AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. Hrg. 110–621

WATCHING THE WATCH LIST: BUILDING AN EFFECTIVE TERRORIST SCREENING SYSTEM

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

OCTOBER 24, 2007

Available via http://www.gpoaccess.gov/congress/index.html

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

38–989 PDF WASHINGTON : 2008

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
BARACK OBAMA, Illinois
CLAIRE McCASKILL, Missouri
JON TESTER, Montana

SUSAN M. COLLINS, Maine
TED STEVENS, Alaska
GEORGE V. VOINOVICH, Ohio
NORM COLEMAN, Minnesota
TOM COBURN, Oklahoma
PETE V. DOMENICI, New Mexico
JOHN WARNER, Virginia
JOHN E. SUNUNU, New Hampshire

MICHAEL L. ALEXANDER, *Staff Director*
CHRISTIAN J. BECKNER, *Professional Staff Member*
BRANDON L. MILHORN, *Minority Staff Director and Chief Counsel*
ROBERT L. STRAYER, *Minority Director for Homeland Security*
JOHN K. GRANT, *Minority Professional Staff Member*
TRINA DRIESSNACK TYRER, *Chief Clerk*

CONTENTS

	Page
Opening statements:	
Senator Lieberman	1
Senator Collins	3
Senator Tester	19
Senator Voinovich	21
Senator Warner	23
Senator Carper	23
Senator Levin	27

WITNESSES

WEDNESDAY, OCTOBER 24, 2007

Eileen R. Larence, Director, Homeland Security and Justice Issues, U.S. Government Accountability Office	5
Hon. Glenn A. Fine, Inspector General, U.S. Department of Justice	8
Leonard C. Boyle, Director, Terrorist Screening Center, Federal Bureau of Investigation, U.S. Department of Justice	10
Paul Rosenzweig, Deputy Assistant Secretary for Policy, U.S. Department of Homeland Security	13

ALPHABETICAL LIST OF WITNESSES

Boyle, Leonard C.:	
Testimony	10
Prepared statement	65
Fine, Hon. Glenn A.:	
Testimony	8
Prepared statement	54
Larence, Eileen R.:	
Testimony	5
Prepared statement	37
Rosenzweig, Paul:	
Testimony	13
Prepared statement	71

APPENDIX

"Promoting Accuracy and Fairness in the Use of Government Watch Lists, Statement of the Constitution Project's Liberty and Security Initiative," The Constitution Project, December 5, 2006	78
U.S. Government Accountability Office, Report to Congressional Requestors, "Terrorist Watch List Screening: Opportunities Exist to Enhance Management Oversight, Reduce Vulnerabilities in Agency Screening Processes, and Expand Use of the List," October 2007	87
U.S. Department of Justice, Office of the Inspector General, Audit Division, "Follow-Up Audit of the Terrorist Screening Center," Audit Report 07–41, September 2007	169
Questions and responses for the record from:	
Ms. Larence	275
Mr. Fine	278
Mr. Boyle	284
Mr. Rosenzweig	293

WATCHING THE WATCH LIST: BUILDING AN EFFECTIVE TERRORIST SCREENING SYSTEM

WEDNESDAY, OCTOBER 24, 2007

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:02 a.m., in Room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Levin, Carper, Tester, Collins, Voinovich, and Warner.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. Good morning. In this hearing, we continue this Committee's oversight of our homeland security programs that have been created since September 11, 2001. Last week, we had one on port security. Yesterday, we had another interesting hearing on an aspect that we still need some help on. And today, we go to one where we have made some progress, although we still have some questions, and this is our focus on the terrorist watch list—a critical tool in our battle to keep terrorists from entering the United States and attacking our homeland again as they did on September 11, 2001.

After September 11, 2001, we found as part of the investigation of how that event occurred that lists of suspected or potential terrorists that were in the possession of the Federal Government, many different Federal agencies, were, however, not shared, and certainly not shared in a way that increased deterrence of a terrorist attack. As a result, we now know that two of the September 11, 2001, hijackers—Nawaf al-Hazmi and Khalid al-Mihdhar—were known to the CIA and NSA and were regarded as dangerous by both agencies. But that information was never shared with the Immigration and Naturalization Service or the State Department, and therefore, these two terrorists were allowed to enter our country and be part of carrying out the most devastating attack on our homeland in our history.

The Terrorist Screening Center, operated by the FBI, was created in December 2003, to state it simply, to make sure that nothing like that ever happened again. Its mission was to pull together all the different lists of potential terrorists into one master list and to make sure that everyone who needed that information to protect our homeland had easy access to it. This master list is used as the basis for the creation of separate databases used by a number of

Federal agencies today, including as TSA's No Fly List and the State Department's CLASS list or database, which is used to screen visa applicants. The terrorism watch list is also a vital tool State and local law enforcement can now access, creating a powerful new link to generate leads on potential terrorists within our country because of the access that hundreds of thousands of State and local law enforcement officers have to that list.

This is a vast improvement over where we were before and on September 11, 2001. I want to thank the Terrorist Screening Center, the National Counterterrorism Center, the Department of Homeland Security, and other Federal agencies for the significant progress they have made over the last 4 years in closing this previous gap in our homeland security.

The Government Accountability Office reports today in a report that we are releasing on this progress.[1] But it also discusses some remaining vulnerabilities and weaknesses in the watch list system which we will want to discuss. The Department of Justice Inspector General, also appearing before us today, has found similar problems in the watch list system in his audits of the Terrorist Screening Center.

Some of the concerns that we are going to discuss stem from the sheer size of the list. It contained 158,000 names in July 2004. That grew to 755,000 names by May of this year, and it now stands at about 860,000 names. That is nearly a 500-percent increase in 3 years. Of course, if there is a good reason to have each of those names there, the increase in the size of the list is good news for our homeland security. But if many of these names are mistakenly there, the credibility of the terrorism watch list and its usefulness will be compromised. So we want to talk about that.

