-related screening.

To conduct this work, GAO reviewed documentation obtained from and interviewed officials at TSC, the FBI, the National Counterterrorism Center, the Department of Homeland Security, and other agencies that perform terrorism-related screening.

What GAO Recommends

GAO is making recommendations to promote a comprehensive and coordinated approach to terrorist-related screening. Among them are actions to monitor and respond to vulnerabilities and to establish up-to-date guidelines, strategies, and plans to facilitate expanded and enhanced use of the list.

GAO provided a draft copy of this report to relevant departments and agencies. The departments that provided comments generally agreed with GAO's findings and recommendations.

To view the full product, including the scope and methodology, click on [GAO-08-110](#). For more information, contact Eileen Larence at (202) 512-8777 or larencee@gao.gov.

TERRORIST WATCH LIST SCREENING

Opportunities Exist to Enhance Management Oversight, Reduce Vulnerabilities in Agency Screening Processes, and Expand Use of the List

What GAO Found

The FBI and the intelligence community use standards of reasonableness to evaluate individuals for nomination to the consolidated watch list. In general, individuals who are reasonably suspected of having possible links to terrorism—in addition to individuals with known links—are to be nominated. As such, being on the list does not automatically prohibit, for example, the issuance of a visa or entry into the United States. Rather, when an individual on the list is encountered, agency officials are to assess the threat the person poses to determine what action to take, if any. As of May 2007, the consolidated watch list contained approximately 755,000 records.

From December 2003 through May 2007, screening and law enforcement agencies encountered individuals who were positively matched to watch list records approximately 53,000 times. Many individuals were matched multiple times. The outcomes of these encounters reflect an array of actions, such as arrests; denials of entry into the United States; and, most often, questioning and release. Within the federal community, there is general agreement that the watch list has helped to combat terrorism by (1) providing screening and law enforcement agencies with information to help them respond appropriately during encounters and (2) helping law enforcement and intelligence agencies track individuals on the watch list and collect information about them for use in conducting investigations and in assessing threats.

Regarding potential vulnerabilities, TSC sends records daily from the watch list to screening agencies. However, some records are not sent, partly because screening against them may not be needed to support the respective agency's mission or may not be possible due to the requirements of computer programs used to check individuals against watch list records. Also, some subjects of watch list records have passed undetected through agency screening processes and were not identified, for example, until after they had boarded and flew on an aircraft or were processed at a port of entry and admitted into the United States. TSC and other federal agencies have ongoing initiatives to help reduce these potential vulnerabilities, including efforts to improve computerized name-matching programs and the quality of watch list data.

Although the federal government has made progress in promoting effective terrorism-related screening, additional screening opportunities remain untapped—within the federal sector, as well as within critical infrastructure components of the private sector. This situation exists partly because the government lacks an up-to-date strategy and implementation plan for optimizing use of the terrorist watch list. Also lacking are clear lines of authority and responsibility. An up-to-date strategy and implementation plan, supported by a clearly defined leadership or governance structure, would provide a platform to establish governmentwide screening priorities, assess progress toward policy goals and intended outcomes, consider factors related to privacy and civil liberties, ensure that any needed changes are implemented, and respond to issues that hinder effectiveness.

Contents

Letter		1
	Results in Brief	7
	Background	13
	In Assessing Individuals for Inclusion on TSC’s Watch List, Officials Rely upon Standards of Reasonableness That Inherently Involve Some Subjectivity	18
	Agencies Have Had Approximately 53,000 Encounters with Individuals on the Watch List, and Outcomes Indicate the List Has Helped to Combat Terrorism	25
	TSC Exports Applicable Watch List Records to Screening Agency Databases, Depending on Agency Mission and Technical Capacity; but Some Technical Requirements May Present Security Vulnerabilities	30
	DHS Agencies Are Addressing Incidents of Persons on the Watch List Passing Undetected through Screening; TSC Has Ongoing Initiatives That Could Help Reduce This Vulnerability	37
	The U.S. Government Has Made Progress in Using the Watch List but a Strategy and Plan Supported by a Governance Structure with Clear Lines of Authority Would Enhance Use and Effectiveness	45
	Conclusions	53
	Recommendations for Executive Action	55
	Agency Comments and Our Evaluation	56
Appendix I	Objectives, Scope, and Methodology	60
Appendix II	Homeland Security Presidential Directive/HSPD-6 (Sept. 16, 2003)	66
Appendix III	Homeland Security Presidential Directive/HSPD-11 (Aug. 27, 2004)	68
Appendix IV	Outcomes of Screening Agency Encounters with Individuals on the Terrorist Watch List	71

Appendix V**Comments from the Department of Homeland Security 77**

Table

Table 1: Distribution List for TSC's Daily Summary of Positive Matches	29
------------------------------------------------------------------------	----

Figures

Figure 1: General Overview of the Process Used to Resolve Encounters with Individuals on the Terrorist Watch List	17
Figure 2: General Overview of the Process Used to Nominate Individuals for Inclusion on TSC's Watch List	23
Figure 3: Increase in Terrorist Watch List Records, June 2004 through May 2007	24
Figure 4: General Overview of the Process Used to Export Records from TSC's Consolidated Watch List to Screening Agency Databases	31

Abbreviations

CBP	U.S. Customs and Border Protection
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
HSPD	Homeland Security Presidential Directive
NCTC	National Counterterrorism Center
TSA	Transportation Security Administration
TSC	Terrorist Screening Center

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

October 11, 2007

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

The Honorable Carl Levin
Chairman
The Honorable Norm Coleman
Ranking Member
Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Bennie G. Thompson
Chairman
The Honorable Peter T. King
Ranking Member
Committee on Homeland Security
House of Representatives

Since the events of September 11, 2001, agencies within the Departments of Homeland Security, Justice, and State, as well as state and local law enforcement organizations and the intelligence community, have implemented enhanced procedures to collect and share information about known or suspected terrorists who pose a threat to homeland security and to track their movements. One important tool used by these agencies is the terrorist watch list, which contains records with identifying or

biographical information—such as name and date of birth—of foreign and U.S. citizens with known or appropriately suspected links to terrorism.¹

Pursuant to Homeland Security Presidential Directive 6, the Terrorist Screening Center—an entity that has been operational since December 2003 under the administration of the Federal Bureau of Investigation (FBI)—was established to develop and maintain the U.S. government’s consolidated terrorist screening database (the watch list) and to provide for the use of watch list records during security-related screening processes.² To build upon and provide additional guidance related to this directive, in August 2004, the President signed Homeland Security Presidential Directive 11.³ Among other things, this directive required the Secretary of Homeland Security—in coordination with the heads of appropriate federal departments and agencies—to outline a strategy to enhance the effectiveness of terrorist-related screening activities and develop a prioritized investment and implementation plan for detecting and interdicting suspected terrorists and terrorist activities.

The Terrorist Screening Center receives the vast majority of its information about known or appropriately suspected terrorists from the National Counterterrorism Center, which compiles information on international terrorists from a wide range of executive branch departments and agencies, such as the Department of State, the Central Intelligence Agency, and the FBI. In general, international terrorists engage in terrorist activities that occur primarily outside the territorial

¹There is no specific definition of terrorism for purposes of the watch list, though agencies utilizing watch list records recognize various definitions of the term. For example, the Federal Bureau of Investigation defines terrorism to include the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. See 28 C.F.R. § 0.85(l). See also, e.g., 18 U.S.C. § 2331 and 22 U.S.C. § 2656f(d) (providing definitions of terrorism and international terrorism in criminal and foreign relations contexts, respectively). Also, terrorist activity has been more broadly defined in the Immigration and Nationality Act for purposes of immigration benefits. See 8 U.S.C. § 1182(a)(3)(B). Additional information on standards used to determine whether an individual is a “known or appropriately suspected terrorist”—which for purposes of this report includes any individual known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism—is discussed later in this report.

²The White House, *Homeland Security Presidential Directive/HSPD-6, Subject: Integration and Use of Screening Information* (Washington, D.C.: Sept. 16, 2003).

³The White House, *Homeland Security Presidential Directive/HSPD-11, Subject: Comprehensive Terrorist-Related Screening Procedures* (Washington, D.C.: Aug. 27, 2004).

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. In addition to providing information on international terrorists to the National Counterterrorism Center, the FBI directly provides the Terrorist Screening Center with information about known or suspected domestic terrorists, that is, individuals who operate primarily within the United States, such as Ted Kaczynski (the “Unabomber”). The center consolidates this information into a sensitive but unclassified watch list and makes records available as appropriate for a variety of screening purposes. For instance, the Transportation Security Administration directs airlines to use portions of the Terrorist Screening Center’s watch list—the No Fly and Selectee lists—to screen the names of passengers to identify those who may pose threats to aviation.⁴ Also, to help ensure that known or appropriately suspected terrorists are tracked, and denied entry into the United States, as appropriate, applicable watch list records are to be checked by Department of State consular officers before issuing U.S. visas and passports, and by U.S. Customs and Border Protection officers before admitting persons—including U.S. citizens—at air, land, and sea ports of entry. Further, screening against applicable watch list records can occur anywhere in the nation when, for example, state or local law enforcement officers stop individuals for traffic violations or other offenses.

When an individual on the terrorist watch list is identified or encountered during screening, several entities—the Terrorist Screening Center, the screening agency, investigative agencies, and the intelligence community—can be involved in deciding what action to take.⁵ Regarding a foreign citizen seeking to immigrate to the United States permanently or temporarily for business or pleasure purposes, screening agencies rely on immigration laws that specify criteria and rules for deciding whether or not to admit the individual.⁶ In general, foreign citizens that have engaged in or are likely to engage in terrorist-related activities are ineligible to

⁴In 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 physical screening prior to boarding an aircraft.

⁵As used in this report, the term “encounter” refers to any incident where a screening or law enforcement entity has contact with a person who is positively matched to a record in the terrorist watch list.

⁶See, 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).

receive visas and ineligible to enter the United States. If a foreign citizen is legally admitted into the United States—either permanently or temporarily—and subsequently engages in or is likely to engage in a terrorist activity, the individual may be removed to that person’s country of citizenship. U.S. citizens returning to the United States from abroad are not subject to the admissibility requirements applicable to foreign citizens, regardless of whether or not they are subjects of watch list records. 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 These individuals, however, can be subjected to additional screening by U.S. Customs and Border Protection before being admitted to determine the potential threat they pose, with related actions taken, if needed.

This report is a public version of the restricted report that we also provided to you on October 11, 2007. The various departments and agencies we reviewed deemed some of the information in the restricted report as Sensitive Security Information or Law Enforcement Sensitive information, which must be protected from public disclosures. Therefore, this report omits certain information associated with vulnerabilities we identified in existing screening processes and measures that could be taken to address those vulnerabilities. This report also omits key details regarding (1) certain policies and procedures associated with the development and use of the terrorist watch list and (2) specific outcomes of encounters with individuals who were positively matched to the watch list. In the context of agency efforts to screen for known or appropriately suspected terrorists, the restricted report addressed the following questions:

- In general, what standards do the National Counterterrorism Center and the FBI use in determining which individuals are appropriate for inclusion on the Terrorist Screening Center’s consolidated watch list?
- Since the Terrorist Screening Center became operational in December 2003, how many times have screening and law enforcement agencies positively matched individuals to terrorist watch list records, and what

⁷See 8 C.F.R. § 235.1. Similarly, lawful permanent residents generally are not regarded as seeking admission to the United States and, as with U.S. citizens, 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.

do the results or outcomes of these encounters indicate about the role of the watch list as a counterterrorism tool?

- To what extent do the principal screening agencies whose missions most frequently and directly involve interactions with travelers check against all records in the Terrorist Screening Center's consolidated watch list? If the entire watch list is not being checked, why not, what potential vulnerabilities exist, and what actions are being planned to address these vulnerabilities?
- To what extent are Department of Homeland Security component agencies monitoring known incidents in which subjects of watch list records pass undetected through screening processes, and what corrective actions have been implemented or are being planned to address these vulnerabilities?
- What actions has the U.S. government taken to ensure that the terrorist watch list is used as effectively as possible, governmentwide and in other appropriate venues?

Although the information provided in this version of the report is more limited in scope, it covers the same general questions as the restricted report. Also, the overall methodology used for our restricted report is relevant to this report because the information contained in this report was derived from the restricted report. To address the questions in our restricted report, we reviewed the Terrorist Screening Center's standard operating procedures, statistics on encounters with individuals on the terrorist watch list, and other relevant documentation; and we interviewed Terrorist Screening Center officials, including the director and the principal deputy director. To identify standards used to nominate individuals for inclusion on the watch list, we reviewed documentation and interviewed senior officials from the National Counterterrorism Center and the FBI.

Also, to assess the outcomes of encounters and the extent to which screening agencies check against the entire watch list, we reviewed documentation and interviewed senior officials from the FBI's Counterterrorism Division and the principal screening agencies whose missions most frequently and directly involve interactions with travelers. Specifically, at the Transportation Security Administration, we examined the prescreening of air passengers prior to their boarding a flight; at U.S. Customs and Border Protection, we examined the screening of travelers entering the United States through ports of entry; and, at the Department

of State, we examined the screening of nonimmigrant visa applicants. We did not review the Department of State's use of the watch list to screen passport applicants. We also visited a nonprobability sample of screening agencies and investigative agencies in geographic areas of four states (California, Michigan, New York, and Texas).⁸ We chose these locations on the basis of geographic variation and other factors. Further, to determine the extent to which agencies monitor known incidents in which subjects of watch list records pass undetected through screening processes and efforts to address these vulnerabilities, we reviewed documentation and interviewed senior officials from U.S. Customs and Border Protection, U.S. Citizenship and Immigration Services—which screens individuals who apply for immigration benefits or U.S. citizenship—and the Transportation Security Administration. Finally, to assess the actions the U.S. government has taken to ensure that the terrorist watch list is used as effectively as possible, we compared the status of watch list-related strategies, planning, and initiatives with the expectations set forth in Homeland Security Presidential Directives 6 and 11. We considered federal plans to identify screening opportunities, the private sector's use of watch list records, and the Department of State's progress in sharing watch list information with foreign governments.

Regarding statistical information we obtained from the Terrorist Screening Center and screening agencies—such as the number of positive matches and actions taken—we discussed the sources of the data with agency officials and reviewed documentation regarding the compilation of the statistics. We determined that the statistics were sufficiently reliable for the purposes of this review. We did not review or assess the derogatory information available on individuals nominated to the terrorist watch list, partly because such information involved ongoing counterterrorism investigations. Also, a primary agency that collects information on known or suspected terrorists—the Central Intelligence Agency—declined to meet with us or provide us documentation on its watch list-related activities. The Homeland Security Council—which is chaired by the Assistant to the President for Homeland Security and Counterterrorism—

⁸In a nonprobability sample, some elements of the population being studied have no chance or an unknown chance of being selected as part of the sample. Thus, results from a nonprobability sample cannot be used to make inferences about the population.

also denied our request for an interview.⁹ We performed our work on the restricted version of this report from April 2005 through September 2007 in accordance with generally accepted government auditing standards. Appendix I presents more details about our objectives, scope, and methodology.

Results in Brief

The National Counterterrorism Center and the FBI rely upon standards of reasonableness in determining which individuals are appropriate for inclusion on the Terrorist Screening Center's consolidated watch list. In general, individuals who are reasonably suspected of having possible links to terrorism—in addition to individuals with known links—are to be nominated. To determine if the suspicions are reasonable, the National Counterterrorism Center and the FBI are to assess all available information on the individual. According to the National Counterterrorism Center, determining whether to nominate an individual can involve some level of subjectivity. Nonetheless, any individual reasonably suspected of having links to terrorist activities is to be nominated to the list and remain on it until the FBI or the agency that supplied the information supporting the nomination, such as one of the intelligence agencies, determines the person is not a threat and should be removed from the list. Moreover, according to the FBI, individuals who are subjects of ongoing FBI counterterrorism investigations are generally nominated to the list. If an investigation finds no nexus to terrorism, the FBI generally is to close the investigation and request that the Terrorist Screening Center remove the person from the watch list. Because individuals can be added to the list based on reasonable suspicion, inclusion on the list does not automatically prohibit an individual from, for example, obtaining a visa or entering the United States. Rather, when an individual on the list is encountered, agency officials are to assess the threat the person poses to determine what action to take, if any. Based on these standards, the number of records in the Terrorist Screening Center's consolidated watch list has

⁹The Homeland Security Council was established to ensure coordination of all homeland security-related activities among executive departments and agencies and promote the effective development and implementation of all homeland security policies. See The White House, *Homeland Security Presidential Directive/HSPD-1, Subject: Organization and Operation of the Homeland Security Council* (Washington, D.C.: Oct. 29, 2001).

increased from about 158,000 records in June 2004 to about 755,000 records as of May 2007.¹⁰

From December 2003 (when the Terrorist Screening Center began operations) through May 2007, screening and law enforcement agencies encountered individuals who were positively matched to watch list records approximately 53,000 times, according to Terrorist Screening Center data.¹¹ Many individuals were positively matched to watch list records multiple times. Agencies took a range of actions in response to these encounters, such as arresting individuals and denying others entry into the United States. Most often, however, the agencies questioned and then released the individuals because there was not sufficient evidence of criminal or terrorist activity to warrant further legal action. Our analysis of data on outcomes and our interviews with screening agency, law enforcement, and intelligence community officials indicate that the use of the watch list has enhanced the government's counterterrorism efforts in two ways:

- Use of the watch list has helped federal, state, and local screening and law enforcement officials obtain information to make better-informed decisions when they encounter an individual on the list as to the threat posed and the appropriate response or action to take, if any.
- Information collected from watch list encounters is shared with agents conducting counterterrorism investigations and with the intelligence community for use in analyzing threats. Such coordinated collection of information for use in investigations and threat analyses is one of the stated policy objectives for the watch list.

The principal screening agencies whose missions most frequently and directly involve interactions with travelers do not check against all records in the Terrorist Screening Center's consolidated watch list because screening against certain records (1) may not be needed to support the

¹⁰The approximately 755,000 records in the Terrorist Screening Center's watch list as of May 2007 is greater than the total number of individuals on the list. If an individual has one or more aliases, the database will contain multiple records for the same individual. The Terrorist Screening Center did not have data on the number of unique individuals on the watch list.