I know that the Terrorist Screening Center has undertaken efforts to review portions of the watch list, such as the entire No Fly List, and has a long-term plan to review the entire watch list. But with the list likely to go over 1 million names in the near future, we need to know that there are clear standards for placing names on it and, of course, for taking them off it.

Another concern expressed by the Department of Justice—and I guess I would say the traveling public, or some of it—is providing an appeal for individuals who are caught in the watch list system because they have the same name or a similar name to someone who deserves to be on the list.

The most famous of these cases is our own colleague, Senator Edward M. Kennedy, famously denied boarding on different airline flights because his name resembled that of an IRA terrorist. It took weeks to get this cleared up. I am going to try to avoid humor here because this is a serious subject. But it is essential that we have a redress system that is easy for people to navigate and can quickly resolve problems of mistaken identity without, of course, weakening the terrorist watch lists and their utility.

Now, on the other side of the spectrum, the GAO report does cite some cases where people whose names were justifiably on the watch list have, nonetheless, been admitted into our country by Customs and Border Protection and cases where people on the No

[1] The GAO Report on "Terrorist Watch List Screening" appears in the Appendix on page 87.

Fly List have been allowed to board international flights traveling to the United States. That, of course, is the most serious of all vulnerabilities that could exist in this system.

So, bottom line, the picture I believe we are going to see today and the testimony we are going to hear and the questions we are going to ask, I think, will be around this reality. We have a new system in place. It is a great improvement over what existed before, but there are still occasions when that system lets in people who are on the watch list and keeps out people who should not be on the list. And, of course, all of us want to fix those vulnerabilities. But it is with appreciation for all that you have done that I welcome the witnesses and that I call on the Committee's Ranking Member now, Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman, and let me begin by commending you for holding this hearing. I think continuing oversight by this Committee is so important, and this is certainly an issue that directly affects the security of our country, but also affects our constituents day in and day out.

The use of the terrorist watch list inspires both confidence and concern—confidence that our counterterrorism agencies are determined to detect and disrupt the travels of those who would do us harm, but also concern that this increased security may come at a cost to privacy and civil liberties.

As the Chairman indicated, the 9/11 Commission noted that as many as 15 of the 19 hijackers might have been intercepted by border authorities if a procedure had been in place to link previously accumulated information to their names. Several of the hijackers had been cited in intelligence community files for terrorist links. Existing but untapped data on travel patterns, bogus visa applications, and fraudulent passport information could have focused official attention on some of the terrorists. Prior to the attacks of September 11, 2001, however, the government simply had no such consolidated system.

Based on its investigation, the 9/11 Commission recommended that the Federal Government design a comprehensive screening system to help front-line officials at our borders and other critical points confirm the identity of people trying to enter our country or to board airplanes and to disrupt their plans if they pose a security threat.

The need for effective information sharing and for tools to track terrorists' movements is self-evident. But if these databases contain information that is inaccurate, obsolete, or error-prone, then watch lists can prove to be both ineffective and unfair. Suspects who pose a security threat can pass unimpeded if they are not listed or if technical problems prevent their identification.

On the other hand, all of us have heard from innocent constituents who have had the misfortune to share a similar name or other identifying data with a suspect on the watch list. Individuals who do not belong on the list can face frustrating delays every time they travel, and as Senator Kennedy and others have found, it can be very difficult to get erroneous information corrected. In addition,

volumes of personal information in the hands of government can present a tempting target for identity thieves.

Creating and maintaining a comprehensive terrorist watch list is an enormous endeavor fraught with technical and tactical challenges. On the technical side, integrating information from multiple government databases and then transmitting that information securely and accurately is no easy task. To be useful to our officers in the field, the watch list must provide reliable and accurate information that can be quickly evaluated and then used as a basis for action.

The GAO report[1] that we release today and the DOJ Inspector General's report[2] that we received last month provide us with the means to review the screening process and assess its strengths and weaknesses.

The GAO report details the use of the watch lists by law enforcement over a 42-month period. Federal, State, and local officials had more than 53,000 encounters with individuals on the watch lists during that period.

Unfortunately, as the Chairman mentioned, there are troubling examples of targeted individuals passing through screening undetected. We also have the more recent, very troubling case where Customs and Border Protection allowed an individual from Mexico who was infected with a dangerous strain of TB to pass across the border several times.

A particularly troubling problem has been the failure to detect individuals on the No Fly List before they board a U.S.-bound aircraft overseas. In some cases, the government's response to delayed detection has resulted in planes being diverted for an emergency landing—almost always, they seem to get diverted to Bangor, Maine—so that a suspicious individual can be questioned, detained, or refused entry. And perhaps the most recent example of that happening that resonated with people my age was when Cat Stevens was on the plane that was diverted to Bangor, Maine.

These reports underscore the need to make the watch lists more accurate and more timely. After all, if we are dealing with the problem when the suspect is already on the plane, it is really a bit too late. We need to also improve the system for seeking redress if individuals believe that they have been wrongfully targeted. My understanding is that the Terrorist Screening Center is working with the GAO and the Inspector General to implement their recommendations.

Any system that relies on judgments made by various personnel in different agencies applying varying standards will never be perfect, particularly when we are dealing with very large, complex databases. It is, nevertheless, imperative that improvements be made so that the American people can have more confidence and less concern about this important safeguard against terrorist attacks.

Chairman LIEBERMAN. Thanks very much, Senator Collins. Thanks to the witnesses for being here. We have an excellent group of witnesses. We are going to vote around 11 or so, so hopefully we

[1] The GAO report appears in the Appendix on page 87.
[2] The DOJ Inspector General's report appears in the Appendix on page 169.

can get through the opening statements and some questioning by the Senators who are here before we have to go and come back.

We will begin with Ms. Larence—is it Larence, you say?

Ms. LARENCE. Larence.

Chairman LIEBERMAN. Larence. OK, forget the "W."

Ms. LARENCE. It was there before Ellis Island. [Laughter.]

Chairman LIEBERMAN. Yes, we have a lot of stories we could tell about that.

OK. Ms. Larence is the Director of Homeland Security and Justice Issues at the Government Accountability Office of the United States, which has been such a strong source of support and assistance to this Committee and the Congress in general. So we welcome your testimony now.

TESTIMONY OF EILEEN R. LARENCE,[1] DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Ms. LARENCE. Thank you, sir. Mr. Chairman and Members of the Committee, I am pleased to be here this morning to summarize a report released today on the Federal Government's use of the terrorist watch list to screen individuals for possible threats to homeland security. As you acknowledged already, unlike September 11, 2001, when agencies generally did not share information on known or suspected terrorists, our work shows that now the Terrorist Screening Center maintains one master repository of records on individuals with real or potential ties to terrorism. Agencies use the list to, for example, screen people applying for a visa, crossing through ports of entry into the country, or stopped for traffic violations.

Our work also shows that agencies find the terrorist watch list to be an important counterterrorism tool, but we have found that it could be strengthened by addressing potential security vulnerabilities, using all appropriate screening opportunities, and providing for greater accountability and effectiveness.

In our report, we address several fundamental questions. First, how do people get on and off the list? Intelligence agencies, the FBI, and other Federal agencies nominate individuals to the watch list using a relatively low bar because they want to make certain they do not miss any threats. Generally, agencies determine whether the information available on an individual provides a reasonable suspicion that the person has known or potential links to terrorism. Sometimes agencies have limited information and so must use their subjective judgment to determine who to list. To help guide these decisions, agencies use criteria and have review processes. For example, according to the FBI, generally any person subject to a counterterrorism investigation is put on the list after going through a formal review and approval process. If the investigation does not show a terrorist threat, as defined by Attorney General guidelines, the person is to come off the list.

We do not know how the intelligence community makes such decisions because, in part, the CIA chose not to discuss this with us. Officials from both the National Counterterrorism Center that re-

[1] The prepared statement of Ms. Larence appears in the Appendix on page 37.

ceives and forwards to the Terrorist Screening Center all nominations with international links to terrorism as well as the Screening Center itself said they review nominations to ensure there is a nexus to terrorism and have criteria to do so. While the Terrorist Screening Center reports deleting some 100,000 total records from the watch list so far, as you noted, it continues to grow significantly.

The second question we answered is: How often have agencies encountered people on the list, and what has happened to them? As of May, airlines or agencies matched the names of travelers with names of people on the watch list about 53,000 times, although they matched some people more than once. Most matches were within the United States by State and local law enforcement or other government agencies. Individuals were sometimes arrested or denied a visa, boarding an aircraft, or entry into the country. But most often they were questioned and released because the derogatory information on the person did not show a legal basis, such as a criminal violation, to take any other action.

Agency officials said that they use information collected during questioning to assess the threat posed by the individual, to track the person's movement, and to update intelligence or investigation files. And the Terrorist Screening Center shares information on encounters daily through a reporting process.

On a related note, our prior work that we issued in a report in September 2006 showed that agencies were almost as often mistakenly identifying and stopping, questioning, and in some cases searching individuals who are not the person on the watch list but who unfortunately have a name similar to someone on the list. We reported why this happens, how this is being addressed, and what redress is available to these individuals, and I would be glad to discuss that work further.

The third question our report today addresses is whether there are potential security vulnerabilities in agency screening processes. Agencies do not check against all names on the watch list. According to the Terrorist Screening Center, this can be a vulnerability, or at least a missed opportunity to collect information. Rather, the center sends subsets of the watch list to other information systems that agencies use to screen individuals depending on the agency's mission or operational capabilities. For example, Customs and Border Protection maintains an information system it uses to check all travelers, including U.S. citizens, for criminal or immigration violations or other concerns before they enter the country. Because of this broad mission, the Terrorist Screening Center sends CBP the highest percentage of watch list records to use during its screening.

In contrast, airlines receive fewer names to screen passengers using the No Fly List or Selectee List. According to TSA, this is because its mission is transportation safety, not intelligence or investigations. And nominations to these two lists must pass a higher bar or more stringent criteria established by the Homeland Security Council, such as posing a threat to civil aviation.

In addition, TSA requires that watch list records used for screening contain sufficient identifying information, but not all watch list records do so, and so these records are not passed to the airlines

for screening. This is also the case for State and local law enforcement.

TSA and FBI officials told us that the requirement for full information and records is to minimize the times people are misidentified and that screening against all names on the list would not necessarily result in increased security, but they did not provide the basis for their position; therefore, we continue to recommend that both agencies assess the extent of vulnerabilities in their screening processes and address them.

Agencies also acknowledged that individuals on the watch list have passed undetected through their screening, but they said they are taking steps to address this problem. For example, CBP has cases of people on the watch list who were not identified until they had entered the country, but it is working on corrective actions.

Likewise, as noted in your opening statements, individuals on the No Fly List have boarded aircraft, and sometimes flights had to be diverted. Agencies know this because for international flights into the United States, Customs and Border Protection screens all passengers a second time after the airlines to determine if the passengers can enter the country. To do this screening, CBP needs passenger data that currently is not sent to CBP in time to screen before a flight departs. A new rule in February will require that the data be provided to CBP sooner, which could help to identify individuals on the No Fly List before planes are airborne.

It is important to note that there is no such second screening on domestic flights, but considering such a process would require assessing impacts on privacy and air travel, and TSA's new Secure Flight passenger pre-screening system, once implemented, may help to alleviate this concern.

Finally, our work showed that the Federal Government has not identified and implemented all possible terrorist screening opportunities as mandated. The State Department is pursuing opportunities with some foreign partners, the Terrorist Screening Center is entering agreements with some agency components, and DHS is working on guidelines to help the private sector owners and operators of critical infrastructure screen employees to see if they pose threats. But we have recommended that all appropriate screening opportunities be identified and implemented and that DHS complete and implement the private sector guidelines, and the agency has agreed with these recommendations.