¹¹The approximately 53,000 total encounters with individuals who were positively matched to the watch list constitute screening results from all agencies that use the list, not just the specific screening agencies and processes we reviewed.

respective agency's mission, (2) may not be possible due to the requirements of computer programs used to check individuals against watch list records, or (3) may not be operationally feasible.¹² Rather, each day, the center exports applicable records from the consolidated watch list to federal government databases that agencies use to screen individuals for mission-related concerns. For example, the database that U.S. Customs and Border Protection uses to check incoming travelers for immigration violations, criminal histories, and other matters contained the highest percentage of watch list records as of May 2007. This is because its mission is to screen all travelers, including U.S. citizens, entering the United States at ports of entry. The database that the Department of State uses to screen applicants for visas contained the second highest percentage of all watch list records. This database does not include U.S. citizens and lawful permanent residents because these individuals would not apply for U.S. visas. Also, the FBI database that state and local law enforcement agencies use for screening contained the third highest percentage of the records. According to the FBI, the remaining records were not included in this database primarily because they did not contain sufficient identifying information, which is required to minimize instances of individuals being misidentified as being subjects of watch list records. Further, the No Fly and Selectee lists disseminated by the Transportation Security Administration to airlines for use in prescreening passengers contained the lowest percentage of watch list records. The lists did not contain the remaining records either because they (1) did not meet criteria for the No Fly or Selectee lists established by the Homeland Security Council or (2) did not contain sufficient identifying information, which is required to help airlines verify identities and minimize instances of individuals being falsely identified as being on the No Fly or Selectee lists. According to the Department of Homeland Security, increasing the number of records used to prescreen passengers would expand the number of misidentifications to unjustifiable proportions without a measurable increase in security.

Department of Homeland Security component agencies are separately taking steps to address certain aspects of screening processes that occasionally have resulted in subjects of watch list records passing undetected through screening processes. For example, U.S. Customs and Border Protection has encountered situations where it identified the

¹²Also, some watch list records can be excluded from screening agency databases for other reasons, such as the records were pending deletion or quality assurance resolution.

subject of a watch list record after the individual had been processed at a port of entry and admitted into the United States. The agency did not maintain aggregated, national data on the number of these incidents or the specific causes, but noted several possible reasons. In response to our inquiries, U.S. Customs and Border Protection created an interdisciplinary working group within the agency to study the causes of this vulnerability. The working group held its first meeting in early 2007 and subsequently has begun to implement corrective actions. U.S. Citizenship and Immigration Services—the agency responsible for screening persons who apply for U.S. citizenship or immigration benefits—has also acknowledged areas that need improvement in the processes used to detect subjects of watch list records. According to agency representatives, each instance of an individual on the watch list getting through agency screening is reviewed on a case-by-case basis to determine the cause, with appropriate follow-up and corrective action taken, if needed. The agency is working with the Terrorist Screening Center to enhance screening effectiveness. Further, Transportation Security Administration data show that in the past, a number of individuals who were on the government’s No Fly list passed undetected through airlines’ prescreening of passengers and flew on international flights bound to or from the United States. The individuals were subsequently identified in-flight by U.S. Customs and Border Protection, which used information that was collected from air carriers’ passenger manifests to check passengers against watch list records to help the agency prepare for the passengers’ arrival in the United States. However, the potential onboard security threats posed by the undetected individuals required an immediate counterterrorism response, which in some instances resulted in diverting the aircraft to a new location.¹³ According to the Transportation Security Administration, such incidents were subsequently investigated and, if needed, corrective action was taken with the respective air carrier. In addition, U.S. Customs and Border Protection has issued a final rule that should better position the government to identify individuals on the No Fly list before an international flight is airborne.¹⁴ For domestic flights within the United States, there is no second screening opportunity—like the one U.S.

¹³In July 2007, we issued a report that examined federal coordination for responding to in-flight security threats. See GAO, *Aviation Security: Federal Coordination for Responding to In-flight Security Threats Has Matured, but Procedures Can Be Strengthened*, [GAO-07-891R](#) (Washington, D.C.: July 31, 2007).

¹⁴See 72 Fed. Reg. 48,320 (Aug. 23, 2007). The provisions of the final rule take effect on February 19, 2008.

Customs and Border Protection conducts for international flights—and, consequently, the Transportation Security Administration generally does not know whether individuals on the No Fly list have passed undetected through airlines’ prescreening. Because such instances have occurred on international flights, it is possible they have also occurred but have not been detected on domestic flights. The government plans to take over from air carriers the function of prescreening passengers prior to departure against watch list records for both international and domestic flights.

Although the federal government has made progress in using the consolidated watch list for screening purposes, additional opportunities exist for using the list. Internationally, the Department of State has made progress in making bilateral arrangements to share terrorist screening information with certain foreign governments. The department had two such arrangements in place before September 11, 2001. More recently, the department has made four new arrangements and is in negotiations with several other countries. Also, the Department of Homeland Security has made progress in using watch list records to screen employees in some critical infrastructure components of the private sector, including certain individuals who have access to vital areas of nuclear power plants, work in airports, or transport hazardous materials. However, many critical infrastructure components are not using watch list records. The Department of Homeland Security has not, consistent with Homeland Security Presidential Directive 6, finalized guidelines to support private sector screening processes that have a substantial bearing on homeland security—such as screening certain employees against the list—which is an important action to ensure that watch list records are used by the private sector where appropriate. Further, federal departments and agencies have not identified all appropriate opportunities for which terrorist-related screening should be applied, in accordance with presidential directives.

A primary reason why screening opportunities remain untapped is because the government lacks an up-to-date strategy and implementation plan—supported by a clearly defined leadership or governance structure—for enhancing the effectiveness of terrorist-related screening, consistent with presidential directive. Currently, numerous existing entities have roles in watch list-related activities, including the Terrorist Screening Center, screening agencies, law enforcement agencies, and the intelligence community. However, clear lines of responsibility and authority are important to provide monitoring and analysis of watch list-related screening efforts governmentwide, promote information sharing, and

address interagency issues. Without an up-to-date strategy and implementation plan and clearly defined leadership, it is difficult to establish governmentwide priorities for screening, assess progress toward intended outcomes, ensure that any needed changes are implemented, and respond to issues that hinder effectiveness, such as the potential vulnerabilities discussed in this report.

To promote more comprehensive and coordinated use of terrorist screening information to detect, identify, track, and interdict known or appropriately suspected terrorists, the restricted version of this report makes several recommendations to the heads of relevant departments and agencies intended to help (1) mitigate security vulnerabilities in terrorist watch list screening processes and (2) optimize the use and effectiveness of the watch list as a counterterrorism tool, including development of an up-to-date strategy and implementation plan for using terrorist-related information. Also, to help ensure that governmentwide terrorist-related screening efforts are effectively coordinated, we recommended in the restricted version of this report that the Assistant to the President for Homeland Security and Counterterrorism ensure that the leadership or governance structure proposed by the implementation plan identifies clear lines of responsibility and authority.

The Department of Homeland Security and the FBI, which provided the Department of Justice's comments on a draft of the restricted version of this report, generally agreed with our findings and recommendations. The Department of Homeland Security noted, among other things, that it had already begun work to correct issues identified in the report, including ongoing efforts with other federal entities to ensure that potential watch list vulnerabilities are identified and addressed and that watch list records and screening programs are appropriate. The FBI's comments focused primarily on two issues. First, the FBI noted that the extent of vulnerabilities in current screening processes that arise when the FBI database that state and local law enforcement agencies use for screening does not contain certain watch list records has been determined to be low or nonexistent. However, the FBI's assessment was based on operational concerns and did not specifically address the extent to which security risks are raised by not using these records. Second, the FBI commented that it believes the Terrorist Screening Center's governance board is the appropriate forum for obtaining a commitment from all of the entities involved in the watch listing process. However, as discussed in this report, while the governance board could be suited to assume more of a leadership role, its current authority is limited to issues specific to the Terrorist Screening Center, and it would need additional authority to

provide effective coordination of terrorist-related screening activities and interagency issues governmentwide. The Homeland Security Council was provided a draft of the restricted version of this report but did not provide comments. The Office of the Director of National Intelligence, the Department of State, and the Social Security Administration provided technical comments only on a draft of the restricted version of this report, which we incorporated where appropriate.

Background

In April 2003, we reported that watch lists were maintained by numerous federal agencies and that the agencies did not have a consistent and uniform approach to sharing information on individuals with possible links to terrorism.¹⁵ Our report recommended that the Secretary of the Department of Homeland Security (DHS), in collaboration with the heads of departments and agencies that have and use watch lists, lead an effort to consolidate and standardize the federal government's watch list structures and policies. Subsequently, pursuant to Homeland Security Presidential Directive 6 (HSPD-6), dated September 16, 2003, the Attorney General established the Terrorist Screening Center (TSC) to consolidate the government's approach to terrorism screening and provide for the appropriate and lawful use of terrorist information in screening processes.¹⁶ TSC's consolidated watch list is the U.S. government's master repository for all known or appropriately suspected international and domestic terrorist records used for watch list-related screening. TSC records contain sensitive but unclassified information on terrorist identities—such as name and date of birth—that can be shared with screening agencies, whereas the classified derogatory information that supports the watch list records is maintained in other law enforcement and intelligence agency databases. Records for inclusion on the consolidated watch list are nominated to TSC from the following two sources:

- Identifying information on individuals with ties to international terrorism is provided to TSC through the National Counterterrorism Center (NCTC), which is managed by the Office of the Director of National Intelligence.

¹⁵GAO, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*, [GAO-03-322](#) (Washington, D.C.: Apr. 15, 2003).

¹⁶The full text of HSPD-6 is reprinted in appendix II.

-
- Identifying information on individuals with ties to purely domestic terrorism is provided to TSC by the FBI.¹⁷

HSPD-6 required the Attorney General—in coordination with the Secretary of State, the Secretary of Homeland Security, and the Director of Central Intelligence—to implement appropriate procedures and safeguards with respect to all terrorist information related to U.S. persons (i.e., U.S. citizens and lawful permanent residents) that is provided to NCTC (formerly the Terrorist Threat Integration Center). According to TSC, agencies within the intelligence community that collect and maintain terrorist information and nominate individuals for inclusion on TSC’s consolidated watch list are to do so in accordance with Executive Order 12333.¹⁸ With respect to U.S. persons, this order addresses the nature or type of information that may be collected and the allowable methods for collecting such information. It provides that agencies within the intelligence community are authorized to collect, retain, or disseminate information concerning U.S. persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General, consistent with the authorities set out earlier in the order. The order further provides that agencies within the intelligence community are to use the least intrusive collection techniques feasible when such collection is conducted within the United States or when directed against U.S. persons abroad. Also, according to TSC officials, the center requires annual training for all personnel concerning the Privacy Act of 1974 to ensure that information collected on U.S. persons is handled in accordance with applicable law.¹⁹

To facilitate operational or mission-related screening, TSC sends applicable records from its terrorist watch list to screening agency systems for use in efforts to deter or detect the movements of known or suspected terrorists. For instance, applicable TSC records are provided to the Transportation Security Administration (TSA) for use by airlines in

¹⁷The FBI also has information on individuals with possible international terrorism ties, which it provides to NCTC.

¹⁸Exec. Order No. 12,333 (Dec. 4, 1981).

¹⁹See 5 U.S.C. § 552a.

prescreening passengers;²⁰ to a U.S. Customs and Border Protection (CBP) system for use in screening travelers entering the United States;²¹ to a Department of State system for use in screening visa applicants;²² and to an FBI system for use by state and local law enforcement agencies pursuant to arrests, detentions, and other criminal justice purposes.

When an individual makes an airline reservation, arrives at a U.S. port of entry, or applies for a U.S. visa, or is stopped by state or local police within the United States, the frontline screening agency or airline conducts a name-based search of the individual against applicable terrorist watch list records. In general, when the computerized name-matching system of an airline or screening agency generates a “hit” (a potential name match) against a watch list record, the airline or agency is to review each potential match. Any obvious mismatches (negative matches) are to be resolved by the airline or agency, if possible, as discussed in our September 2006 report.²³ However, clearly positive or exact matches and matches that are inconclusive (uncertain or difficult-to-verify) generally are to be referred to the applicable screening agency’s intelligence or operations center and TSC for closer examination. Specifically, airlines are to contact TSA’s Office of Intelligence; CBP officers at U.S. ports of entry are to contact

²⁰TSA is developing a new advanced passenger prescreening program, known as Secure Flight. Under the program, the agency plans to take over from aircraft operators the responsibility for comparing identifying information on airline passengers against watch list records. See 72 Fed. Reg. 48,356 (Aug. 23, 2007). The agency expects that Secure Flight will improve passenger prescreening as compared with the current airline-operated process. In June 2006, we reported that TSA still faces significant challenges in developing and implementing the Secure Flight program. See GAO, *Aviation Security: Management Challenges Remain for the Transportation Security Administration’s Secure Flight Program*, [GAO-06-864T](#) (Washington, D.C.: June 14, 2006).

²¹CBP’s system is also used to assist law enforcement and other personnel at approximately 20 other federal agencies, including the following: U.S. Immigration and Customs Enforcement; U.S. Citizenship and Immigration Services; the FBI; the Drug Enforcement Administration; the Bureau of Alcohol, Tobacco, Firearms and Explosives; the Internal Revenue Service; the U.S. Coast Guard; the Federal Aviation Administration; and the U.S. Secret Service.

²²The Department of State also uses watch list records in screening passport applicants, which we did not cover during this review.

²³Terrorist watch list-related screening can cause travel delays and other inconveniences, which may be inevitable consequences of enhanced homeland security. Nonetheless, as we reported in September 2006, it is important for TSC and screening agencies to provide effective redress for individuals who are inadvertently and adversely affected by watch list-related screening. See GAO, *Terrorist Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public*, [GAO-06-1031](#) (Washington, D.C.: Sept. 29, 2006).

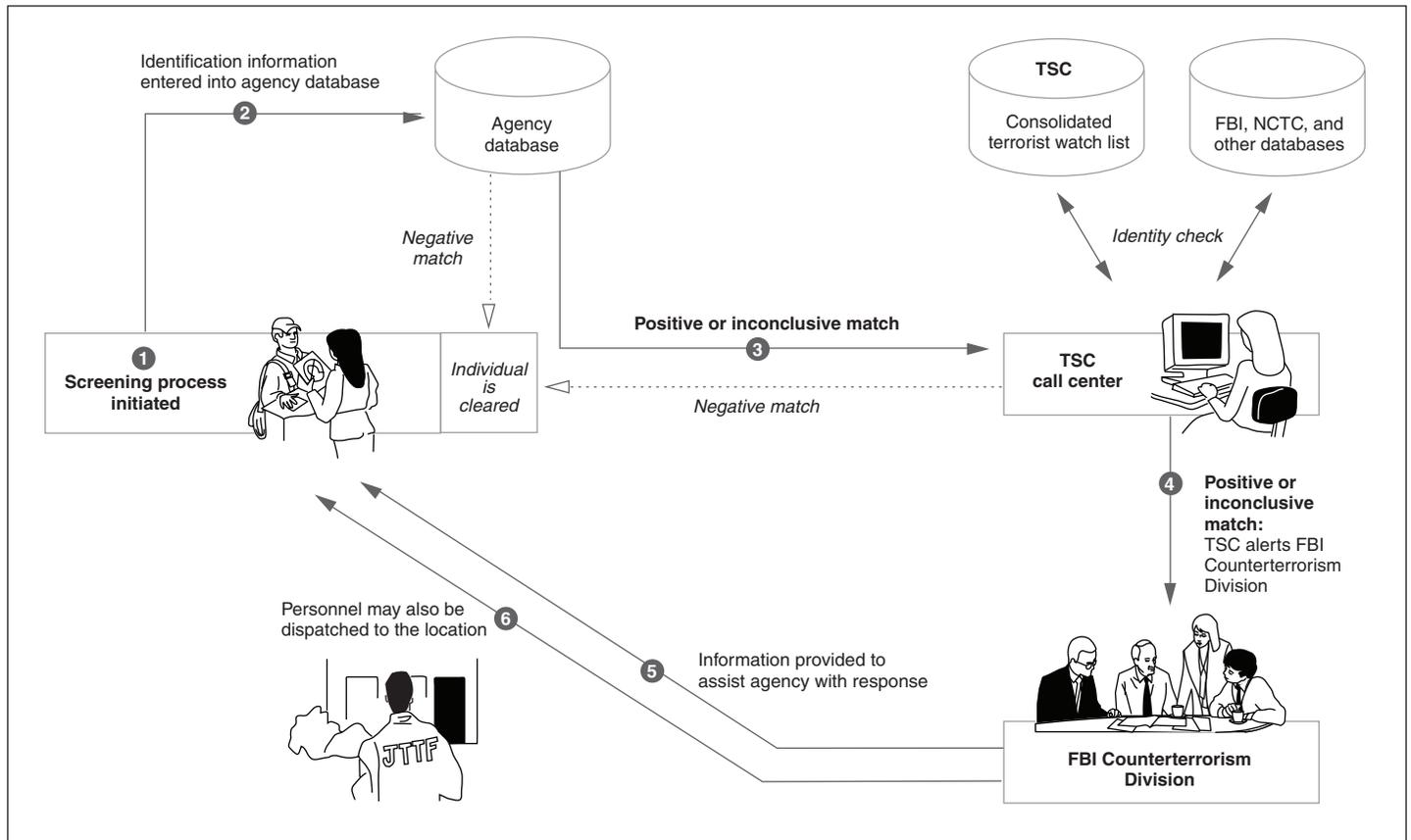
CBP's National Targeting Center; and Department of State consular officers who process visa applications are to submit a request for a security advisory opinion to Department of State headquarters.²⁴ The intelligence or operations center is to refer exact matches and inconclusive matches to TSC. State and local law enforcement officials generally are to refer exact matches and inconclusive matches directly to TSC. In turn, TSC is to check its databases and other sources—including classified databases maintained by NCTC and the FBI—and confirm whether the individual is a positive, negative, or inconclusive match to the watch list record.

TSC is to refer positive and inconclusive matches to the FBI's Counterterrorism Division to provide an opportunity for a counterterrorism response. Deciding what law enforcement or screening agency action to take, if any, can involve collaboration among the frontline screening agency, NCTC or other intelligence community members, and the FBI or other investigative agencies. If the encounter arises in the context of an application for a visa or admission into the United States, the screening agency's adjudicating official determines whether the circumstances trigger a statutory basis for inadmissibility. Generally, NCTC and the FBI are involved because they maintain the underlying derogatory information that supports terrorist watch list records, which is needed to help determine the appropriate counterterrorism response. If necessary, a member of an FBI Joint Terrorism Task Force can respond in person to interview and obtain additional information about the person encountered.²⁵ In other cases, the FBI will rely on the screening agency and other law enforcement agencies—such as U.S. Immigration and Customs Enforcement—to respond and collect information. Figure 1 presents a general overview of the process used to resolve encounters with individuals on the terrorist watch list.