In conclusion, overall GAO's findings stem in part from the fact that while each agency owns a parochial piece of the watch list process, no one entity is accountable overall for resolving interagency conflicts, addressing vulnerabilities, monitoring results, and ensuring that the list is working as intended. Furthermore, the government does not have an up-to-date strategy and implementation plan with a recommended governance structure to provide for the most effective watch list screening. The President tasked DHS to work with relevant agencies to develop these plans. DHS said it submitted them in November 2004. The Homeland Security Council did not approve and implement the plans, however. We were not given copies of the plans to review or the opportunity to discuss this issue with the Homeland Security Council. So we have recommended that DHS update and resubmit these plans and that

the Assistant to the President for Homeland Security and Counterterrorism ensure that they are implemented and that the governance structure agencies recommend be given the responsibilities and authorities needed to manage and be held accountable for screening governmentwide. DHS agreed to its recommendation, but the White House chose not to respond to our report.

Mr. Chairman, that concludes my statement, and I would be happy to answer any questions.

Chairman LIEBERMAN. Thanks very much, Ms. Larence, for an excellent report. I appreciate the question you posed at the end and really the challenge, and we will want to hear from the other witnesses about that, about accountability and responsibility here.

Glenn Fine is the Inspector General of the Department of Justice, familiar to us, even respected by us. Thanks for being here.

TESTIMONY OF HON. GLENN A. FINE,[1] INSPECTOR GENERAL, U.S. DEPARTMENT OF JUSTICE

Mr. FINE. Thank you, Mr. Chairman, Senator Collins, and Members of the Committee. Thank you for inviting me to testify on the development and status of the terrorist watch list screening system.

For the past several years, the Department of Justice Office of the Inspector General (OIG) has examined the work of the Terrorist Screening Center (TSC), a multi-agency effort administered by the FBI. Created in 2003, the TSC integrates U.S. Government terrorist watch lists into a consolidated database and provides 24-hour-a-day, 7-day-a-week responses to Federal, State, and local governments to assist in screening for individuals with possible ties to terrorism. Prior to the establishment of the TSC, the Federal Government's terrorist screening system was fragmented, relying on at least a dozen separate watch lists maintained by a variety of Federal agencies.

In June 2005, the OIG issued our first audit of the TSC's operations. This audit found that the TSC had made significant strides in developing a consolidated terrorist watch list database. But we also found weaknesses in various areas of TSC operations, including that the TSC had not ensured that information in the consolidated database was complete and accurate.

Last month, we completed a follow-up review examining the TSC's progress in improving its operations since our 2005 audit. The recent audit found that the TSC has continued to make significant progress in important areas. However, we also concluded that the TSC's management of the watch list continues to have significant weaknesses and that the information in the watch list database was not complete or fully accurate.

These weaknesses can have enormous consequences. Inaccuracies in watch list data increase the possibility that reliable information will not be available to front-line screening agents, which could prevent them from successfully identifying a known or suspected terrorist. Furthermore, inaccurate watch list information increases the chances of innocent persons being stopped or detained because of misidentifications.

[1] The prepared statement of Mr. Fine appears in the Appendix on page 54.

For these reasons, we believe it is critical that the TSC and the agencies providing watch list data to the TSC further improve the accuracy of the information. In short, our September 2007 audit credited the TSC for improving its operations. It has enhanced its efforts to ensure the quality of watch list data, increased staff assigned to data quality management, and developed a process and a separate office to address complaints by persons seeking redress related to terrorist watch list screening. However, we also determined that the TSC needs further improvement. I would like to make five observations about these needed improvements.

First, the TSC still maintains two versions of the watch list database. While the TSC is developing an upgraded, consolidated database that will eliminate the need to maintain parallel systems, the two databases were not identical in content when we tested them, which they should be. In addition, the number of duplicate records in the TSC database has significantly increased.

Second, we found that not all watch list records were being sent to downstream screening databases. We discussed this issue with TSC officials, who agreed with our findings and began correcting those omissions.

Third, our review found that the TSC did not have a process for regularly reviewing the contents of the consolidated database to ensure that all outdated information is removed, as well as to affirm that appropriate records are watch-listed.

We concluded that the TSC needs to further improve its quality assurance efforts for ensuring the accuracy of the watch list records. Since our last report, the TSC has increased its quality assurance efforts and implemented a data quality improvement plan. In general, we believe that these actions are positive steps. We also recognize that it is impossible to completely eliminate the potential for errors in such a large database. However, we identified continuing inaccuracies in records that had undergone the TSC's quality assurance processes.

For example, the TSC completed a special quality assurance review of the No Fly List, which dramatically reduced the number of records on the list. But our examination of the TSC's routine quality assurance reviews revealed continued problems. Specifically, we examined 105 records subjected to the routine quality assurance review and found that 38 percent of these records continued to contain errors or inconsistencies that were not identified through the routine quality assurance efforts. Thus, the TSC continues to lack important safeguards for ensuring data integrity, including a comprehensive protocol outlining the quality assurance procedures and a method for regularly reviewing the work of TSC staff to ensure consistency.

Fourth, we found that the TSC's efforts to resolve complaints from individuals about their possible inclusion on the watch list have improved since our previous audit, and the TSC has created a dedicated unit to handle redress complaints. However, the TSC's redress activities were not always timely. Moreover, a high percentage of complaints requiring modification or removal is a further indicator that watch list data needs continuous monitoring and attention.

Fifth, we found that the TSC does not have a policy or procedures to proactively use information from encounters with individuals to reduce watch list misidentifications. Considering that nearly half of all encounters referred to the TSC Call Center are negative for a watch list match, we recommended that the TSC consider misidentifications a priority and develop strategic goals and policy for mitigating misidentifications, particularly for individuals who are repeatedly misidentified.

In total, our report made 18 recommendations to further improve the TSC's watch-listing process. These recommendations include making improvements to increase the quality of watch list data; revising the FBI's watch list nominations process; and developing goals, measures, and timeliness standards related to the redress process. In response, the TSC agreed with the recommendations and stated that it would take corrective action.

Finally, I want to mention a separate audit that we are currently conducting to examine the specific policies and procedures of Department of Justice components for nominating individuals to the consolidated watch list, which is a very important issue. We are conducting this review in conjunction with other Intelligence Community OIGs, who are examining the watch list nomination process in their agencies. These OIG reviews are being coordinated by the OIG for the Office of the Director of National Intelligence.

In conclusion, the TSC deserves credit for creating and implementing a consolidated watch list and for making significant progress in improving the watch list and screening processes. However, our reviews have found continuing weaknesses in some of those processes. We believe it is critical that the TSC further improve the quality of its data and its redress procedures. Inaccurate, incomplete, and obsolete watch list information can increase the risk of not identifying known or suspected terrorists, and it can also increase the risk that innocent persons will be repeatedly stopped or detained. While the TSC has a difficult task and has made significant progress, we believe it needs to make additional improvements.

That concludes my statement, and I would be pleased to answer any questions.

Chairman LIEBERMAN. Thanks very much, Mr. Fine, for an excellent statement and for your continuing interest in this subject, which we all want to get right and want to be fair.

The next witness is Leonard Boyle, Director of the Terrorist Screening Center. It is a personal pleasure for me to welcome Mr. Boyle here because he comes to this position having previously served with honor and effect as the Commissioner of Public Safety of the great State of Connecticut. We welcome your testimony.

TESTIMONY OF LEONARD C. BOYLE,[1] DIRECTOR, TERRORIST SCREENING CENTER, FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT OF JUSTICE

Mr. BOYLE. Thank you very much, Chairman Lieberman, thank you for those kind words, Senator Collins, and Members of the

[1] The prepared statement of Mr. Boyle appears in the Appendix on page 65.

Committee. Thank you for the opportunity to address the Committee today on these two important reports that have been issued.

As both reports note, the Terrorist Screening Center plays a critical role in the government's multi-layered strategy to prevent another terrorist attack on the United States. That multi-layered strategy calls for, in the first instance, every effort to prevent a potential terrorist from leaving his or her country of origin.

To that extent, the Terrorist Screening Center, having created the Terrorist Screening Database, sends to the State Department a significant number of identities of persons who may be seeking to obtain a visa to enter the United States. Because of the work that has been done by the TSC, all consular officers around the world now have access to the U.S. Government's best understanding, both the intelligence and law enforcement community, of those who pose a terrorist threat to the United States. Every consular officer, in considering a visa application, can query the database and use any information that is found there as one factor in determining whether that particular person ought to be granted a visa to enter the United States.

The second phase of that multi-layered strategy is for persons who are trying to enter the United States at our borders, for our Customs and Border Protection agents to have access to a similar set of information, slightly broader than what is given to the State Department, which is tailored to meet the needs of Customs and Border Protection so that a CBP agent can make the best informed determination as to whether he should grant a person access to the United States. He queries the IBIS or TECS system, which is supplied by the Terrorist Screening Center, for a determination as to whether that person, who is seeking entry to the United States, has been identified as a known or suspected terrorist.

The third level of protection is within our borders. If a person does manage to get into the United States, or is already here, and is in the view of the law enforcement community or the intelligence community a potential terrorist threat to our Nation, information is now made available to all State, county, municipal, and tribal police officers throughout the United States, a force multiplier of about 750,000 law enforcement officers that did not exist prior to the creation of the TSC.

While law enforcement officers did have access to Federal databases regarding certain types of suspected problem persons, they did not have access to the intelligence community's assessment of known and suspected terrorists. They do now.

Chairman Lieberman, in your earlier remarks, you made reference to two of the September 11, 2001, hijackers. I would also cite a particular example. On the morning of September 9, 2001, a State trooper stopped a young man who was traveling north on I–95, did all the appropriate actions, including run that man's name through the National Crime Information Center, found no negative or derogatory information. The trooper did his job and sent that person on his way. Two days later, that person, Ziad Jarrah, and four of his co-conspirators hijacked United Airlines Flight 93 and, but for the actions of some very brave and heroic people, would have probably crashed that plane into some significant national asset.

That is the type of information that is now available to all State, county, municipal, and tribal police officers as a result of the work that is being done by the TSC.

That being the case, of course, we will not be satisfied until we are certain that we have the best, most effective, and most accurate watch list possible. And to that end, we welcome the recommendations that have been made by the Office of the Inspector General as well as by the Government Accountability Office. We are using those reports as a road map to improve the watch list, to make our processes better.

I think a fair assessment of what the TSC has done in 3½ years is that it has achieved with remarkable success the basic objectives that were tasked to it by HSPD–6, that is, the creation of a unified watch list, the creation of a means to update that watch list on a daily basis, the creation of a system to export those lists to Customs and Border Protection, the State Department, State and municipal law enforcement, as well as the TSA, to protect our flying public and also to create a call center, a 24-hour-a-day, 7-day-a-week call center, so that anytime any of those screening agents or law enforcement agents encounters a known or suspected terrorist, they call the Terrorist Screening Center, they do not get a busy signal, and they do not get a recording. They get a human being who answers that phone, who has full access, electronic access, to all of the underlying derogatory information about the person who has been encountered.

We have also spent a great deal of effort reaching out to our foreign partners in satisfaction of the goals tasked to us by HSPD–6. We now have six agreements with foreign partners. Spain recently publicly announced that we had executed an agreement with Spain to share watch-listing information, and we have numerous discussions going on with our foreign partners around the world to try to increase the amount of sharing that we have with our foreign partners. So we are, I believe, in a position where we are now ready, having satisfied those basic objectives, to refine the watch list and make it better.