²⁴Regarding the process for screening nonimmigrant visa applicants against applicable watch list records, the Department of State emphasized that for any positive or inconclusive match, consular officers are required to ask Department of State headquarters to initiate a process of requesting that TSC and other relevant agencies check their respective databases or systems for the existence of any investigative or intelligence information regarding the individual and pass the results back to the department for use in recommending a course of action to the consular officer.

²⁵Joint Terrorism Task Forces are teams of state and local law enforcement officials, FBI agents, and other federal agents and personnel whose mission is to investigate and prevent acts of terrorism. There is a Joint Terrorism Task Force in each of the FBI's 56 main field offices, and additional task forces are located in smaller FBI offices.

Figure 1: General Overview of the Process Used to Resolve Encounters with Individuals on the Terrorist Watch List



Source: GAO analysis of TSC information.

To build upon and provide additional guidance related to HSPD-6, in August 2004, the President signed Homeland Security Presidential Directive 11 (HSPD-11).²⁶ Among other things, this directive required the Secretary of Homeland Security—in coordination with the heads of appropriate federal departments and agencies—to submit two reports to the President (through the Assistant to the President for Homeland Security) related to the government’s approach to terrorist-related

²⁶The full text of HSPD-11 is reprinted in appendix III.

screening.²⁷ The first report was to outline a strategy to enhance the effectiveness of terrorist-related screening activities by developing comprehensive and coordinated procedures and capabilities. The second report was to provide a prioritized investment and implementation plan for detecting and interdicting suspected terrorists and terrorist activities. Specifically, the plan was to describe the “scope, governance, principles, outcomes, milestones, training objectives, metrics, costs, and schedule of activities” to implement the U.S. government’s terrorism-related screening policies. According to DHS officials, the department submitted the required strategy and the investment and implementation plan to the President in November 2004. Additional information on the status of the strategy and implementation plan is presented later in this report.

In Assessing Individuals for Inclusion on TSC’s Watch List, Officials Rely upon Standards of Reasonableness That Inherently Involve Some Subjectivity

NCTC and FBI officials rely upon standards of reasonableness in determining which individuals are appropriate for inclusion on TSC’s watch list, but determining whether individuals meet these minimum standards can involve some level of subjectivity.²⁸ In accordance with HSPD-6, TSC’s watch list is to contain information about individuals “known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism.” In implementing this directive, NCTC and the FBI strive to ensure that individuals who are reasonably suspected of having possible links to terrorism—in addition to individuals with known links—are nominated for inclusion on the watch list. Thus, as TSC adds nominated records to its watch list, the list may include individuals with possible ties to terrorism, establishing a broad spectrum of individuals that meet the “known or appropriately suspected” standard specified in HSPD-6. As such, inclusion on the list does not automatically cause an alien to be, for example, denied a visa or deemed inadmissible to enter the United States when the person is identified by a screening agency. Rather, in these cases, screening agency and law enforcement personnel may use the encounter with the

²⁷In HSPD-11, the term “terrorist-related screening” is defined as the collection, analysis, dissemination, and use of information related to people, cargo, conveyances, and other entities and objects that pose a threat to homeland security. Terrorist-related screening also includes risk assessment, inspection, and credentialing.

²⁸In general, and in this context, a standard of reasonableness can be described as a government agent’s particularized and objective basis for suspecting an individual of engaging in terrorist-related activities, considering the totality of circumstances known to the government agent at that time. See, e.g., *United States v. Price*, 184 F.3d 637, 640-41 (7th Cir. 1999); *Terry v. Ohio*, 392 U.S. 1, 30 (1968).

individual as an opportunity to collect information for assessing the potential threat the person poses, tracking the person's movements or activities, and determining what actions to take, if any.²⁹

The National Counterterrorism Center Uses a “Reasonable Suspicion” Standard in Determining Which Individuals Are Appropriate for Inclusion on the Watch List

NCTC receives international terrorist-related information from executive branch departments and agencies—such as the Department of State, the Central Intelligence Agency, and the FBI—and enters this information into its terrorist database.³⁰ On a formal basis, Department of State embassies around the world—in collaboration with applicable federal agencies involved in security, law enforcement, and intelligence activities—are expected to participate in the “Visas Viper” terrorist reporting program. This congressionally mandated program is primarily administered through a Visas Viper Committee at each overseas post.³¹ The committee is to meet at least monthly to share information on known or suspected terrorists and determine whether such information should be sent to NCTC for inclusion in its terrorist database.³² NCTC's database, known as the Terrorist Identities Datamart Environment, contains highly classified information and serves as the U.S. government's central classified database with information on known or suspected international terrorists. According to NCTC's fact sheet on the Terrorist Identities Datamart Environment, examples of conduct that will warrant an entry into NCTC's database includes persons who

²⁹The purpose of certain screening processes is to address a specific security concern, such as airlines' prescreening of passengers wherein the use of watch list records is primarily intended to enhance aviation security. However, such screening may also support government efforts to track a person's movements or activities.

³⁰According to NCTC data, other sources of information on known or suspected international terrorists include the National Security Agency; the military, including the Department of Defense, the Defense Intelligence Agency, the Air Force Office of Special Investigations, and the U.S. Navy; DHS, including U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection, and the National Targeting Center; other federal departments and agencies, including the Department of Justice, the Department of the Treasury, and the Federal Aviation Administration; foreign sources; and the press, including the Foreign Broadcast Information System, Reuters, and Associated Press International.

³¹See 8 U.S.C. § 1733.

³²See GAO, *Border Security: Strengthened Visa Process Would Benefit from Improvements in Staffing and Information Sharing*, [GAO-05-859](#) (Washington, D.C.: Sept. 13, 2005).

-
- commit 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 benefit, false documentation or identification, weapons, explosives, or training; or
 - are members of or represent a foreign terrorist organization.³³

If NCTC determines that an individual meets the “known or appropriately suspected” standard of HSPD-6, NCTC is to extract sensitive but unclassified information on the individual’s identity from its classified database—such as name and date of birth—and send forward a record to TSC for inclusion on the watch list. According to NCTC procedures, NCTC analysts are to review all information involving international terrorists using a “reasonable suspicion” standard to determine whether an individual is appropriate for nomination to TSC for inclusion on the watch list. NCTC defines reasonable suspicion as information—both facts, as well as rational inferences from those facts and the experience of the reviewer—that is sufficient to cause an ordinarily prudent person to believe that the individual under review may be a known or appropriately suspected terrorist. According to NCTC, this information can include past conduct, current actions, and credible intelligence concerning future conduct. In making this determination, NCTC generally relies upon the originating agency’s designation that there is reasonable suspicion to believe a person is engaged in terrorist or terrorist-related activities as being presumptively valid. For example, NCTC will rely on the FBI’s designation of an individual as a known or suspected international terrorist unless NCTC has specific and credible information that such a designation is not appropriate.

Also, NCTC officials noted that an individual is to remain on the watch list until the respective department or agency that provided the terrorist-

³³In general, these types of conduct are related to provisions in the Immigration and Nationality Act that establish grounds for alien admissibility on terrorism-related grounds. See 8 U.S.C. § 1182(a)(3)(B) (codifying section 212(a)(3)(B) of the Immigration and Nationality Act, as amended).

related information that supports a nomination determines the individual should be removed from the list. According to TSC, if the FBI conducts a threat assessment on an individual that reveals no nexus to international terrorism, then NCTC will initiate the process for deleting the record from its database and the watch list. If NCTC receives information that it determines is insufficient to nominate an individual to TSC for inclusion on the watch list, the available information may remain in the NCTC database until additional information is obtained to warrant nomination to TSC or be deleted from the NCTC database.

Individuals Who Are Subjects of FBI Counterterrorism Investigations Are Generally Nominated to the Watch List

In general, individuals who are subjects of ongoing FBI counterterrorism investigations are nominated to TSC for inclusion on the watch list, including persons who are being preliminarily investigated to determine if they have links to terrorism. If an investigation does not establish a terrorism link, the FBI generally is to close the investigation and request that TSC remove the person from the watch list.

In determining whether to open an investigation, the FBI uses guidelines established by the Attorney General. These guidelines contain specific standards for opening investigations. According to FBI officials, there must be a “reasonable indication” of involvement in terrorism before opening an investigation. The FBI noted, for example, that it is not sufficient to open an investigation based solely on a neighbor’s complaint or an anonymous tip or phone call. In such cases, however, the FBI could use techniques short of opening an investigation to assess the potential threat the person poses, which would not result in adding the individual to the watch list at that time.

The FBI has established formal review and approval processes for nominating individuals for inclusion on the watch list. In general, FBI case agents are to send nominations to a unit at FBI headquarters for review and approval. If approved, information on domestic terrorists is sent to TSC for inclusion on the watch list. For approved international terrorist nominations, the FBI sends the information to NCTC, who then sends forward the nomination to TSC.

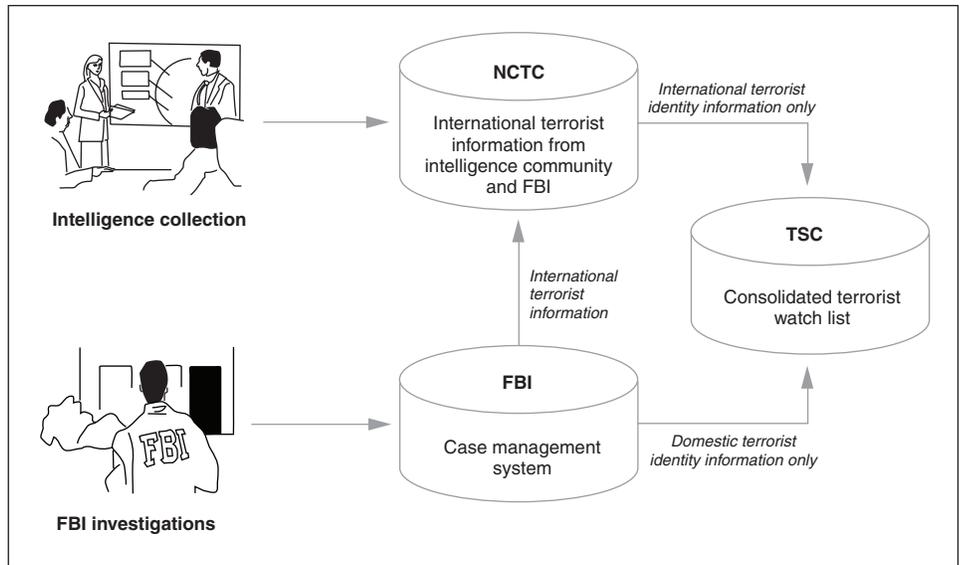
TSC's Watch List Is the Master Repository for Watch List Records

For each nomination, NCTC and the FBI provide TSC with biographic or other identifying data, such as name and date of birth. This identifying information on known or suspected terrorists is deemed sensitive but unclassified by the intelligence and law enforcement communities.³⁴ Then, TSC is to review the identifying information and the underlying derogatory information—by directly accessing databases maintained by NCTC, the FBI, and other agencies—to validate the requirements for including the nomination on the watch list.³⁵ On the basis of the results of its review, TSC is to either input the nomination into the watch list—which is the U.S. government's master repository for all known or appropriately suspected international and domestic terrorist records that are used for watch list-related screening—or reject the nomination and send it back to NCTC or the FBI for further investigation. TSC relies predominantly on the nominating agency to determine whether or not an individual is a known or appropriately suspected terrorist. According to TSC, on the basis of its review of relevant identifying and derogatory information, the center rejects approximately 1 percent of all nominations. Figure 2 presents a general overview of the process used to nominate individuals for inclusion on TSC's watch list.

³⁴TSC does not receive or maintain the derogatory information that supports watch list records. Rather, NCTC, the FBI, and other agencies that originate nominations maintain this information.

³⁵In March 2006, TSC implemented a formal process to review each nomination. Before March 2006, TSC generally accepted nominations without reviewing the supporting derogatory information, but it had processes in place to review the identifying information.

Figure 2: General Overview of the Process Used to Nominate Individuals for Inclusion on TSC's Watch List

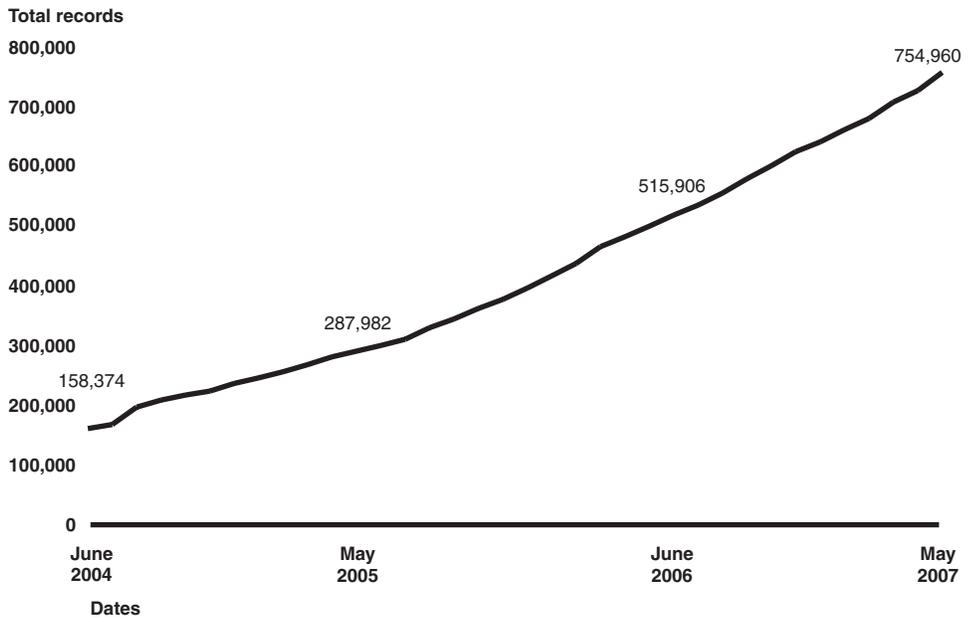


Source: GAO analysis of TSC information.

TSC's watch list of individuals with known or appropriately suspected links to terrorism has increased from 158,374 records in June 2004 to 754,960 records in May 2007 (see fig. 3).³⁶ It is important to note that the total number of records on TSC's watch list does not represent the total number of individuals on the watch list. Rather, if an individual has one or more known aliases, the watch list will contain multiple records for the same individual. For example, if an individual on the watch list has 50 known aliases, there could be 50 distinct records related to that individual in the watch list.

³⁶TSC completed its initial consolidation of terrorist watch list records in March 2004 but did not specifically track the number of records in the database until June 2004.

Figure 3: Increase in Terrorist Watch List Records, June 2004 through May 2007



Source: GAO analysis of TSC data.

TSC's database is updated daily with new nominations, modifications to existing records, and deletions. According to TSC data, as of May 2007, a high percentage of watch list records were international terrorist records nominated through NCTC, and a small percentage were domestic terrorist records nominated through the FBI. TSC data also show that more than 100,000 records have been removed from the watch list since TSC's inception. As discussed later in this report, agencies that conduct terrorism screening do not check against all records in the watch list. Rather, TSC exports applicable records to federal government databases used by agencies that conduct terrorism screening based on the screening agency's mission responsibilities and other factors.

Agencies Have Had Approximately 53,000 Encounters with Individuals on the Watch List, and Outcomes Indicate the List Has Helped to Combat Terrorism

For the 42-month period of December 2003 (when TSC began operations) through May 2007, screening and law enforcement agencies encountered individuals who were positively matched to watch list records 53,218 times, according to our analysis of TSC data. These encounters include many individuals who were positively matched to watch list records multiple times. Agencies took a range of actions, such as arresting individuals, denying other individuals entry into the United States, and most commonly, releasing the individuals following questioning and information gathering. Our analysis of data on the outcomes of these encounters and interviews with screening agency, law enforcement, and intelligence community officials indicate that the watch list has enhanced the U.S. government's counterterrorism efforts by (1) helping frontline screening agencies obtain information to determine the level of threat a person poses and the appropriate action to take, if any, and (2) providing the opportunity to collect and share information on known or appropriately suspected terrorists with law enforcement agencies and the intelligence community.

The Number of Positive Matches to the Watch List Has Increased Each Year, and Many Individuals Have Been Encountered Multiple Times

A breakdown of encounters with positive matches to the terrorist watch list shows that the number of matches has increased each year—from 4,876 during the first 10-month period of TSC's operations (December 2003 through September 2004) to 14,938 during fiscal year 2005, to 19,887 during fiscal year 2006. This increase can be attributed partly to the growth in the number of records in the consolidated terrorist watch list and partly to the increase in the number of agencies that use the list for screening purposes. Since its inception, TSC has worked to educate federal departments and agencies, state and local law enforcement, and foreign governments about appropriate screening opportunities. Our analysis of TSC data also indicates that many individuals who were positively matched to the terrorist watch list were encountered multiple times. For example, a truck driver who regularly crossed the U.S.-Canada border or an individual who frequently took international flights could each account for multiple encounters.

Further, TSC data show that the highest percentage of encounters with individuals who were positively matched to the watch list involved screening within the United States by a state or local law enforcement agency, U.S. government investigative agency, or other governmental entity. Examples of these encounters include screening by police departments, correctional facilities, FBI agents, and courts. The next highest percentage of encounters with positive matches to the watch list involved border-related encounters, such as passengers on airline flights

inbound from outside the United States or individuals screened at land ports of entry.³⁷ Examples include (1) a passenger flying from London (Heathrow), England, to New York (JFK), New York, and (2) a person attempting to cross the border from Canada into the United States at the Rainbow Bridge port of entry in Niagara Falls, New York. The smallest percentage of encounters with positive matches occurred outside of the United States.

State and local law enforcement agencies historically have had access to an FBI system that contains watch list records produced by the FBI. However, pursuant to HSPD-6 (Sept. 16, 2003), state and local law enforcement agencies were, for the first time, given access to watch list records produced by the intelligence community, which are also included in the FBI system. This access has enabled state and local agencies to better assist the U.S. government's efforts to track and collect information on known or appropriately suspected terrorists. These agencies accounted for a significant percentage of the total encounters with positive matches to the watch list that occurred within the United States.

The Watch List Has Helped Screening Agencies Assess the Potential Threat a Person Poses and Take a Wide Range of Counterterrorism Responses

The watch list has enhanced the U.S. government's counterterrorism efforts by allowing federal, state, and local screening and law enforcement officials to obtain information to help them make better-informed decisions during encounters regarding the level of threat a person poses and the appropriate response to take, if any. The specific outcomes of encounters with individuals on the watch list are based on the government's overall assessment of the intelligence and investigative information that supports the watch list record and any additional information that may be obtained during the encounter. Our analysis of data of the outcomes of encounters revealed that agencies took a range of actions, such as arresting individuals, denying others entry into the United States, and most commonly, releasing the individuals following questioning and information gathering. The following provides additional information on arrests, as well as the outcomes of encounters involving

³⁷Passengers on airline flights coming into the United States are generally to be screened against applicable records in the watch list two times—first, at TSA's direction, by air carriers against the No Fly and Selectee lists prior to boarding and then by CBP against watch list records in its database before being admitted into the United States. To avoid double counting, TSC generally reports these instances as one encounter, typically as CBP border-crossing encounters. In addition, prior to flight, an initial watch list screening is to occur in cases where a visa is required, which TSC reports as Department of State encounters.

the Department of State, TSA, CBP, and state or local law enforcement, respectively.