I would address just a couple of matters that have previously been raised, and the first has to do with redress. We understand that our obligation is to protect the safety of this Nation, but to do so in a way that protects and preserves civil liberties and privacy. To that end, as a result of the recommendations that were made by the OIG in 2005, the TSC has created a redress office staffed by seven people, dedicated employees who review every matter that comes to our attention. To date, they have reviewed close to 500 separate matters that have been brought to us. They do a complete *de novo* review of the watch-listing status of any person who is referred to us to make an independent determination as to whether that person is properly listed or not.

We also have put in place a number of processes to address the concerns that have been raised by the Office of Inspector General to ensure that we are now, in fact, consolidating both components of our system so that there is a single, unified, one-component system of our watch list. We have set up a daily reconciliation process to make sure that those two components every day are reconciled. We also have added a compliance officer to make sure that we have

appropriate standard operating procedures in place. And we have also brought on a data integrity officer, a senior official from the Department of Homeland Security, to make sure that we do not have gaps within our systems so that we are properly structured to meet our needs, to meet our requirements, and to meet the mission that has been set out before us.

So, again, I thank you for the opportunity to address you today, and I am happy to answer any questions that members might have.

Chairman LIEBERMAN. Very good. Thanks for that excellent testimony, Mr. Boyle. We will have some questions for you.

Our final witness on the panel this morning is Paul Rosenzweig, who is the Deputy Assistant Secretary for Policy at the U.S. Department of Homeland Security. Welcome.

TESTIMONY OF PAUL ROSENZWEIG,[1] DEPUTY ASSISTANT SECRETARY FOR POLICY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. ROSENZWEIG. Thank you very much. Thank you, Senator Lieberman and Senator Collins, for inviting me. It is a particular pleasure to be here today. Though I have been with the Department 2 years and have testified nearly a dozen times, this is my first opportunity to actually testify in front of my home Committee in the Senate.

Chairman LIEBERMAN. There is a story there.

Mr. ROSENZWEIG. I know it very well.

Chairman LIEBERMAN. We tried.

Mr. ROSENZWEIG. It is especially a pleasure because of the constructive and thoughtful nature of the discussion we are having today. I would have a great deal of difficulty disagreeing with any of the comments and recommendations that we have heard from the General Accounting Office or with any of the statements that have gone before. As Senator Collins so aptly said, it is a big system, and that makes it imperfect to some degree. And our goal is to make it as close to perfect as we can, recognizing that it is an unachievable objective.

I speak not as a nominator to the TSC because DHS puts very few people onto the watch list but, rather, as a consumer of its product. And as a consumer, we are as troubled by errors in the system when they exist as anybody, simply because they are an annoyance to the traveling public with whom we deal every day; more importantly, they are a waste of resources. For every time that we look at somebody who is not the right person, that is time not spent looking in the right place.

I think it is fair to say that, by and large, we have had a number of successes and much work needs to be done. Let me briefly give you a sense of some of those successes.

We have put in place a layered system for checking people as they arrive at the border, to take but one example. That includes not only the Department of State Visa Lookout System, but also the export of the No Fly and Selectee Lists to international airlines for checking of those who are traveling to the United States. It in-

[1] The prepared statement of Mr. Rosenzweig appears in the Appendix on page 71.

cludes capture of data on all travelers to the United States, alien and U.S. citizens, through the Advanced Passenger Information System and the Passenger Name Records. And, finally, of course, it includes the final check at the port of entry by Customs and Border Protection officers provided with the watch list to make a determination, as Mr. Boyle said, given the best information available whether or not a particular individual should be admitted.

We have also had great success and made great strides, I think, in improving our redress process. Mr. Boyle has described some of the improvements that were made at TSC. Within DHS, we have developed the Traveler Redress Inquiry Program (TRIP) in partnership with the Department of State, which is a one-stop shop for people to enter the system to seek redress and, if appropriate, to receive notifications from us that they get put on a cleared list, in effect.

We have also developed at the ports of entry themselves something we call the Primary Lookout Override (PLOR) system, which means that we can make corrections directly on the screens in front of us and ensure that once we have identified somebody as a misidentification, a false positive, he never again gets troubled. And that gets propagated through the system.

So we have made great strides, I think, but as you said, there is much work to be done. You mentioned, Senator Collins, the unfortunate visits of several airlines to Bangor. I am happy to say that we have not had any in 2 years, and that is part of our ongoing process. There are two other pieces that are going forward that should come online in the next months to year that will improve that even further. One is, as Ms. Larence noted, the development of the Advance Passenger Information System (APIS) quick query system. That will require the transmission of passenger information to CBP for checking at the National Targeting Center against the Terrorist Screening Database before the airplane takes off from a foreign country. It will allow that transmission up until the doors are actually closed, but will require it before wheels-up. So we will be doing that checking.

We will also be developing a system called Secure Flight, which will take into the TSA the watch list name matching for the No Fly and Selectee lists. As you probably know, today we export that list to the airlines, and a lot of the problems we have is simply because there are 63 different airlines that fly here, and they do it 63 different ways. That creates, at worst, inconsistency if not error. We have published a Notice of Proposed Rulemaking to anticipate bringing that on board into the United States sometime late this year or early next year.

I am constrained to mention at this juncture that we are resource constrained in doing that. We have requested $53 million in the President's budget for that effort. The Senate appropriations mark is $28 million, and that will, of course, delay that implementation going forward. But, nonetheless, those two pieces of the puzzle ought to improve our ability a great deal.