- TSC data show that agencies reported arresting many subjects of watch list records for various reasons, such as the individual having an outstanding arrest warrant or the individual's behavior or actions during the encounter. TSC data also indicated that some of the arrests were based on terrorism grounds.
- TSC data show that when visa applicants were positively matched to terrorist watch list records, the outcomes included visas denied, visas issued (because the consular officer did not find any statutory basis for inadmissibility), and visa ineligibility waived.³⁸
- TSA data show that when airline passengers were positively matched to the No Fly or Selectee lists, the vast majority of matches were to the Selectee list. Other outcomes included individuals matched to the No Fly list and denied boarding (did not fly) and individuals matched to the No Fly list after the aircraft was in-flight, which required an immediate counterterrorism response. Additional information on individuals on the No Fly list passing undetected through airline prescreening and being identified in-flight is presented later in this report.
- CBP data show that a number of nonimmigrant aliens encountered at U.S. ports of entry were positively matched to terrorist watch list records. For many of the encounters, CBP determined there was sufficient derogatory information related to watch list records to preclude admission under terrorism grounds. However, for most of the encounters, CBP determined that there was not sufficient derogatory information related to the records to preclude admission.
- TSC data show that state or local law enforcement officials have encountered individuals who were positively matched to terrorist watch list records thousands of times. Although data on the actual outcomes of these encounters were not available, the vast majority involved watch list records that indicated that the individuals were

³⁸In this context, ineligibility waived refers to individuals who were ineligible for a visa based on terrorism grounds, but DHS approved a waiver for a one-time visit or multiple entries into the United States. In general, waivers are approved when the U.S. government has an interest in allowing the individual to enter the United States, such as an individual on the terrorist watch list who is invited to participate in peace talks under U.S. auspices.

released, unless there were reasons other than terrorism-related grounds for arresting or detaining the individual.

Appendix IV presents more details on the outcomes of screening agency encounters with individuals on the terrorist watch list.

The Watch List Has Helped Support Law Enforcement Investigations and the Intelligence Community by Tracking the Movements of Known or Appropriately Suspected Terrorists and Collecting Information about Them

According to federal officials, encounters with individuals who were positively matched to the watch list assisted government efforts in tracking the respective person's movements or activities and provided the opportunity to collect additional information about the individual that was shared with agents conducting counterterrorism investigations and with the intelligence community for use in analyzing threats. Such coordinated collection of information for use in investigations and threat analyses is one of the stated policy objectives for the watch list. Most of the individuals encountered were questioned and released because the intelligence and investigative information on these persons that supported the watch list records and the information obtained during the encounter did not support taking further actions, such as denying an individual entry into the United States.

Specifically, as discussed previously, for most Department of State, TSA (via air carriers), CBP, and state and local encounters with individuals who were positively matched to the terrorist watch list, the counterterrorism response consisted of questioning the individuals and gathering information. That is, the encounters provided screening agency and law enforcement personnel the opportunity to conduct in-depth questioning and inspect travel documents and belongings to collect information for use in supporting investigations and assessing threats. TSC plays a central role in the real-time sharing of this information, creating a bridge among screening agencies, the law enforcement community, and the intelligence community. For example, in addition to facilitating interagency communication and coordination during encounters, TSC creates a daily report of encounters involving positive matches to the terrorist watch list. This report contains a summary of all positive encounters for the prior day. TSC summarizes the type of encounter, what occurred, and what action was taken. The report notes the person's affiliation with any groups and provides a summary of derogatory information available on the individual. Overview maps depicting the encounters and locations are also included in the report. The daily reports are distributed to numerous federal entities, as shown in table 1.

Table 1: Distribution List for TSC’s Daily Summary of Positive Matches

White House	Homeland Security Council
FBI	Director
	Counterterrorism Division
	National Joint Terrorism Task Force
	Office of Intelligence
Departments	Department of Homeland Security (Secretary and other units)
	Department of State
Agencies	Federal Air Marshal Service
	Transportation Security Administration (Administrator and intelligence staff)
	U.S. Immigration and Customs Enforcement
	U.S. Customs and Border Protection
	United States Secret Service
Intelligence community	Central Intelligence Agency
	Defense Intelligence Agency
	Department of Defense Counterintelligence Field Activity
	FBI Field Intelligence Group members ^a
	National Counterterrorism Center
	National Security Agency
	Office of the Director of National Intelligence

Source: GAO summary of TSC information.

^aAccording to the FBI, Field Intelligence Groups consist of FBI intelligence analysts, special agents, language analysts, and surveillance specialists who take raw information from local cases and make big-picture sense out of it; fill gaps in national cases with local information; and share their findings, assessments, and reports with other Field Intelligence Groups across the country and with other law enforcement and intelligence agencies. There is one Field Intelligence Group in each of the FBI’s 56 field offices.

According to federal law enforcement officials, the information collected during encounters with individuals on the terrorist watch list helps to develop cases by, among other means, tracking the movement of known or appropriately suspected terrorists and determining relationships among people, activities, and events. According to NCTC officials, information obtained from encounters is added to NCTC’s Terrorist Identities Datamart Environment database, which serves as the U.S. government’s central classified database on known or suspected international

terrorists.³⁹ This information can be electronically accessed by approximately 5,000 U.S. counterterrorism personnel around the world.

TSC Exports Applicable Watch List Records to Screening Agency Databases, Depending on Agency Mission and Technical Capacity; but Some Technical Requirements May Present Security Vulnerabilities

Each day, TSC exports applicable records from the watch list—containing biographic or other identifying data, such as name and date of birth—to federal government databases used by agencies that conduct terrorism screening. Specifically, applicable watch list records are exported to the following federal agency databases, which are described later in this report:

- DHS’s Interagency Border Inspection System.
- The Department of State’s Consular Lookout and Support System.⁴⁰
- The FBI’s Violent Gang and Terrorist Organization File.
- TSA’s No Fly and Selectee lists.

The applicable records that TSC exports to each of these databases vary based on the screening agency’s mission responsibilities, the technical capabilities of the agency’s computer system, and operational considerations.⁴¹ For example, records on U.S. citizens and lawful permanent residents are not exported to the Department of State’s system used to screen visa applicants for immigration violations, criminal histories, and other matters, because these individuals would not apply for a U.S. visa. Also, to facilitate the automated process of checking an individual against watch list records, all of these databases require certain minimum biographic or identifying data in order to accept records from TSC’s consolidated watch list. The identifying information required depends on the policies and needs of the screening agency and the technical capacity of the respective agency’s computerized name-matching program. Also, certain records may not be exported to screening agency

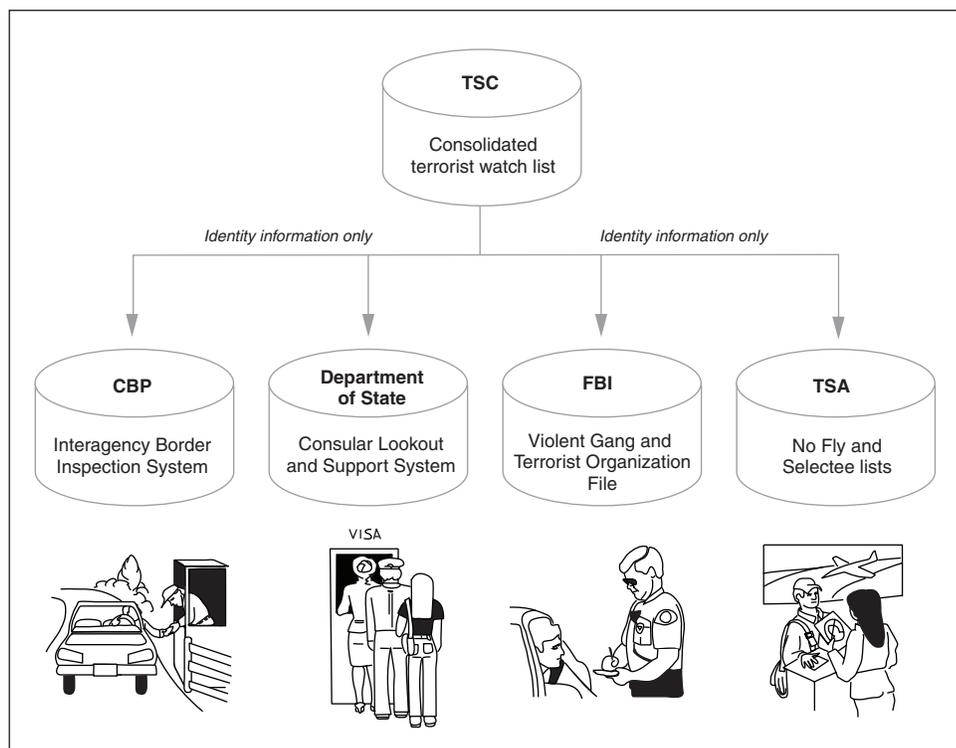
³⁹As discussed previously in this report, sensitive but unclassified identifying information from NCTC’s database is provided to TSC for inclusion on the consolidated terrorist watch list.

⁴⁰The Department of State’s Consular Lookout and Support System is used to screen (1) citizens of a foreign country who apply for U.S. visas and (2) U.S. citizens who apply for U.S. passports. Our work covered the use of the terrorist watch list in screening visa applicants, but we did not review or assess information related to passports.

⁴¹In addition to exporting applicable watch list records to federal government databases, TSC shares watch list records with certain foreign governments on a reciprocal basis. Additional information on U.S. government efforts to exchange watch list information with foreign governments is presented later in this report.

systems based on operational considerations, such as the amount of time available to conduct related screening. In general, the agency governing a particular screening database establishes the criteria for which records from the consolidated watch list will be accepted into its own system. Figure 4 presents a general overview of the process used to export records from TSC's consolidated watch list to screening agency databases.

Figure 4: General Overview of the Process Used to Export Records from TSC's Consolidated Watch List to Screening Agency Databases



Source: GAO analysis of TSC information.

Note: In addition to sending applicable watch list records to these federal government databases, TSC shares applicable records with certain foreign governments on a reciprocal basis, which is discussed later in this report.

According to TSC, in addition to agency mission, technical, and operational considerations, an individual's record may be excluded from an agency's database in rare cases when there is a reasonable and detailed justification for doing so and the request for exclusion has been reviewed and approved by the FBI's Counterterrorism Division and TSC. The following sections provide additional information on the databases of the

screening processes we reviewed, the percentage of records accepted as of May 2007, and potential security vulnerabilities.

Interagency Border Inspection System (CBP)

The Interagency Border Inspection System is DHS's primary lookout system available at U.S. ports of entry and other locations. CBP officers use the system to screen travelers entering the United States at ports of entry, which include land border crossings along the Canadian and Mexican borders, sea ports, and U.S. airports for international flight arrivals.⁴² This system includes not only the applicable records exported by TSC, but also additional information on people with prior criminal histories, immigration violations, or other activities of concern that CBP wants to identify and screen at ports of entry. The system is also used to assist law enforcement and other personnel at approximately 20 other federal agencies, including the following: U.S. Immigration and Customs Enforcement; U.S. Citizenship and Immigration Services; the FBI; the Drug Enforcement Administration; the Bureau of Alcohol, Tobacco, Firearms and Explosives; the Internal Revenue Service; the U.S. Coast Guard; the Federal Aviation Administration; and the U.S. Secret Service.

Of all the screening agency databases discussed in this report, the Interagency Border Inspection System has the least restrictive acceptance criteria and therefore contained the highest percentage of records from TSC's consolidated watch list as of May 2007. This is because CBP's mission is to screen all travelers, including U.S. citizens, entering the United States at ports of entry.

Consular Lookout and Support System (Department of State)

The Consular Lookout and Support System is the Department of State's name-check system for visa applicants. Consular officers abroad use the system to screen the names of visa applicants to identify terrorists and other aliens who are potentially ineligible for visas based on criminal histories or other reasons specified by federal statute. According to the Department of State, all visa-issuing posts have direct access to the system and must use it to check each applicant's name before issuing a visa.

⁴²The Interagency Border Inspection System is also part of DHS's United States Visitor and Immigrant Status Indicator Technology Program—known as US-VISIT—an automated entry-exit system that records the arrival and departure of aliens. See GAO, *Homeland Security: Planned Expenditures for U.S. Visitor and Immigrant Status Program Need to Be Adequately Defined and Justified*, GAO-07-278 (Washington, D.C.: Feb. 14, 2007).

Records on U.S. citizens and lawful permanent residents are not to be included in the part of the Consular Lookout and Support System that is used to screen visa applicants—because these individuals would not apply for U.S. visas—but may be included in another part of the system that is used to screen passport applicants. According to TSC officials, the part of the system that is used to screen visa applicants generally contains the same information as is contained in the Interagency Border Inspection System, except for records on U.S. citizens and lawful permanent residents. As of May 2007, the Consular Lookout and Support System contained the second highest percentage of all watch list records.

Violent Gang and Terrorist Organization File (FBI)

The Violent Gang and Terrorist Organization File is the FBI's lookout system for known or appropriately suspected terrorists, as well as gang groups and members. The file is part of the FBI's National Crime Information Center database, which is accessible by federal, state, and local law enforcement officers and other criminal justice agencies for screening in conjunction with arrests, detentions, and other criminal justice purposes.⁴³ A subset of the Violent Gang and Terrorist Organization file consists of TSC's records to be used to screen for possible terrorist links.⁴⁴ As of May 2007, the FBI database contained the third highest percentage of watch list records.

According to TSC officials, if the remaining watch list records were included in the Violent Gang and Terrorist Organization File, the system would identify an unmanageable number of records of individuals as potentially being matches to the National Crime Information Center database. The officials explained that name checks against the National Crime Information Center database return not only potential matches to terrorist watch list records in the Violent Gang and Terrorist Organization File, but also potential matches to the millions of other records in the

⁴³The FBI's National Crime Information Center is a computerized database of documented criminal justice information. It is available to federal, state, and local law enforcement and other criminal justice agencies nationwide and is operational 24 hours a day, 365 days a year.

⁴⁴Also, the FBI and designated state and local criminal justice agencies access the Violent Gang and Terrorist Organization File in conducting background checks on individuals seeking to purchase firearms or obtain permits to possess, acquire, or carry firearms. See GAO, *Gun Control and Terrorism: FBI Could Better Manage Firearm-Related Background Checks Involving Terrorist Watch List Records*, [GAO-05-127](#) (Washington, D.C.: Jan. 19, 2005).

database. TSC officials noted, however, that not including these records has resulted in a potential vulnerability in screening processes—or at least a missed opportunity to track the movements of individuals who are the subjects of watch list records and collect additional relevant information. According to the FBI, the remaining records are not included to ensure the protection of civil rights and prevent law enforcement officials from taking invasive enforcement action on individuals misidentified as being on the watch list. The FBI also noted that while law enforcement encounters of individuals on the watch list provide significant information, unnecessary detentions or queries of misidentified persons would be counterproductive and potentially damaging to the efforts of the FBI to investigate and combat terrorism. Because of these operational concerns, the FBI noted that the extent of vulnerabilities in current screening processes that arise when the Violent Gang and Terrorist Organization File cannot accept certain watch list records has been determined to be low or nonexistent. We note, however, that the FBI did not specifically address the extent to which security risks are raised by not using these records.

No Fly and Selectee Lists (TSA)

The No Fly and Selectee lists are compiled by TSC and forwarded to TSA, which distributes the lists to air carriers for use in identifying individuals who either should be precluded from boarding an aircraft or should receive additional physical screening prior to boarding a flight. TSA requires that U.S. aircraft operators use these lists to screen passengers on all of their flights and that foreign air carriers use these lists to screen passengers on all flights to and from the United States. Of all of the screening agency databases that accept watch list records, only the No Fly and Selectee lists require certain nomination criteria or inclusion standards that are narrower than the “known or appropriately suspected” standard of HSPD-6. Specifically, the lists are to contain any individual, regardless of citizenship, who meets certain nomination criteria established by the Homeland Security Council.⁴⁵

- Persons on the No Fly list are deemed to be a threat to civil aviation or national security and therefore should be precluded from boarding an aircraft. Passengers who are a match to the No Fly list are to be denied boarding unless subsequently cleared by law enforcement personnel in accordance with TSA procedures. The Homeland Security Council

⁴⁵The Homeland Security Council issued revised implementation guidelines related to the No Fly and Selectee list criteria in July 2006.

criteria contain specific examples of the types of terrorism-related conduct that may make an individual appropriate for inclusion on the No Fly list.

- Persons on the Selectee list are also deemed to be a threat to civil aviation or national security but do not meet the criteria of the No Fly list. Being on the Selectee list does not mean that the person will not be allowed to board an aircraft or enter the United States. Instead, persons on this list are to receive additional security screening prior to being permitted to board an aircraft, which may involve a physical inspection of the person and a hand-search of the passenger's luggage. The Homeland Security Council criteria contain specific examples of the types of terrorism-related conduct that may make an individual appropriate for inclusion on the Selectee list, as well as the types of activities that generally would not be considered appropriate for inclusion on the list.

According to the Homeland Security Council criteria, the No Fly and Selectee lists are not intended as investigative or information-gathering tools, or tracking mechanisms. Rather, the lists are intended to help ensure the safe transport of passengers and their property and to facilitate the flow of commerce. An individual must meet the specific nomination criteria to be placed on one of the lists, and the watch list record must contain a full name and date of birth to be added to either of the lists.

As of May 2007, the No Fly list and the Selectee list collectively contained the lowest percentage of watch list records. The remaining records in TSC's watch list either did not meet the specific Homeland Security Council nomination criteria or did not meet technical requirements that the records contain a full name and date of birth. TSC could not readily determine how many records fell into each of these two categories. Nonetheless, these records are not provided to TSA for use in prescreening passengers. According to TSA officials, without a full name and date of birth, the current name-matching programs used by airlines would falsely identify an unacceptable number of individuals as potentially being on the watch list.

According to DHS, the amount or specific types of biographical information available on the population to be screened should also be considered when determining what portion of the watch list should be used. For example, DHS noted that screening international airline passengers who have provided passport information is very different from screening domestic airline passengers for whom the government has little

biographical information. Further, DHS noted that for airline passengers, there is not much time to resolve false positives or determine whether someone on the watch list should be subjected to additional screening prior to departure of a flight, whereas for individuals arriving at U.S. ports of entry from international locations, CBP has more time to interview individuals and resolve issues upon their arrival.

For international flights bound to or departing from the United States, two separate screening processes occur. Specifically, in addition to TSA requiring that air carriers prescreen passengers prior to boarding against the No Fly and Selectee lists, CBP screens all passengers on international flights—for border security purposes—against watch list records in the Interagency Border Inspection System.⁴⁶ CBP's screening generally occurs after the aircraft is in flight.⁴⁷ This layered or secondary screening opportunity does not exist for passengers traveling domestically within the United States.

In 2006, the conference report accompanying the Department of Homeland Security Appropriations Act, 2007, directed TSA to provide a detailed plan describing key milestones and a schedule for checking names against the full terrorist watch list in its planned Secure Flight passenger prescreening program if the administration believes a security vulnerability exists under the current process of checking names against only the No Fly and Selectee lists.⁴⁸ According to TSA, the administration has concluded that non-use of the full watch list does not constitute a security vulnerability; however, TSA did not explain the basis for this determination. Also, DHS's Office for Civil Rights and Civil Liberties emphasized that there is a strong argument against increasing the number of watch list records TSA uses to prescreen passengers. Specifically, the office noted that if more records were used, the number of misidentifications would expand to unjustifiable proportions, increasing administrative costs within DHS, without a

⁴⁶As discussed previously, as of May 2007, CBP's system contained the highest percentage of the records in TSC's watch list.

⁴⁷Pursuant to a final rule published in the *Federal Register* in August 2007, this process will take place, in all instances, before an aircraft is in flight by the end of February 2008. See 72 Fed. Reg. 48,320 (Aug. 23, 2007).

⁴⁸See H.R. Conf. Rep. No. 109-669, at 140 (2006) (accompanying H.R. 5441, enacted into law as the Department of Homeland Security Appropriations Act, 2007, Pub. L. No. 109-295, 120 Stat. 1355 (2006)). See also Department of Homeland Security Appropriations Act, 2008, H.R. 2638, 110th Cong. (as passed by House of Representatives, June 15, 2007) (containing a similar requirement).

measurable increase in security. The office also noted that an expansion of the No Fly and Selectee lists could even alert a greater number of individuals to their watch list status, compromising security rather than advancing it. Further, according to the office, as the number of U.S. citizens denied and delayed boarding on domestic flights increases, so does the interest in maintaining watch list records that are as accurate as possible. Also, the office noted that an increase in denied and delayed boarding of flights could generate volumes of complaints or queries that exceed the current capabilities of the watch list redress process.

DHS Agencies Are Addressing Incidents of Persons on the Watch List Passing Undetected through Screening; TSC Has Ongoing Initiatives That Could Help Reduce This Vulnerability

Key frontline screening agencies within DHS—CBP, U.S. Citizenship and Immigration Services, and TSA—are separately taking actions to address potential vulnerabilities in terrorist watch list-related screening. A particular concern is that individuals on the watch list not pass undetected through agency screening. According to the screening agencies, some of these incidents—commonly referred to as false negatives—have occurred. Irrespective of whether such incidents are isolated aberrations or not, any individual on the watch list who passes undetected through agency screening constitutes a vulnerability. Regarding other ameliorative efforts, TSC has ongoing initiatives that could help reduce false negatives, such as improving the quality of watch list data.

Key Frontline Screening Agencies in DHS Are Separately Addressing Screening Vulnerabilities

CBP, U.S. Citizenship and Immigration Services, and TSA have begun to take actions to address incidents of subjects of watch list records passing undetected through agency screening. The efforts of each of these three DHS component agencies are discussed in the following sections, respectively. Generally, as indicated, positive steps have been initiated by each agency. Given the potential consequences of any given incident, it is particularly important that relevant component agencies have mechanisms in place to systematically monitor such incidents, determine causes, and implement appropriate corrective actions as expeditiously as possible.

U.S. Customs and Border Protection Is Studying Cases Where Some Subjects of Watch List Records Were Not Detected by Screening at Ports of Entry

During our field visits in spring 2006 to selected ports of entry, CBP officers informed us of several incidents involving individuals on the watch list who were not detected until after they had been processed and admitted into the United States.⁴⁹ In response to our inquiry at CBP headquarters in May 2006, agency officials acknowledged that there have been such incidents. CBP did not maintain aggregated data on the number of these incidents nationwide or the specific causes, but it did identify possible reasons for failing to detect someone on the watch list. Subsequently, in further response to our inquiries, CBP created a working group to study the causes of incidents involving individuals on the watch list who were not detected by port-of-entry screening. The working group, coordinated by the National Targeting Center, is composed of subject matter experts representing the policy, technical, and operations facets within CBP. According to headquarters officials, the group is responsible for (1) identifying and recommending policy solutions within CBP and (2) coordinating any corrective technical changes within CBP and with TSC and NCTC, as appropriate. The working group held its first meeting in early 2007. According to CBP, some corrective actions and measures have already been identified and are in the process of being implemented.

Agencies Are Working on Solutions to Prevent Unauthorized Applicants for Citizenship and Other Immigration Benefits from Getting through Agency Screening

Agencies are working to eliminate shortcomings in screening processes that have resulted in unauthorized applicants for citizenship and other immigration benefits getting through agency screening. The cognizant agency, U.S. Citizenship and Immigration Services, is to screen all individuals who apply for U.S. citizenship or other immigration benefits—such as work authorization—for information relevant to their eligibility for these benefits. According to U.S. Citizenship and Immigration Services officials, the agency does not maintain aggregated data on the number of times the initial screening has failed to identify individuals who are subjects of watch list records or the specific causes. The officials noted, however, that for certain applicants—including individuals seeking long-term benefits such as permanent citizenship, lawful permanent residence, or asylum—additional screening against watch list records is conducted. This additional screening has generated some positive matches to watch

⁴⁹We visited various CBP ports of entry at airports and land border crossings in California, Michigan, New York, and Texas (see app. I).

A Final Rule and a Planned
Prescreening Program Could
Help Address the Issue of
Individuals on the No Fly List
Being Inadvertently Allowed
to Fly

list records, whereas these matches were not detected during the initial checks.⁵⁰

According to U.S. Citizenship and Immigration Services, each instance of individuals on the watch list getting through agency screening is reviewed on a case-by-case basis to determine the cause, with appropriate follow-up and corrective action taken, if needed. As a prospective enhancement, in April 2007, U.S. Citizenship and Immigration Services entered into a memorandum of understanding with TSC. If implemented, this enhancement could allow U.S. Citizenship and Immigration Services to conduct more thorough and efficient searches of watch list records during the screening of benefit applicants.

In the past, there have been a number of known cases in which individuals who were on the No Fly list passed undetected through airlines' prescreening of passengers and flew on international flights bound to or from the United States, according to TSA data. These individuals were subsequently identified in-flight by other means—specifically, screening of passenger manifests conducted by CBP's National Targeting Center. However, the onboard security threats required an immediate counterterrorism response, which in some instances resulted in diverting the aircraft to a location other than its original destination. TSA provided various reasons why an individual who is on the No Fly list may not be detected by air carriers during their comparisons with the No Fly list. However, TSA had not analyzed the extent to which each cause contributed to such incidents. According to TSA, the agency's regulatory office is responsible for initiating investigative and corrective actions with the respective air carrier, if needed.

For international flights bound to or from the United States, two separate screening processes occur. In addition to the initial prescreening conducted by the airlines in accordance with TSA requirements, CBP's National Targeting Center screens passengers against watch list records in the Interagency Border Inspection System using information that is collected from air carriers' passenger manifests, which contain information obtained directly from government-issued passports. Specifically, for passengers flying internationally, airlines are required to

⁵⁰In 2005, we reported on U.S. Citizenship and Immigration Services' efforts to manage backlogs of immigration benefit applications. See GAO, *Immigration Benefits: Improvements Needed to Address Backlogs and Ensure Quality of Adjudications*, GAO-06-20 (Washington, D.C.: Nov. 21, 2005).

provide passenger manifest data obtained at check-in from all passengers to CBP.⁵¹ Presently, CBP requires airlines to transmit the passenger data no later than 15 minutes prior to departure for outbound flights and no later than 15 minutes after departure for inbound flights.⁵² Because the transmission of this information occurs so close to the aircraft's departure, the National Targeting Center's screening of the information against watch list records in the Interagency Border Inspection System—which includes a check of records in the No Fly list—often is not completed until after the aircraft is already in the air. If this screening produces a positive match to the No Fly list, the National Targeting Center is to coordinate with other federal agencies to determine what actions to take.

Procedures described in the final rule issued by CBP and published in the *Federal Register* on August 23, 2007, could help mitigate instances of individuals on the No Fly list boarding international flights bound to or from the United States. Specifically, the rule will require air carriers to either transmit complete passenger manifests to CBP no later than 30 minutes prior to the securing of the aircraft doors, or transmit manifest information on an individual basis as each passenger checks in for the flight up to but no later than the securing of the aircraft. When implemented (the rule is to take effect on February 19, 2008), CBP should be better positioned to identify individuals on the No Fly list before an international flight is airborne.⁵³

Regarding domestic flights within the United States, there is no second screening opportunity using watch list-related information. Rather, the airlines are responsible for prescreening passengers prior to boarding in accordance with TSA requirements and using the No Fly and Selectee lists provided by TSA. Although TSA has been mandated to assume

⁵¹See 19 C.F.R. §§ 122.49a, 122.75a (listing the required passenger manifest information for international arrivals and departures, respectively).

⁵²CBP defines “departure” as the point at which the wheels are up on the aircraft and the aircraft is en route directly to its destination. See 19 C.F.R. § 122.49a(a). CBP, however, issued a final rule that, among other things, will require the transmission of passenger data no later than the “securing of the aircraft,” defined as the moment the aircraft's doors are closed and secured for flight. See 72 Fed. Reg. 48,320 (Aug. 23, 2007). The provisions of the final rule take effect on February 19, 2008.

⁵³For additional information on international passenger prescreening, see GAO, *Aviation Security: Efforts to Strengthen International Passenger Prescreening Are Under Way, but Planning and Implementation Issues Remain*, [GAO-07-346](#) (Washington, D.C.: May 16, 2007).

responsibility for conducting the watch list screening function from the airline industry, the agency's proposed prescreening program, known as Secure Flight, has not yet been implemented.⁵⁴ Under the Secure Flight program, TSA plans to take over from aircraft operators the responsibility for comparing identifying information on airline passengers against watch list records. We have reported and TSA has acknowledged significant challenges in developing and implementing the Secure Flight program.⁵⁵ Last year, TSA suspended Secure Flight's development to reassess, or rebaseline, the program. The rebaselining effort included reassessing the program goals, the expected benefits and capabilities, and the estimated schedules and costs. According to TSC officials who have been working with TSA to support implementation of Secure Flight, the program could help to reduce potential vulnerabilities in the prescreening of airline passengers on domestic flights.

The Terrorist Screening Center Has Various Ongoing or Planned Initiatives That Could Help Reduce Vulnerabilities in Watch List-Related Screening

Improving the Effectiveness of Screening: Search Engine Technology and Direct-Query Capability

To help reduce vulnerabilities in watch list-related screening, TSC has ongoing initiatives to improve the effectiveness of screening and ensure the accuracy of data. Also, prospectively, TSC anticipates developing a capability to link biometric data to supplement name-based screening.

Generally, to handle the large volumes of travelers and others who must be screened, federal agencies and most airlines use computer-driven algorithms to rapidly compare the names of individuals against applicable terrorist watch list records.⁵⁶ In the name-matching process, the number of likely matching records returned for manual review depends partly upon the sensitivity thresholds of the algorithms to variations in name spelling or representations of names from other languages. Screening agencies, and airlines in accordance with TSA requirements, have discretion in

⁵⁴See 49 U.S.C. § 44903(j)(2)(C). In August 2007, TSA issued its notice of proposed rulemaking for the Secure Flight program. See 72 Fed. Reg. 48,356 (Aug. 23, 2007).

⁵⁵GAO, *Aviation Security: Management Challenges Remain for the Transportation Security Administration's Secure Flight Program*, [GAO-06-864T](#) (Washington, D.C.: June 14, 2006).

⁵⁶An algorithm is a prescribed set of well-defined, unambiguous rules or processes for the solution of a problem in a finite number of steps.

setting these thresholds, which can have operational implications. If a threshold is set relatively high, for example, more names may be cleared and fewer flagged as possible matches, increasing the risk of false negatives—that is, failing to identify an individual whose name is on the terrorist watch list. Conversely, if a threshold is set relatively low, more individuals who do not warrant additional scrutiny may be flagged (false positives), with fewer cleared through an automated process. A primary factor in designing a computerized name-matching process is the need to balance minimizing the possibility of generating false negatives, while not generating an unacceptable number of false positives (misidentifications).

To help ensure awareness of best practices among agencies, TSC has formed and chairs an interagency working group—the Federal Identity Match Search Engine Performance Standards Working Group—that met initially in December 2005.⁵⁷ An objective of the working group is to provide voluntary guidance for federal agencies that use identity matching search engine technology. Essentially, the prospective guidance is intended to improve the effectiveness of identity matching across agencies by, among other means, assessing which algorithms or search engines are the most effective for screening specific types or categories of names. According to TSC, three agencies have volunteered to participate in pilot programs in the summer of 2007, after which a target date for completing the initiative to develop and provide voluntary guidance to screening agencies will be set. If effectively implemented, this initiative could help reduce potential vulnerabilities in screening processes that are based on limitations in agencies' computerized name-matching programs.

TSC is also developing a process whereby screening agencies can directly “query” the center’s consolidated terrorist screening database. TSC noted that a direct-query capability will ensure that all possible hits against the database will be directed automatically into the center’s resolution process to determine if they are positive matches, thereby ensuring consistency in the government’s approach to screening. Currently, TSC must rely upon the screening agencies to contact the center—generally by telephone or fax—when they have possible hits. As of May 2007, TSC had not developed specific time frames for implementing this initiative.

⁵⁷The working group’s membership includes representatives from the Departments of Homeland Security (including TSA and CBP), State, and Defense; FBI; and the intelligence community (including NCTC, Central Intelligence Agency, National Security Agency, and Defense Intelligence Agency). Also, the National Institute of Standards and Technology acts as a special advisor to the working group.

Improving Data Quality

According to TSC, the technology for a direct-query capability is in place, but related agreements with screening agencies were still being negotiated.

Preventing incidents of individuals on the watch list passing undetected through agency screening is dependent partly on the quality and accuracy of data in TSC's consolidated terrorist watch list. In June 2005, the Department of Justice's Office of the Inspector General reported that its review of TSC's consolidated watch list found several problems—such as inconsistent record counts and duplicate records, lack of data fields for some records, and unclear sources for some records.⁵⁸ Among other things, the Inspector General recommended that TSC develop procedures to regularly review and test the information contained in the consolidated terrorist watch list to ensure that the data are complete, accurate, and nonduplicative. In its September 2007 follow-up report, the Inspector General noted that TSC has enhanced its efforts to ensure the quality of watch list data and has increased the number of staff assigned to data quality management. However, the Inspector General also determined that TSC's management of the watch list continues to have weaknesses.⁵⁹

TSC has ongoing quality-assurance initiatives to identify and correct incomplete or inaccurate records that could contribute to either false negatives or false positives. The center's director and principal deputy director stressed to us that quality of data is a high priority and also is a continuing challenge, particularly given that the database is dynamic, changing frequently with additions, deletions, and modifications. The officials noted the equal importance of ensuring that (1) the names of known and appropriately suspected terrorists are included on the watch list and (2) the names of any individuals who are mistakenly listed or are cleared of any nexus to terrorism are removed. In this regard, the officials explained that the TSC's standard operating practices include at least three opportunities to review records. First, TSC staff—including subject matter experts detailed to the center from other agencies—review each incoming record submitted (nominated) to the center for inclusion on the consolidated watch list. Second, every time there is a screening encounter—for example, a port-of-entry screening of an individual that

⁵⁸Department of Justice, Office of the Inspector General, *Review of the Terrorist Screening Center*, Audit Report 05-27 (June 2005).

⁵⁹Department of Justice, Office of the Inspector General, *Follow-up Audit of the Terrorist Screening Center*, Audit Report 07-41 (September 2007).

generates an actual or a potential match with a watch list record—that record is reviewed again. And third, records are reviewed when individuals express their concerns or seek correction of any inaccurate data—a process often referred to as redress.⁶⁰

Future Enhancement: Linking to Biometric Data

Conceptually, biometric technologies based on fingerprint recognition, facial recognition, or other physiological characteristics can be used to screen travelers against a consolidated database, such as the terrorist watch list.⁶¹ However, TSC presently does not have this capability, although use of biometric information to supplement name-based screening is planned as a future enhancement. Specifically, TSC’s strategy is not to replicate existing biometric data systems. Rather, the strategy, according to TSC’s director and principal deputy director, is to develop a “pointer” capability to facilitate the online linking of name-based searches to relevant biometric systems, such as the FBI’s Integrated Automated Fingerprint Identification System—a computerized system for storing, comparing, and exchanging fingerprint data in a digital format that contains the largest criminal biometric database in the world. TSC officials recognize that even biometric systems have screening limitations, such as relevant federal agencies may have no fingerprints or other biometrics to correlate with many of the biographical records in the TSC’s watch list. For instance, watch list records may be based on intelligence gathered by electronic wire taps or other methods that involve no opportunity to obtain biometric data. Nonetheless, TSC officials anticipate that biometric information, when available, can be especially useful for confirming matches to watch list records when individuals use false identities or aliases.

⁶⁰Redress generally refers to an agency’s complaint resolution process, whereby individuals may seek resolution of their concerns about an agency action. See GAO, *Terrorist Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public*, [GAO-06-1031](#) (Washington, D.C.: Sept. 29, 2006).

⁶¹In an earlier report, we assessed various biometric technologies. See GAO, *Technology Assessment: Using Biometrics for Border Security*, [GAO-03-174](#) (Washington, D.C.: Nov. 15, 2002).