But the final thing that I would say is that what we have come to recognize as consumers is that there are inherent limitations to watch list name matching by themselves. The case of the Mexican gentleman with tuberculosis that you mentioned is an example of

that, where we can only work with as much information as we have, and if the information is incomplete or inaccurate, that defeats to some degree our ability to conduct watch list name matching. What we need to do and the other piece of the puzzle is to go beyond watch list name matching to enhance our ability to identify people through secure identification documents, to use the information we collect about individuals, to identify unknown names through link analysis—people traveling together where one is known and one is not known, for example—and, finally, of course, through the US–VISIT program to develop enhanced biometric capabilities so that the name does not matter because the fingerprint never changes while the names may. All of those taken together will further enhance our ability.

Now, we will never get away from a name-based watch list matching system because for many people who are deemed threats to us we do not have the biometric identification, we do not have the fingerprint. We have the names and the many aliases that are also records in the Terrorist Screening Database (TSDB). But as we continue to put on these layers, we will, I believe, enhance our ability to identify correctly those who pose a threat and reduce the instances in which we make mistakes or errors.

Taken together, I think that paints a good picture of how we at DHS are using the Terrorist Screening Database. We have had a number of successes. Last year, at the borders, 5,900 positive matches against the watch list—not all of those denied entry, but all of those people of interest who I am glad we identified before they entered the United States.

We can do better for sure, but I share with Mr. Boyle—and, I take it, with Ms. Larence and Mr. Fine—the sense that between where we were on September 10, 2001, and where we are now, we have made great strides. More work needs to be done, but the improvement is quite noticeable.

I thank you for your attention, and I, too, look forward to answering your questions.

Chairman LIEBERMAN. Thanks, Secretary Rosenzweig. I appreciate the testimony very much. We are going to do a 5-minute round so all four of us can have a chance to ask some questions before the votes go off.

Mr. Boyle—and I am having a hard time not calling you Commissioner Boyle—let me ask you to comment on the growth in the size of the watch list. Of course, as I said in my opening statement, this is good news, assuming all those names are correct, but the database has gone from 158,000, GAO reports, in June 2004 to 860,000 today, and it is going up at around 20,000 records per month. And I know there is a process by which they got on that list.

As it approaches 1 million, is it reasonable to assume that there really are 1 million people who are known or suspected terrorists?

Mr. BOYLE. No, and for context, the watch list or the Terrorist Screening Database does not reflect some 800,000 human beings.

Chairman LIEBERMAN. So explain that. I understand that.

Mr. BOYLE. Sure. We have approximately 860,000 records in the Terrorist Screening Database. We create a record for any identification that a person might use if he or she is trying to enter this

country or is trying to obtain documents in support of terrorist activity. So, for example, if a person uses the name Len Boyle and has at various times used three separate dates of birth, that will create three separate records in the Terrorist Screening Database.

Chairman LIEBERMAN. OK.

Mr. BOYLE. We have some persons for whom we have 50 or more records, as the GAO report points out.

Chairman LIEBERMAN. Right.

Mr. BOYLE. So the actual number of human beings reflected in the database is far fewer than 800,000. I cannot give you an exact number because, in fact, we do not know for sure. Some people actually successfully create an entire separate identity.

Chairman LIEBERMAN. Yes.

Mr. BOYLE. So even if we looked at the database, we might see what appear to be two completely separate identities that reflect but one person. So the number is far fewer.

Another thing I think is very important for the public to understand is that about 95 percent of the database consists of non-U.S. persons.

Chairman LIEBERMAN. Right.

Mr. BOYLE. That is, people who are not U.S. citizens or who have been granted permanent resident alien status.

Chairman LIEBERMAN. And you are getting those from the intelligence community, both ours and foreign intelligence, cooperating agencies?

Mr. BOYLE. Most often, yes, sir, and they are coming from hot spots around the world.

Chairman LIEBERMAN. Right.

Mr. BOYLE. Areas of strong anti-American sentiment, and the theory behind watch-listing those persons is if there is a reasonable suspicion that this person has been associated with terrorist activity, perhaps has provided funding to a terrorist organization or has attended a terrorist training camp, we want that person listed in the database so that if next week, next month, next year that person tries to enter the United States, Customs and Border Protection and the State Department are going to be able to look at that person, know what we know about him, what the intelligence community knows about him, and make a determination.

Chairman LIEBERMAN. OK. So, bottom line, not all the people on there are there with full justification but that there is a reason why everyone who is on there is on there, and you are the man who sees it all. I presume you would say that, to the best of your knowledge, most of the names on there deserve to be on there.

Mr. BOYLE. Yes, sir. Using the reasonable suspicion standard, those names are vetted first by the nominating agency, then by NCTC, then by us to make sure that there is a reasonable suspicion of a nexus to terrorism.

Chairman LIEBERMAN. Give me your response to the question that Ms. Larence raised at the end, which is that the TSC is really doing its job, but that there is no one in the Federal Government to oversee the operation of the watch lists overall to make priority decisions about investments or even accountability. How do you respond to that? And if you think she is right, should you do that?

Mr. BOYLE. Well, as the Members of the Committee are aware, HSPD–11 designates the Secretary of the Department of Homeland Security to have overarching responsibility for watch-listing in general. We, at the Terrorist Screening Center, work through our governance board; we work very closely with DHS. But we are, I would put it, more the nuts and bolts of watch-listing and screening rather than the overarching strategic approach to screening.

Chairman LIEBERMAN. Would you say the Secretary of Homeland Security is the one responsible for that overarching view?

Mr. BOYLE. Yes, sir, and we work very closely with DHS in accomplishing those objectives.

Chairman LIEBERMAN. One of the things that really thrills me most about what you have reported today is the access that local, State, tribal, etc., law enforcers have to this terrorism database because it vastly expands our potential to catch these people before they act. Are the State, local, county, and tribal law enforcers using it?

Mr. BOYLE. They are using it, and they have been fantastic partners with us, and we are continuing our outreach with State and local law enforcement. One of the things that we are going to be doing at the TSC over the next several months is providing State and local law enforcement with a daily report showing the encounters with suspected terrorists around the country so that a police chief in Minneapolis will know how many encounters occurred in his general area or the new Commissioner of the Connecticut Department of Public Safety will know how many encounters occurred in Connecticut. They have been wonderful partners.