The U.S. Government Has Made Progress in Using the Watch List but a Strategy and Plan Supported by a Governance Structure with Clear Lines of Authority Would Enhance Use and Effectiveness

Although the U.S. government has made progress in using watch list records to support terrorism-related screening, there are additional opportunities for using the list. Internationally, the Department of State has made arrangements with six foreign governments to exchange terrorist watch list information and is in negotiations with several other countries. Within the private sector, some critical infrastructure components are presently using watch list records to screen current or prospective employees, but many components are not. DHS has not established guidelines to govern the use of watch list records for appropriate screening opportunities in the private sector that have a substantial bearing on homeland security. Further, all federal departments and agencies have not taken action in accordance with HSPD-6 and HSPD-11 to identify and describe all appropriate screening opportunities that should use watch list records. According to TSC, determining whether new screening opportunities are appropriate requires evaluation of multiple factors, including operational and legal issues—particularly related to privacy and civil liberties. To date, appropriate opportunities have not been systematically identified or evaluated, in part because the federal government lacks an up-to-date strategy and a prioritized investment and implementation plan for optimizing the use and effectiveness of terrorist-related screening. Moreover, the lines of authority and responsibility to provide governmentwide coordination and oversight of such screening are not clear, and existing entities with watch list responsibilities may not have the necessary authority, structure, or resources to assume this role.

The Department of State Has Made Progress in Efforts to Exchange Terrorist Watch List Information with Foreign Governments

According to the 9/11 Commission, the U.S. government cannot meet its obligations to the American people to prevent the entry of terrorists into the United States without a major effort to collaborate with other governments.⁶² The commission noted that the U.S. government should do more to exchange terrorist information with trusted allies and raise U.S. and global border security standards for travel and border crossing over the medium and longterm through extensive international cooperation. HSPD-6 required the Secretary of State to develop a proposal for the President's approval for enhancing cooperation with certain foreign governments—beginning with those countries for which the United States

⁶²National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (July 22, 2004).

has waived visa requirements—to establish appropriate access to terrorism screening information of the participating governments.⁶³ This information would be used to enhance existing U.S. government screening processes.

The Department of State determined that the most effective way to obtain this information was to seek bilateral arrangements to share information on a reciprocal basis. The Department of State's Bureau of Consular Affairs and the Homeland Security Council co-chair an interagency working group to implement the international cooperation provisions of HSPD-6.⁶⁴ According to the Department of State, there is no single document or proposal that sets forth the working group's approach or plan. Rather, a series of consensus decisions specify how to proceed, often on a country-by-country basis in order to accommodate each country's laws and political sensitivities. The working group met six times from September 2005 through December 2006 to discuss operational and procedural issues related to sharing terrorism information and to update working group members on the status of bilateral negotiations with foreign governments.

According to the Department of State, the department's Bureau of Consular Affairs has approached all countries for which the United States has waived visa requirements and two non-visa waiver program countries with a proposal to exchange terrorist screening information. From October through December 2006, interagency teams visited six countries to brief government officials and also met in Washington, D.C., with representatives of a number of other countries. According to the Department of State, interagency working groups at U.S. embassies

⁶³Foreign nationals from visa waiver countries are allowed to travel to the United States under limited conditions and for a limited time without obtaining a visa. The following 27 countries are currently in the visa waiver program: Andorra, Austria, Australia, Belgium, Brunei, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Japan, Liechtenstein, Luxembourg, Monaco, the Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom. For additional information on the visa waiver program, see GAO, *Border Security: Stronger Actions Needed to Assess and Mitigate the Risks of the Visa Waiver Program*, [GAO-06-854](#) (Washington, D.C: July 28, 2006).

⁶⁴According to the Department of State, interagency working group members represent agencies and organizations from the intelligence and law enforcement communities with an interest in the implementation of HSPD-6, including the Central Intelligence Agency, the FBI, the Defense Intelligence Agency, the National Security Agency, DHS, the Department of Justice, the Office of Management and Budget, and TSC.

around the world remain actively engaged with foreign counterparts and coordinate discussions on international sharing of terrorist screening information with a Department of State team in Washington, D.C.

Two countries have been sharing terrorist screening information with the United States since before September 11, 2001, and that information has been integrated into TSC's consolidated watch list and, as applicable, into screening agencies' databases. According to the Department of State, since 2006, the United States has made arrangements to share terrorist screening information with four new foreign government partners and is in negotiations with several other countries. The department noted that it had also received indications of interest from governments of non-visa waiver countries.

DHS Has Not Finalized Guidelines for Using Watch List Records to Support Private Sector Screening

Although federal departments and agencies have made progress in using terrorist watch list records to support private sector screening processes, there are additional opportunities for using records in the private sector. However, DHS has not yet finalized guidelines to govern such use. Specifically, HSPD-6 required the Secretary of Homeland Security to develop guidelines to govern the use of terrorist information, as defined by the directive, to support various screening processes, including private sector screening processes that have a substantial bearing on homeland security. The interagency memorandum of understanding that implements HSPD-6 also required the Secretary of Homeland Security to establish necessary guidelines and criteria to (a) govern the mechanisms by which private sector entities can access the watch list and (b) initiate appropriate law enforcement or other governmental action, if any, when a person submitted for query by a private sector entity is identified as a person on the watch list.

According to the Associate Director of the Screening Coordination Office within DHS, in developing guidelines to govern private sector screening against watch list records, the department planned to partner with the

National Infrastructure Advisory Council.⁶⁵ The council had previously reported that the private sector wants to be informed about threats and potential terrorists. Specifically, in its July 2006 report on public and private sector intelligence coordination, the National Infrastructure Advisory Council noted that chief executive officers of private sector corporations expect to be informed when the government is aware of a specific, credible threat to their employees, physical plants, or cyber assets.⁶⁶ The report also noted that chief executive officers expect to be informed if the government knows that their respective company has inadvertently employed a terrorist.

According to DHS's Office of Infrastructure Protection and Infrastructure Partnerships Division, employees in parts of some components of the private sector are being screened against watch list records, including certain individuals who have access to the protected or vital areas of nuclear power plants, work in airports, and transport hazardous materials. However, many critical infrastructure components are not using watch list records. The office also indicated that several components of the private sector are interested in screening employees against watch list records or expanding current screening. In its June 2007 comments on a draft of this report (see app. V), DHS noted that the Screening Coordination Office has drafted initial guidelines to govern the use of watch list records to support private sector screening processes and was in the process of working with federal stakeholders to finalize this document. However, DHS did not provide specific plans and time frames for finalizing the guidelines. Establishing guidelines to govern the private sector's use of watch list records, in accordance with HSPD-6, would help in identifying and implementing appropriate screening opportunities.

⁶⁵The National Infrastructure Advisory Council is to provide the President, through the Secretary of Homeland Security, with advice on the security of critical infrastructure sectors of the economy. It also is authorized to provide advice directly to the heads of other agencies that have shared responsibility for critical infrastructure protection, including the Departments of Health and Human Services, Transportation, and Energy. The council is charged to improve the cooperation and partnership between the public and private sectors in securing the critical infrastructures and advising on related policies and strategies, such as clarification of the roles and responsibilities between public and private sectors.

⁶⁶National Infrastructure Advisory Council, *Public-Private Sector Intelligence Coordination: Final Report and Recommendations by the Council* (June 11, 2006).

Federal Departments and Agencies Have Not Identified All Appropriate Opportunities for Using Watch List Records to Detect and Deter Terrorists

Although required to do so by presidential directives, federal departments and agencies have not identified all appropriate screening opportunities that should use terrorist watch list records. Specifically, HSPD-6 required the heads of executive departments and agencies to conduct screening using the terrorist watch list at all appropriate opportunities, and to report the opportunities at which such screening shall and shall not be conducted to the Attorney General. TSC provided an initial report on screening opportunities to the Attorney General on December 15, 2003.⁶⁷ According to the report, TSC hosted a meeting with representatives of more than 30 agencies in October 2003 to discuss the HSPD-6 requirement. At the meeting, TSC requested that the agencies identify appropriate screening opportunities and report them to TSC. However, the report noted that based on the agency responses TSC received, no meaningful or comprehensive report on screening opportunities could be produced at that time. TSC provided additional reports to the Attorney General in April, July, and December 2004. These reports also did not contain comprehensive information on all screening opportunities, consistent with HSPD-6.

According to the Department of Justice, with the issuance of HSPD-11, which “builds upon” HSPD-6, the Attorney General’s responsibilities for identifying additional screening opportunities were largely overtaken by DHS which, in coordination with the Department of Justice and other agencies, was to create a comprehensive strategy to enhance the effectiveness of terrorist-related screening activities. Among other things, the strategy was to include a description of the screening opportunities for which terrorist-related screening would be applied. DHS has taken some related actions but, as of June 2007, it had not systematically identified all appropriate screening opportunities.⁶⁸ Absent a systematic approach to identifying appropriate screening opportunities, TSC has been working with individual agencies to identify such opportunities. According to TSC, as of May 2007, the center was working on approximately 40 agreements with various federal departments or agencies to use applicable portions of the terrorist watch list.

⁶⁷TSC’s initial report and supplemental reports were provided to the Attorney General via memorandums from the Director of the FBI.

⁶⁸Additional information on DHS’s efforts to develop the strategy is discussed later in the report.

Also, a systematic approach to identifying screening opportunities would help the government determine if other uses of watch list records are appropriate and should be implemented, including uses primarily intended to assist in collecting information to support investigative activities. Such coordinated collection of information for use in investigations is one of the stated policy objectives for the watch list. For example, during our review, TSC noted that screening domestic airline passengers against watch list records in addition to those in the No Fly and Selectee lists would have benefits, such as collecting information on the movements of individuals with potential ties to terrorism. According to TSC, other factors would need to be considered in determining whether such screening is appropriate and should be implemented, including privacy and civil liberties implications. Moreover, it is not clear whether such screening is operationally feasible, and if it were, whether TSC or some other agency would perform the screening.

The U.S. Government Lacks an Updated Strategy and an Investment and Implementation Plan for Enhancing the Use and Effectiveness of Terrorist-Related Screening

Since September 11, 2001, we, as well as the Administration, have called for a more strategic approach to managing terrorist-related information and using it for screening purposes. In April 2003, we made recommendations for improving the information technology architecture environment needed to support watch list-related screening and called for short- and long-term strategies that would provide for (1) more consolidated and standardized watch list information and (2) more standardized policies and procedures for better sharing watch list data and for addressing any legal issues or cultural barriers that affect watch list sharing.⁶⁹ Subsequently, in August 2004, HSPD-11 outlined the Administration's vision to develop comprehensive terrorist-related screening procedures. Specifically, HSPD-11 required the Secretary of Homeland Security—in coordination with the heads of appropriate federal departments and agencies—to submit two reports to the President (through the Assistant to the President for Homeland Security) related to the government's use of the watch list. Among other things, the first report was to outline a strategy to enhance the effectiveness of terrorist-related screening activities by developing comprehensive, coordinated, and systematic procedures and capabilities. The second report was to provide a prioritized investment and implementation plan for a systematic approach to terrorist-related screening that optimizes detection and interdiction of suspected terrorists and terrorist activities. The plan was to

⁶⁹ [GAO-03-322](#).

describe the “scope, governance, principles, outcomes, milestones, training objectives, metrics, costs, and schedule of activities” to enhance and implement the U.S. government’s terrorism-related screening policies.

According to DHS officials, the department submitted the required strategy and the investment and implementation plan to the President in November 2004. However, neither DHS nor the Homeland Security Council would provide us copies of either report. Instead, officials from DHS’s Screening Coordination Office provided us a document that they said contained department-specific information from the 2004 strategy and implementation plan.⁷⁰ According to DHS officials, because the strategy and plan were products of an interagency process, the Screening Coordination Office believed that it needed to redact information that pertained to other departments’ processes, programs, or activities. The DHS document contains information on the department’s efforts to catalogue its terrorist-related screening activities and identifies significant issues that inhibit effective terrorist-related screening. For example, according to the document, “no one entity within the department is responsible for defining roles and responsibilities for terrorist-related screening, identifying gaps and overlaps in screening opportunities, prioritizing investments, measuring performance, or setting technical and non-technical standards.” Also, the document notes that DHS components may have only limited knowledge of what screening is currently being performed by others within the department, because there is no coordination mechanism to share information on these activities.

DHS acknowledged that it has not updated either the strategy or the plan since the 2004 reports, despite the fact that some aspects of the strategy and plan had been overcome by other events, such as results of the “Second Stage Review” initiated in March 2005 by the Secretary of Homeland Security.⁷¹ Moreover, according to DHS screening managers, the departmental office responsible for updating these documents—the Screening Coordination Office—was not established until July 2006 and has had other screening-related priorities. The officials noted that the

⁷⁰DHS established the Screening Coordination Office in July 2006 to enhance security measures by integrating the department’s terrorist- and immigration-related screening efforts, creating unified screening standards and policies, and developing a single redress process for travelers.

⁷¹The review’s purpose was to systematically evaluate DHS’s operations, policies, and structures. On July 13, 2005, the Secretary of Homeland Security announced completion of the review.

Screening Coordination Office is working on various aspects of terrorist-related screening, but that work remains in updating the strategy and the investment and implementation plan.

Without an updated strategy and plan, the federal government lacks mechanisms to support a comprehensive and coordinated approach to terrorist-related screening envisioned by the Administration, including mechanisms for building upon existing systems and best practices. Also, the federal government has not taken necessary actions to promote the effective use of watch list records at all appropriate screening opportunities, including private sector screening processes that have a substantial bearing on homeland security. An updated strategy and an investment and implementation plan that address the elements prescribed by HSPD-11—particularly clearly articulated principles, milestones, and outcome measures—could also provide a basis for establishing governmentwide priorities for screening, assessing progress toward policy goals and intended outcomes, ensuring that any needed changes are implemented, and responding to issues our work identified, such as potential screening vulnerabilities and interagency coordination challenges.

Existing Governance Structures May Not Provide Necessary Oversight and Coordination

Recognizing that achievement of a coordinated and comprehensive approach to terrorist-related screening involves numerous entities within and outside the federal government, HSPD-11 called for DHS to address governance in the investment and implementation plan. To date, however, no governance structure with clear lines of responsibility and authority has been established to monitor governmentwide screening activities—such as assessing gaps or vulnerabilities in screening processes and identifying, prioritizing, and implementing new screening opportunities. Lacking clear lines of authority and responsibility for terrorist-related screening activities that transcend the individual missions and more parochial operations of each department and agency, it is difficult for the federal government to monitor its efforts and to identify best practices or common corrective actions that could help to ensure that watch list records are used as effectively as possible. More clearly defined responsibility and authority to implement and monitor crosscutting initiatives could help ensure a more coordinated and comprehensive approach to terrorist-related screening by providing applicable departments and agencies important guidance, information, and mechanisms for addressing screening issues.

Until the governance component of the investment and implementation plan is clearly articulated and established, it will not be possible to assess whether its structure is capable of providing the oversight necessary for optimizing the use and effectiveness of terrorist-related screening. Our interviews with responsible officials and our analysis of department and agency missions suggest, however, that existing organizations with watch list-related responsibilities may lack the authority, resources, or will to assume this role. Specifically, DHS screening officials told us that the department is the appropriate entity for coordinating the development of the watch list strategy and the related investment and implementation plan, but that it does not have the authority or resources for providing the governmentwide oversight needed to implement the strategy and plan or resolve interagency issues. The Office of the Director of National Intelligence and its NCTC also have important roles in watch list-related issues and information-sharing activities, but officials there told us that the agency is not suited for a governmentwide leadership role either, primarily because its mission focuses on intelligence and information sharing in support of screening but not on actual screening operations. Likewise, since its inception, TSC has played a central role in coordinating watch list-related activities governmentwide and has established its own governance board—composed of senior-level agency representatives from numerous departments and agencies—to provide guidance concerning issues within TSC’s mission and authority. While this governance board could be suited to assume more of a leadership role, its current authority is limited to TSC-specific issues, and it would need additional authority to provide effective coordination of terrorist-related screening activities and interagency issues governmentwide.

Conclusions

Managed by TSC, the terrorist watch list represents a major step forward from the pre-September 11 environment of multiple, disconnected, and incomplete watch lists throughout the government. Today, the watch list is an integral component of the U.S. government’s counterterrorism efforts. However, our work indicates that there are additional opportunities for reducing potential screening vulnerabilities. It is important that responsible federal officials assess the extent to which security vulnerabilities exist in screening processes when agencies are not able to screen individuals on the watch list to determine the level of threat the individuals pose because of technical or operational reasons and—in consultation with TSC and other agencies—determine whether alternative screening or other mitigation activities should be considered. Our work also indicates the need for a more coordinated and comprehensive approach to terrorist-related screening through expanded use of the list

and enhanced collaboration and coordination within and outside the federal government.

To further strengthen the ability of the U.S. government to protect against acts of terrorism, HSPD-6 required the Secretary of Homeland Security to develop guidelines to govern the use of terrorist information to support various screening processes, including private sector screening processes that have a substantial bearing on homeland security. To date, however, DHS has not developed guidelines for the private sector's use of watch list records in screening designed to protect the nation's critical infrastructures. Currently, some but not all relevant components of the private sector use the watch list to screen for terrorist-related threats. Establishing clear guidelines to comply with the presidential directive would help both the private sector and DHS ensure that private sector entities are using watch list records consistently, appropriately, and effectively to protect their workers, visitors, and key critical assets.

HSPD-11 outlined the Administration's vision to implement a coordinated and comprehensive approach to terrorist-related screening and directed the Secretary of Homeland Security to coordinate with other federal departments to develop (1) a strategy for a coordinated and comprehensive approach to terrorist-related screening and (2) a prioritized investment and implementation plan that describes the scope, governance, principles, outcomes, milestones, training objectives, metrics, costs, and schedule of activities necessary to achieve the policy objectives of HSPD-11. DHS officials acknowledged that work remains to update the strategy and the investment and implementation plan. Without an up-to-date strategy and plan, agencies and organizations that engage in terrorist-related screening activities do not have a foundation for a coordinated approach that is driven by an articulated set of core principles. Furthermore, lacking clearly articulated principles, milestones, and outcome measures, the federal government is not easily able to provide accountability and a basis for monitoring to ensure that (1) the intended goals for, and expected results of, terrorist screening are being achieved and (2) use of the list is consistent with privacy and civil liberties. These plan elements, which were prescribed by HSPD-11, are crucial for coordinated and comprehensive use of terrorist-related screening data, as they provide a platform to establish governmentwide priorities for screening, assess progress toward policy goals and intended outcomes, ensure that any needed changes are implemented, and respond to issues that hinder effectiveness, such as the potential vulnerabilities and interagency coordination challenges discussed in this report.

Although all elements of a strategy and an investment and implementation plan cited in HSPD-11 are important to guide realization of the most effective use of watch list data, addressing governance is particularly vital, as achievement of a coordinated and comprehensive approach to terrorist-related screening involves numerous entities within and outside the federal government. Establishing a governance structure with clearly defined responsibility and authority would help ensure that agency efforts are coordinated and the federal government has the means to monitor and analyze the outcomes of interagency efforts and to address common problems efficiently and effectively. To date, however, no clear lines of responsibility and authority have been established to monitor governmentwide screening activities for shared problems and solutions or best practices. Neither does any existing entity clearly have the requisite authority for addressing various governmentwide issues—such as assessing common gaps or vulnerabilities in screening processes and identifying, prioritizing, and implementing new screening opportunities. Indeed, current unresolved interagency issues highlight the need for clearly defined leadership and accountability for managing and overseeing watch list-related issues across the individual departments and agencies, each of which has its own mission and focus.

Recommendations for Executive Action

To promote more comprehensive and coordinated use of terrorist-related screening data to detect, identify, track, and interdict suspected terrorists, we recommended a total of five actions in the restricted version of this report.

First, in order to mitigate security vulnerabilities in terrorist watch list screening processes, we recommended that the Secretary of Homeland Security and the Director of the FBI assess to what extent there are vulnerabilities in the current screening processes that arise when screening agencies do not accept relevant records due to the designs of their computer systems, the extent to which these vulnerabilities pose a security risk, and what actions, if any, should be taken in response.

Further, we recommended the following three actions to enhance the use of the consolidated terrorist watch list as a counterterrorism tool and to help ensure its effectiveness:

- that the Secretary of Homeland Security in consultation with the heads of other appropriate federal departments and agencies and private sector entities, develop guidelines to govern the use of watch list

records to support private sector screening processes that have a substantial bearing on homeland security, as called for in HSPD-6;

- that the Secretary of Homeland Security in consultation with the heads of other appropriate federal departments, develop and submit to the President through the Assistant to the President for Homeland Security and Counterterrorism an updated strategy for a coordinated and comprehensive approach to terrorist-related screening as called for in HSPD-11, which among other things, (a) identifies all appropriate screening opportunities to use watch list records to detect, identify, track, and interdict individuals who pose a threat to homeland security and (b) safeguards legal rights, including privacy and civil liberties; and
- that the Secretary of Homeland Security in consultation with the heads of other appropriate federal departments, develop and submit to the President through the Assistant to the President for Homeland Security and Counterterrorism an updated investment and implementation plan that describes the scope, governance, principles, outcomes, milestones, training objectives, metrics, costs, and schedule of activities necessary for implementing a terrorist-related screening strategy, as called for in HSPD-11.

Finally, to help ensure that governmentwide terrorist-related screening efforts have the oversight, accountability, and guidance necessary to achieve the Administration's vision of a comprehensive and coordinated approach, we recommended that the Assistant to the President for Homeland Security and Counterterrorism ensure that the governance structure proposed by the plan affords clear and adequate responsibility and authority to (a) provide monitoring and analysis of watch list screening efforts governmentwide, (b) respond to issues that hinder effectiveness, and (c) assess progress toward intended outcomes.

Agency Comments and Our Evaluation

We provided a draft of the restricted version of this report for comments to the Homeland Security Council, the Office of the Director of National Intelligence, and the Departments of Homeland Security, Justice, and State. We also provided relevant portions of a draft of the restricted version of this report for comments to the Social Security Administration. We received written responses from each entity, except for the Homeland Security Council.

In its response, DHS noted that it agreed with and supported our work and stated that it had already begun to address issues identified in our report's

findings. The response noted that DHS, working closely with the FBI and the Office of the Director of National Intelligence, has ongoing efforts to ensure that potential watch list vulnerabilities are identified and addressed and that watch list records and screening programs are appropriate. Also, DHS noted that at the time of our audit work, the department's Screening Coordination Office was relatively new—established in July 2006—but had subsequently added key staff and begun the critical work of advancing DHS screening programs and opportunities. According to DHS, the office has drafted initial guidelines to govern the use of watch list records to support private sector screening processes and is working with federal stakeholders to finalize this document, but the department did not provide specific plans and time frames for finalizing the guidelines. The department also noted that it works closely with all DHS and federal offices involved in screening initiatives and has begun appropriate outreach to the private sector. Further, DHS noted that its Screening Coordination Office is working within the department to advance a comprehensive approach to terrorist-related screening and that DHS would review and appropriately update the department's investment and implementation plans for screening opportunities. However, DHS did not specifically address our recommendations related to updating the governmentwide terrorist-related screening strategy and the investment and implementation plan, which is to include the scope, governance, principles, outcomes, milestones, training objectives, metrics, costs, and schedule of activities necessary for implementing the strategy. In our view, an updated strategy and plan are important for helping to ensure a coordinated and comprehensive approach to terrorist-related screening as called for in HSPD-11. The full text of DHS's written comments is reprinted in appendix V. DHS also provided technical comments, which we incorporated in this report where appropriate.

The FBI, responding on behalf of the Department of Justice, commented that the report correctly characterized the FBI's criteria for nominating individuals for inclusion on the watch list. Also, the FBI response noted that to ensure the protection of civil rights and prevent law enforcement officials from taking invasive enforcement action on individuals misidentified as being on the watch list, the Violent Gang and Terrorist Organization File is designed to not accept certain watch list records. The FBI explained that while law enforcement encounters of individuals on the watch list provide significant information, unnecessary detentions or queries of misidentified persons would be counterproductive and potentially damaging to the efforts of the FBI to investigate and combat terrorism. Because of these operational concerns, the FBI noted that our recommendation to assess the extent of vulnerabilities in current

screening processes that arise when the Violent Gang and Terrorist Organization File cannot accept certain watch list records has been completed and the vulnerability has been determined to be low or nonexistent. In our view, however, recognizing operational concerns does not constitute assessing vulnerabilities. Thus, while we understand the FBI's operational concerns, we maintain it is still important that the FBI assess to what extent vulnerabilities or security risks are raised by not screening against certain watch list records and what actions, if any, should be taken in response.

With respect to private sector screening, the FBI commented that it has assigned staff to assist the DHS Screening Coordination Office with drafting related screening guidelines. Finally, the FBI commented that the language of our recommendation related to governance of the watch-listing process may be interpreted to have some overlap with existing mandates carried out by TSC under HSPD-6. Specifically, the FBI noted that governance of the watch-listing process is better suited to be a component of TSC, rather than DHS. The FBI explained that DHS has no authority or provisions for establishing any watch-listing procedures for anyone other than DHS component agencies, whereas TSC has established a governance board composed of senior members from the nominating and screening agencies, the Office of the Director of National Intelligence, and the Homeland Security Council to monitor and update the watch listing process. The FBI further explained that these members meet regularly and address terrorist watch-listing issues ranging from nominations and encounters to dissemination of information and intelligence collected, and that all decisions approved by the governance board are presented at the Deputies Meeting chaired by the White House. The FBI believes this is the appropriate forum for obtaining a commitment from all of the entities involved in the watch-listing process.

We recognize that TSC and its governance board have played and will continue to play a central role in coordinating watch list-related activities governmentwide. However, as discussed in this report, TSC's governance board is currently responsible for providing guidance concerning issues within TSC's mission and authority and would need additional authority to provide effective coordination of terrorist-related screening activities and interagency issues governmentwide. We are not recommending that a new governance structure be created that overlaps with existing mandates or activities currently carried out by TSC and other entities. Rather, we are recommending that a governance structure be established that affords clear and adequate responsibility and authority to (a) provide monitoring and analysis of watch list screening efforts governmentwide, (b) respond

to issues that hinder effectiveness, and (c) assess progress toward intended outcomes. The FBI also provided technical comments, which we incorporated in this report where appropriate.

The Office of the Director of National Intelligence, the Department of State, and the Social Security Administration provided technical comments only, which we incorporated in this report where appropriate.

As arranged with your offices, we plan no further distribution of this report until 30 days after the date of this report. At that time, we will send copies of the report to interested congressional committees and subcommittees.

If you or your staff have any questions about this report or wish to discuss the matter further, please contact me at (202) 512-8777 or larencee@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Other key contributors to this report were Danny R. Burton, Virginia A. Chanley, R. Eric Erdman, Michele C. Fejfar, Jonathon C. Fremont, Kathryn E. Godfrey, Richard B. Hung, Thomas F. Lombardi, Donna L. Miller, Raul Quintero, and Ronald J. Salo.



Eileen Larence
Director, Homeland Security and Justice Issues

Appendix I: Objectives, Scope, and Methodology

Objectives

In response to a request from the Chairman and the Ranking Member of the Senate Committee on Homeland Security and Governmental Affairs, the Chairman and the Ranking Member of the Permanent Subcommittee on Investigations, and the Chairman and the Ranking Member of the House Committee on Homeland Security, we addressed the following questions:

- In general, what standards do the National Counterterrorism Center (NCTC) and the Federal Bureau of Investigation (FBI) use in determining which individuals are appropriate for inclusion on the Terrorist Screening Center's (TSC) consolidated watch list?
- Since TSC became operational in December 2003, how many times have screening and law enforcement agencies positively matched individuals to terrorist watch list records, and what do the results or outcomes of these encounters indicate about the role of the watch list as a counterterrorism tool?
- To what extent do the principal screening agencies whose missions most frequently and directly involve interactions with travelers check against all records in TSC's consolidated watch list? If the entire watch list is not being checked, why not, what potential vulnerabilities exist, and what actions are being planned to address these vulnerabilities?
- To what extent are Department of Homeland Security component agencies monitoring known incidents in which subjects of watch list records pass undetected through screening processes, and what corrective actions have been implemented or are being planned to address these vulnerabilities?
- What actions has the U.S. government taken to ensure that the terrorist watch list is used as effectively as possible, governmentwide and in other appropriate venues?

Scope and Methodology

In addressing these questions, we reviewed TSC's standard operating procedures and other relevant documentation, including statistics on screening encounters with individuals who were positively matched to terrorist watch list records, and we interviewed TSC officials, including the director and the principal deputy director. Further, we reviewed documentation and interviewed senior officials from the FBI's Counterterrorism Division and the principal screening agencies whose missions most frequently and directly involve interactions with travelers. Specifically, at the Transportation Security Administration (TSA), we

examined the screening of air passengers prior to their boarding a flight; at U.S. Customs and Border Protection (CBP), we examined the screening of travelers entering the United States through ports of entry; and at the Department of State, we examined the screening of nonimmigrant visa applicants. We also visited a nonprobability sample of screening agencies and investigative agencies in geographic areas of four states (California, Michigan, New York, and Texas).¹ We chose these locations on the basis of geographic variation and other factors. More details about the scope and methodology of our work regarding each of the objectives are presented in the following sections, respectively.

Standards Used by NCTC and the FBI in Determining Which Individuals Are Appropriate for Inclusion on TSC's Consolidated Watch List

To ascertain the general standards used in determining which individuals are appropriate for inclusion on TSC's consolidated watch list, we reviewed available documentation. In particular, we reviewed

- Homeland Security Presidential Directive 6, which specifies that TSC's consolidated watch list is to contain information about individuals "known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism;"²
- an NCTC document on building a single database of known and suspected terrorists for the U.S. government, which provides NCTC's standards for including individuals on the watch list;
- the *Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection*, which provide standards for opening FBI international terrorism investigations; and
- the *Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorist Enterprise Investigations*, which provide standards for opening FBI domestic terrorism investigations.

We discussed implementation of applicable guidance with responsible NCTC and FBI Counterterrorism Division officials. However, we did not

¹Results from nonprobability samples cannot be used to make inferences about a population, because in a nonprobability sample some elements of the population being studied have no chance or an unknown chance of being selected as part of the sample.

²The White House, *Homeland Security Presidential Directive/HSPD-6, Subject: Integration and Use of Screening Information* (Washington, D.C.: Sept. 16, 2003).

audit or evaluate agencies' compliance with the guidance. For instance, we did not review or assess the derogatory information related to terrorist watch list records, partly because such information involved ongoing counterterrorism investigations. Also, a primary agency that collects information on known or suspected terrorists—the Central Intelligence Agency—declined to meet with us or provide us with documentation on its watch list-related activities.

Number of Times That Screening and Law Enforcement Agencies Have Positively Matched Individuals to the Watch List: Results or Outcomes

From TSC, we obtained statistics on the number of positive encounters, that is, the number of times that individuals have been positively matched during screening against terrorist watch list records. Generally, the statistics cover the period from December 2003 (when TSC began operations) through May 2007. To the extent possible on the basis of available information, we worked with the applicable agencies (particularly the FBI, CBP, TSA, and the Department of State) to quantify the results or outcomes of these positive encounters—which included actions ranging from arrests and visa denials to questioning and releasing individuals. Further, we inquired about the existence and resolution of any issues regarding interagency collaboration in managing encounters with individuals on the terrorist watch list. Moreover, in our interviews with officials at TSC and the frontline screening agencies and in the law enforcement and intelligence communities, we obtained perspectives on whether (and how) watch list screening has enhanced the U.S. government's counterterrorism efforts.

Extent That Screening and Law Enforcement Agencies Check against All Records in the TSC's Consolidated Watch List

We determined from TSC what subsets of records from the consolidated watch list are exported for use by the respective frontline screening agencies and law enforcement. Each day, TSC exports subsets of the consolidated watch list to federal government databases used by agencies that conduct terrorism-related screening. Specifically, we focused on exports of records to the following agencies' databases:

- **Department of Homeland Security's Interagency Border Inspection System.** Among other users, CBP officers use the Interagency Border Inspection System to screen travelers entering the United States at international ports of entry, which include land border crossings along the Canadian and Mexican borders, sea ports, and U.S. airports for international flight arrivals.
- **Department of State's Consular Lookout and Support System.** This system is the primary sensitive but unclassified database used by

consular officers abroad to screen the names of visa applicants to identify terrorists and other aliens who are potentially ineligible for visas based on criminal histories or other reasons specified by federal statute.

- **FBI’s Violent Gang and Terrorist Organization File.** This file, which is a component of the FBI’s National Crime Information Center, is accessible by federal, state, and local law enforcement officers for screening in conjunction with arrests, detentions, or other criminal justice purposes.
- **TSA’s No Fly and Selectee lists.** TSA provides updated No Fly and Selectee lists to airlines for use in prescreening passengers. Through the issuance of security directives, the agency requires that airlines use these lists to screen passengers prior to boarding.

The scope of our work included inquiries regarding why only certain records are exported for screening rather than use of the entire consolidated watch list by all agencies. At TSC and the frontline screening agencies, we interviewed senior officials and we reviewed mission responsibilities, standard operating procedures, and documentation regarding the technical capabilities of the respective agency’s database.

Extent That Screening Agencies Monitor Incidents in Which Subjects of Watch List Records Pass Undetected through Screening Processes; Corrective Actions Implemented or Planned to Address Vulnerabilities

We inquired about incidents of subjects of watch list records who were able to pass undetected through screening conducted by the various frontline screening agencies or, at TSA direction, airlines. More specifically, we reviewed available documentation and interviewed senior officials at the FBI, CBP, TSA, U.S. Citizenship and Immigration Services, and the Department of State regarding the frequency of such incidents and the causes, as well as what corrective actions have been implemented or planned to address vulnerabilities.

Actions the U.S. Government Has Taken to Ensure That the Terrorist Watch List Is Used as Effectively as Possible

Regarding actions taken by the U.S. government to ensure the effective use of the watch list, we reviewed Homeland Security Presidential Directive 6 and Homeland Security Presidential Directive 11, which address the integration and use of screening information and comprehensive terrorist-related screening procedures. Generally, these directives require federal departments and agencies to identify all appropriate opportunities or processes that should use the terrorist watch list. We did not do an independent evaluation of whether all screening opportunities were identified. Rather, to determine the implementation status of these directives, we reviewed available documentation and interviewed senior officials at the Departments of Homeland Security, Justice, and State, as well as TSC and the Social Security Administration. Our inquiries covered domestic screening opportunities within the federal community and critical infrastructure sectors of private industry. Further, our inquiries covered international opportunities, that is, progress made in efforts to exchange terrorist watch list information with trusted foreign partners on a reciprocal basis. Finally, we compared the status of watch list-related strategies, planning, and initiatives with the expectations set forth in Homeland Security Presidential Directive 6 and Homeland Security Presidential Directive 11. The Homeland Security Council—which is chaired by the Assistant to the President for Homeland Security and Counterterrorism—denied our request for an interview.³

Data Reliability

Regarding statistical information we obtained from TSC and screening agencies—such as the number of positive matches and actions taken—we discussed the sources of the data with agency officials and reviewed documentation regarding the compilation of the statistics. We determined that the statistics were sufficiently reliable for the purposes of this review.

³The Homeland Security Council was established to ensure coordination of all homeland security-related activities among executive departments and agencies and promote the effective development and implementation of all homeland security policies. See the White House, *Homeland Security Presidential Directive/HSPD-1, Subject: Organization and Operation of the Homeland Security Council* (Washington, D.C.: Oct. 29, 2001).

We did not review or assess the derogatory information related to terrorist watch list records, primarily because such information involved ongoing counterterrorism investigations or intelligence community activities.

We performed our work on the restricted version of this report from April 2005 through September 2007 in accordance with generally accepted government auditing standards.

Appendix II: Homeland Security Presidential Directive/HSPD-6 (Sept. 16, 2003)



For Immediate Release
Office of the Press Secretary
September 16, 2003

Homeland Security Presidential Directive/Hspd-6

Subject: Integration and Use of Screening Information

To protect against terrorism it is the policy of the United States to (1) develop, integrate, and maintain thorough, accurate, and current information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism (Terrorist Information); and (2) use that information as appropriate and to the full extent permitted by law to support (a) Federal, State, local, territorial, tribal, foreign-government, and private-sector screening processes, and (b) diplomatic, military, intelligence, law enforcement, immigration, visa, and protective processes.

This directive shall be implemented in a manner consistent with the provisions of the Constitution and applicable laws, including those protecting the rights of all Americans.

To further strengthen the ability of the United States Government to protect the people, property, and territory of the United States against acts of terrorism, and to the full extent permitted by law and consistent with the policy set forth above:

- (1) The Attorney General shall establish an organization to consolidate the Government's approach to terrorism screening and provide for the appropriate and lawful use of Terrorist Information in screening processes.
- (2) The heads of executive departments and agencies shall, to the extent permitted by law, provide to the Terrorist Threat Integration Center (TTIC) on an ongoing basis all appropriate Terrorist Information in their possession, custody, or control. The Attorney General, in coordination with the Secretary of State, the Secretary of Homeland Security, and the Director of Central Intelligence shall implement appropriate procedures and safeguards with respect to all such information about United States persons. The TTIC will provide the organization referenced in paragraph (1) with access to all appropriate information or intelligence in the TTIC's custody, possession, or control that the organization requires to perform its functions.
- (3) The heads of executive departments and agencies shall conduct screening using such information at all appropriate opportunities, and shall report to the Attorney General not later than 90 days from the date of this directive, as to the opportunities at which such screening shall and shall not be conducted.
- (4) The Secretary of Homeland Security shall develop guidelines to govern the use of such information to support State, local, territorial, and tribal screening processes, and private sector screening processes that have a substantial bearing on homeland security.
- (5) The Secretary of State shall develop a proposal for my approval for enhancing cooperation with certain foreign governments, beginning with those countries for which the United States has waived visa requirements, to establish appropriate access to terrorism screening information of the participating governments.

This directive does not alter existing authorities or responsibilities of department and agency heads to carry out operational activities or provide or receive information. This directive is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees or agents, or any other person.

**Appendix II: Homeland Security Presidential
Directive/HSPD-6 (Sept. 16, 2003)**

The Attorney General, in consultation with the Secretary of State, the Secretary of Homeland Security, and the Director of Central Intelligence, shall report to me through the Assistant to the President for Homeland Security not later than October 31, 2003, on progress made to implement this directive and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate.

GEORGE W. BUSH

###

Appendix III: Homeland Security Presidential Directive/HSPD-11 (Aug. 27, 2004)



For Immediate Release
Office of the Press Secretary
August 27, 2004

Homeland Security Presidential Directive/Hspd-11

Subject: Comprehensive Terrorist-Related Screening Procedures

(1) In order more effectively to detect and interdict individuals known or reasonably suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism ("suspected terrorists") and terrorist activities, it is the policy of the United States to:

(a) enhance terrorist-related screening (as defined below) through comprehensive, coordinated procedures that detect, identify, track, and interdict people, cargo, conveyances, and other entities and objects that pose a threat to homeland security, and to do so in a manner that safeguards legal rights, including freedoms, civil liberties, and information privacy guaranteed by Federal law, and builds upon existing risk assessment capabilities while facilitating the efficient movement of people, cargo, conveyances, and other potentially affected activities in commerce; and

(b) implement a coordinated and comprehensive approach to terrorist-related screening -- in immigration, law enforcement, intelligence, counterintelligence, and protection of the border, transportation systems, and critical infrastructure -- that supports homeland security, at home and abroad.

(2) This directive builds upon HSPD-6, "Integration and Use of Screening Information to Protect Against Terrorism." The Terrorist Screening Center (TSC), which was established and is administered by the Attorney General pursuant to HSPD-6, enables Government officials to check individuals against a consolidated Terrorist Screening Center Database. Other screening activities underway within the Terrorist Threat Integration Center (TTIC) and the Department of Homeland Security further strengthen the ability of the United States Government to protect the people, property, and territory of the United States against acts of terrorism.

(3) In this directive, the term "terrorist-related screening" means the collection, analysis, dissemination, and use of information related to people, cargo, conveyances, and other entities and objects that pose a threat to homeland security. Terrorist-related screening also includes risk assessment, inspection, and credentialing.

(4) Not later than 75 days after the date of this directive, the Secretary of Homeland Security, in coordination with the Attorney General, the Secretaries of State, Defense, Transportation, Energy, Health and Human Services, Commerce, and Agriculture, the Directors of Central Intelligence and the Office of Management and Budget, and the heads of other appropriate Federal departments and agencies, shall submit to me, through the Assistant to the President for Homeland Security, a report setting forth plans and progress in the implementation of this directive, including as further described in sections 5 and 6 of this directive.

(5) The report shall outline a strategy to enhance the effectiveness of terrorist-related screening activities, in accordance with the policy set forth in section 1 of this directive, by developing comprehensive, coordinated, systematic terrorist-related screening procedures and capabilities that also take into account the need to:

(a) maintain no less than current levels of security created by existing screening and protective measures;

(b) encourage innovations that exceed established standards;

(c) ensure sufficient flexibility to respond rapidly to changing threats and priorities;

**Appendix III: Homeland Security Presidential
Directive/HSPD-11 (Aug. 27, 2004)**

- (d) permit flexibility to incorporate advancements into screening applications and technology rapidly;
 - (e) incorporate security features, including unpredictability, that resist circumvention to the greatest extent possible;
 - (f) build upon existing systems and best practices and, where appropriate, integrate, consolidate, or eliminate duplicative systems used for terrorist-related screening;
 - (g) facilitate legitimate trade and travel, both domestically and internationally;
 - (h) limit delays caused by screening procedures that adversely impact foreign relations, or economic, commercial, or scientific interests of the United States; and
 - (i) enhance information flow between various screening programs.
- (6) The report shall also include the following:
- (a) the purposes for which individuals will undergo terrorist-related screening;
 - (b) a description of the screening opportunities to which terrorist-related screening will be applied;
 - (c) the information individuals must present, including, as appropriate, the type of biometric identifier or other form of identification or identifying information to be presented, at particular screening opportunities;
 - (d) mechanisms to protect data, including during transfer of information;
 - (e) mechanisms to address data inaccuracies, including names inaccurately contained in the terrorist screening data consolidated pursuant to HSPD-6;
 - (f) the procedures and frequency for screening people, cargo, and conveyances;
 - (g) protocols to support consistent risk assessment and inspection procedures;
 - (h) the skills and training required for the screeners at screening opportunities;
 - (i) the hierarchy of consequences that should occur if a risk indicator is generated as a result of a screening opportunity;
 - (j) mechanisms for sharing information among screeners and all relevant Government agencies, including results of screening and new information acquired regarding suspected terrorists between screening opportunities;
 - (k) recommended research and development on technologies designed to enhance screening effectiveness and further protect privacy interests; and
 - (l) a plan for incorporating known traveler programs into the screening procedures, where appropriate.
- (7) Not later than 90 days after the date of this directive, the Secretary of Homeland Security, in coordination with the heads of the Federal departments and agencies listed in section 4 of this directive, shall also provide to me, through the Assistant to the President for Homeland Security and the Director of the Office of Management and Budget, a prioritized investment and implementation plan for a systematic approach to terrorist-related screening that optimizes detection and interdiction of suspected terrorists and terrorist activities. The plan shall describe the scope, governance, principles, outcomes, milestones, training objectives, metrics, costs, and schedule of activities to implement the policy set forth in section 1 of this directive. The Secretary of Homeland Security shall further provide a report on the status of the implementation of the plan to me through the Assistant to the President for Homeland Security 6 months after the date of this directive and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate.

**Appendix III: Homeland Security Presidential
Directive/HSPD-11 (Aug. 27, 2004)**

(8) In order to ensure comprehensive and coordinated terrorist-related screening procedures, the implementation of this directive shall be consistent with Government-wide efforts to improve information sharing. Additionally, the reports and plan required under sections 4 and 7 of this directive shall inform development of Government-wide information sharing improvements.

(9) This directive does not alter existing authorities or responsibilities of department and agency heads including to carry out operational activities or provide or receive information. This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees, or agents, or any other person.

GEORGE W. BUSH

###

Appendix IV: Outcomes of Screening Agency Encounters with Individuals on the Terrorist Watch List

This appendix presents details on the outcomes of screening agency encounters with individuals on the terrorist watch list. Specifically, the following sections provide information on arrests and other outcomes of encounters involving the Department of State, TSA, CBP, and state or local law enforcement.

Subjects of Watch List Records Have Been Arrested Hundreds of Times, with Some Arrests Based on Terrorism Grounds

According to TSC data, for the period December 2003 through May 2007, agencies reported arresting subjects of watch list records for various reasons hundreds of times, such as the individual having an outstanding arrest warrant or the individual's behavior or actions during the encounter. For this period, TSC data also indicated that some of the arrests were based on terrorism grounds. For example, according to TSC, in November 2004, the subject of a watch list record was encountered at the El Paso, Texas, border crossing by CBP and U.S. Immigration and Customs Enforcement agents and subsequently arrested as a result of their interview with the person. According to TSC, the arrest was done in conjunction with the FBI on grounds of material support to terrorism. In January 2007, TSC officials told us that—because of the difficulty in collecting information on the basis of arrests—the center has changed its policy on documentation of arrests and no longer categorizes arrests as terrorism-related. As such, the number of times individuals on the watch list have been arrested based on terrorism grounds is no longer being tracked.

Subjects of Watch List Records Were Denied Visas and Also Granted Visas

U.S. consulates and embassies around the world are required to screen the names of all visa applicants against the Department of State's Consular Lookout and Support System and to notify TSC when the applicant's identifying information matches or closely matches information in a terrorist watch list record.¹ For positive matches, officials at Department of State headquarters are to review available derogatory information and provide advice to the consular officer, who is responsible for deciding whether to grant or refuse a visa to the applicant under the immigration laws and regulations of the United States. According to TSC data, when visa applicants were positively matched to terrorist watch list records, the outcomes included visas denied, visas issued (because the consular officer

¹Department of State officials assigned to TSC handle all referrals from consulates and embassies.

did not find any statutory basis for inadmissibility), and visa ineligibility waived.²

The Department of State described several scenarios under which an individual on the terrorist watch list might still be granted a visa. According to the department, visas can be issued following extensive interagency consultations regarding the individuals who were matched to watch list records. The department explained that the information that supports a terrorist watch list record is often sparse or inconclusive. It noted, however, that having these records exported to the Consular Lookout and Support System provides an opportunity for a consular officer to question the alien to obtain additional information regarding potential inadmissibility. For instance, there might be a record with supporting information showing that the person attended a political rally addressed by radical elements. According to the Department of State, while this activity may raise suspicion about the individual, it also requires further development and exploration of the person's potential ability to receive a visa. Thus, using watch list records allows the department to develop information and pursue a thorough interagency vetting process before coming to a final conclusion about any given prospective traveler who is the subject of a watch list record.

Further, individuals can receive a waiver of inadmissibility from the Department of Homeland Security. According to the Department of State, there may be U.S. government interest in issuing a visa to someone who has a record in the terrorist watch list and who may have already been found ineligible for a visa or inadmissible to the United States. For instance, an individual might be a former insurgent who has become a foreign government official. This person might be invited to the United States to participate in peace talks under U.S. auspices. According to the Department of State, in such a case, the visa application would go through normal processing, which would include a review of the derogatory information related to the terrorist watch list record. This information, along with the request for a waiver, would be passed to the Department of Homeland Security, which normally grants waivers recommended by the Department of State.

²In this context, ineligibility waived refers to individuals who were ineligible for a visa based on terrorism grounds, but DHS approved a waiver for a one-time visit or multiple entries into the United States. In general, waivers are approved when the U.S. government has an interest in allowing the individual to enter the United States, such as an individual on the terrorist watch list who is invited to participate in peace talks under U.S. auspices.

Another scenario under which an individual on the terrorist watch list might still be granted a visa involves instances where a watch list record is not exported to the Department of State's Consular Lookout and Support System. According to the department, originating agencies that nominate terrorist watch list records occasionally ask TSC to not export a record to the Department of State's system for operational reasons, such as to not alert the individuals about an ongoing investigation. In this case, if a terrorist watch list record is not exported to the Consular Lookout and Support System database, a consular officer will not be notified of the record and may otherwise proceed in adjudicating the visa without consulting Department of State officials in Washington, D.C.

Passengers Were Matched to the No Fly and Selectee Lists

TSA requires aircraft operators to screen the names of all passengers against extracts from TSC's consolidated watch list to help ensure that individuals who pose a threat to civil aviation are denied boarding or subjected to additional screening before boarding, as appropriate. Specifically, TSA provides the No Fly and Selectee lists to airlines for use in prescreening passengers. According to TSA policy, if a situation arises in which a person on the No Fly list is erroneously permitted to board a flight, upon discovery, that flight may be diverted to a location other than its original destination.

According to TSA data, when airline passengers were positively matched to the No Fly or Selectee lists, the vast majority of matches were to the Selectee list. Other outcomes included individuals matched to the No Fly list and denied boarding (did not fly) and individuals matched to the No Fly list after the aircraft was in-flight. Regarding the latter, TSA officials explained that there have been situations in which individuals on the No Fly list have passed undetected through airlines' prescreening of passengers and flew on international flights bound to or from the United States. These individuals were subsequently identified in-flight by other means—specifically, screening of passengers conducted by CBP.

Many Nonimmigrant Aliens on the Watch List Were Refused Entry into the United States, but Most Were Allowed to Enter

CBP officers at U.S. ports of entry use the Interagency Border Inspection System to screen the names of individuals entering the United States against terrorist watch list records.³ Specifically, all individuals entering the United States at seaports and U.S. airports for international flight arrivals are to be checked against watch list records. At land border ports of entry, screening against watch list records depends on the volume of traffic and other operational factors.

While U.S. citizens who have left the United States and seek to reenter may be subjected to additional questioning and physical screening to determine any potential threat they pose, they may not be excluded and must be admitted upon verification of citizenship (for example, by presenting a U.S. passport).⁴ Alien applicants for admission are questioned by CBP officers, and their documents are examined to determine admissibility based on requirements of the Immigration and Nationality Act.⁵ For nonimmigrant aliens who are positively matched to a terrorist watch list record, officials at CBP are to review available derogatory information related to the watch list record and advise port officers regarding whether sufficient information exists to refuse admission under terrorism or other grounds. CBP officers at ports of entry are ultimately responsible for making determinations regarding whether an individual should be admitted or denied entry into the United States.

According to CBP policies, CBP officers at the port of entry are required to apprise the local FBI Joint Terrorism Task Force and the local U.S. Immigration and Customs Enforcement of all watch list encounters, regardless of the individual's citizenship and whether or not the person is refused admission into the United States. If the individual is a U.S. citizen or an admitted non-citizen, CBP officers at the port are to apprise the local Joint Terrorism Task Force of any suspicions about the person after questioning, in order to permit post-entry investigation or surveillance.

³U.S. ports of entry include land border crossings along the Canadian and Mexican borders, seaports, and U.S. airports for international flight arrivals.

⁴See 8 C.F.R. § 235.1. Similarly, lawful permanent residents are generally not regarded as seeking admission to the United States and, like U.S. citizens, are not subject to the grounds for inadmissibility unless they fall within certain criteria listed at 8 U.S.C. § 1011(a)(13)(C) that describe why an alien lawfully admitted for permanent residence would be regarded as seeking admission.

⁵See 8 U.S.C. § 1182 (codifying section 212 of the Immigration and Nationality Act, as amended).

According to CBP data, a number of nonimmigrant aliens encountered at U.S. ports of entry were positively matched to terrorist watch list records. For many of the encounters, CBP determined there was sufficient derogatory information related to the watch list records to preclude admission under terrorism grounds in the Immigration and Nationality Act, and the individuals were refused entry. However, for most of the encounters, CBP determined there was not sufficient derogatory information related to terrorist watch list records to refuse admission on terrorism-related grounds in the Immigration and Nationality Act. According to CBP, the center did not know how many times these encounters ultimately resulted in individuals being admitted or denied entry into the United States. The officials explained that after in-depth questioning and inspection of travel documents and belongings, CBP officers could still have refused individuals the right to enter the United States based on terrorism-related or other grounds set forth in the Immigration and Nationality Act, such as immigration violations.

Watch List Records Related to State and Local Encounters Indicate the Vast Majority of Subjects Were Released

To assist state and local officials during encounters, all watch list records in the FBI's Violent Gang and Terrorist Organization File contain a specific category or handling code and related instructions about actions that may be taken in response to a positive watch list encounter.⁶ These actions may include—in appropriate and lawfully authorized circumstances—arresting, detaining, or questioning and then releasing the individual. State and local officials are to contact TSC when the names of individuals queried match or closely match a terrorist watch list record in the Violent Gang and Terrorist Organization File. For positive or inconclusive matches, TSC is to refer the matter to the FBI's Counterterrorism Division, which provides specific instructions to state and local officials about appropriate actions that may be taken or questions that should be asked.

According to TSC data, state or local law enforcement officials have encountered individuals who were positively matched to terrorist watch list records in the Violent Gang and Terrorist Organization File thousands of times. Although data on the actual outcomes of these encounters were not available, the vast majority involved watch list records that indicated

⁶The FBI's Violent Gang and Terrorist Organization File contains terrorist watch list records and records involving gang-related activities that do not meet the terrorism-related standard for inclusion in TSC's consolidated watch list. Screening officials are to notify TSC only when there is a positive match to a terrorist record in the file.

**Appendix IV: Outcomes of Screening Agency
Encounters with Individuals on the Terrorist
Watch List**

that the individuals were released, unless there were other reasons for arresting or detaining the individual.

Appendix V: Comments from the Department of Homeland Security

Note: GAO-07-1206 is the previous number for this report.

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

US GAO

2007 SEP -7 AM 10: 54



Homeland
Security

September 4, 2007

Ms Eileen Larence
Director
Homeland Security and Justice Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms Larence:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO's) draft report GAO-07-1206 entitled *TERRORIST WATCH LIST SCREENING: Opportunities Exist to Enhance Management Oversight, Reduce Vulnerabilities in Agency Screening Processes, and Expand Use of the List*.

The implementation and use of the Terrorist Watch List has enhanced the Department of Homeland Security's (DHS's) screening programs. The use of this single tool across all federal, state and local law enforcement agencies has become one of our most valuable resources in our coordinated fight against terrorist activity. The Department agrees with and supports the work performed by GAO and has already begun work to correct issues identified in the report findings.

DHS works closely with the FBI and the Office of the Director of National Intelligence to review watch list opportunities, enhancements, and potential vulnerabilities. DHS acts as a partner to ensure that vulnerabilities are identified and addressed and that watch list records and screening programs are appropriate. This is an on-going effort.

DHS established the Screening Coordination Office (SCO) in July 2006 to enhance security measures by integrating the Department's terrorist and immigration related screening efforts, creating unified screening standards and policies, and developing a single redress process for travelers. At the time of the audit work, this office was relatively new, but it has subsequently added key staff and begun the critical work of advancing DHS screening programs and opportunities. The SCO has drafted initial guidelines to govern the use of watch list records to support private-sector screening processes and is in the process of working with federal stakeholders to finalize this document. The SCO also works closely with all DHS and federal offices involved in screening initiatives and has begun appropriate outreach to the private sector.

www.dhs.gov

**Appendix V: Comments from the Department
of Homeland Security**

DHS has completed and submitted the HSPD-11 required reports concerning the screening investment plan and implementation plans. The DHS Screening Coordination Office is working across the Department to advance a comprehensive approach to terrorist-related screening, as specified in the HSPD-11 report. As recommended, DHS will review and appropriately update the DHS investment and implementation plans for screening opportunities. We will also continue to work closely with our federal partners to advance screening opportunities and we appreciate the work done by the GAO audit team.

Thank you again for the opportunity to comment on this draft report and we look forward to working with you on future homeland security issues.

Sincerely,



Steven J. Pecinovsky
Director
Departmental GAO/OIG Liaison Office

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

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

Public Affairs

Susan Becker, Acting Manager, BeckerS@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548