Chairman LIEBERMAN. OK. Thanks very much. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Commissioner Boyle—I will use that name as well.

Mr. BOYLE. Thank you.

Senator COLLINS. I could not help but think that, as you described the incident that I remember so well from the 9/11 Commission's report, had that State trooper had access to the kind of information in the system today, that individual terrorist would have been stopped and many of the others would have been as well. So I want to commend all of you for the work that you are doing even as I ask some questions about some concerns that I have.

Mr. Secretary, this morning we received information from CBP that the original information that it had received on the Mexican national with TB on April 16 was not actually an alias, which had been the agency's justification for not stopping the individual in the first place. What we found is that, in fact, CBP and the system had the individual's middle name, his two hyphenated last names, and a date of birth that had an error in it, but the error was corrected the very next day.

So the information and the lookout was entered into the computer system on April 16, and yet this individual was able to cross the border an astonishing 21 times. And it was only when his Mexican doctor confiscated his visa and turned it over to U.S. authorities that he was stopped.

That raises real concerns to me about the effectiveness of the computerized system and the name-matching process, and indeed,

in the report that GAO did, it found that individuals were able to pass despite being on the watch list due to not only errors in the computer system but also that the name-matching process is not very sophisticated.

If an individual with a dangerous strain of TB can cross 21 times after being put on the list, that raises a lot of concerns to me about whether you are capable of stopping terrorists or other public health threats when there is a slight variation in the name.

Mr. ROSENZWEIG. Thank you for the question, and it actually allows me, if you will permit me, to explain the watch list name-matching algorithms we use in a little bit of detail because it is important to understand. And to explain, I will use myself as an example because we are not publicly discussing this gentleman's name.

My name is Paul Samuel Rosenzweig. My mother's maiden name is Hahn. And my birth date is actually 10/31/59, but let's assign me 10/8/59 as a birth date. So when we do a name check against that, we use as a parameter the very first initial of my first name, my last name, and my date of birth. So I am P. Rosenzweig, 10/8/59, in my hypothetical example.

If the information we get from another source, in this case CDC from the Mexican health officials, is different from that, the question is how closely that match exists. The individual that we are talking about used his second name and flipped his two last names, so he would have been in my hypothetical example Samuel Rosenzweig Hahn, and he also flipped at least initially the date of birth, from 10/8 to 8/10. So the match algorithm would have been S. Hahn, 8/10/59, matched against P. Rosenzweig, 10/8/59. All three of the parameters that we search against miss. And what happened on the very first day was we used those parameters, and we said this person is not in the system, something must be wrong.

Now, in order to find further information about a person, we start by suppressing some of the information. We say maybe there is a mistake in the date of birth, so you take that out and you ask for all the S. Hahns. But, of course, that does not catch P. Rosenzweig either because that does not work.

Then you say let's get rid of the first name, S., and catch all of the Hahns. That, too, would not catch a person whose last name is not Hahn but is, in fact, Rosenzweig.

It is only when you start asking all people who might have the name in any particular order—because we do not know the nature of the mistake up front—that is, Hahn or Rosenzweig or S. or that date of birth, that I would pop up.

Now, that, too, does not actually sound like too much of a problem for us to do a check, but then we actually have to resolve those hits. And we get approximately 1 million land border crossings a day, and though Hahn and Rosenzweig are relatively uncommon names, this individual had a more common set of names.

So to give you an example, and, again, using a hypothetical example, on Monday of this week J. Rodriguez, picking a relatively common Hispanic name, there were 816 crossers with that name. Now, if you suppress the first initial and just went for Rodriguez, you probably do something like 20 times that, or 16,000. And if you did Rodriguez plus another common Hispanic name like Gutierrez,

to pick our Commerce Secretary, as either/or, you would maybe get 30,000. I have not run the numbers, but that is a rough order of magnitude. That 30,000, that is 29,999 false positives for sure, plus, of course, this individual does not cross every day, and that is repeated every day in the system.

We have had many complaints that the lines on the Southern border are already too long. As the type of information we get is less and less accurate and we widen the field to make an examination based upon the name check, we get more and more people who will be overwhelming our secondary inspection capabilities, extending the line beyond belief and inconveniencing lots of people who are not matches for any of those.

In retrospect, it is easy to understand that we should have just switched the matrilineal and patrilineal names and dropped the first name and corrected the date of birth. But that is only because we know what the right answer is now. It is very hard. And I am happy to talk about it more when——

Senator COLLINS. My time has expired.

Mr. ROSENZWEIG. I am sorry.

Senator COLLINS. But I appreciate the explanation. It is my understanding that the birth date was corrected very quickly, so it is not exactly the same as your hypothetical example, but I understand your point. Thank you.

Chairman LIEBERMAN. Thanks, Senator Collins. Senator Tester.

OPENING STATEMENT OF SENATOR TESTER

Senator TESTER. Thank you, Mr. Chairman.

Chairman LIEBERMAN. I bet there are not too many Testers coming in every day.

Senator TESTER. It makes me appreciate that my name is not John Smith. [Laughter.]

I appreciate the work that each and every one of you folks do in your respective roles.

I guess the first question is for Director Boyle, and it gets down to what the rules are for getting into the database. You had said 95 percent of the people are not U.S. citizens. Is that correct?

Mr. BOYLE. Roughly, yes.

Senator TESTER. So are the rules the same for folks that are not U.S. citizens and folks that are U.S. citizens for getting on that watch list?

Mr. BOYLE. The standard is the same, sir. It is a reasonable suspicion standard. Each agency may have its own protocol. For example, an FBI nomination comes about after an FBI case agent opens a preliminary inquiry or a case on terrorism, and that has to be consistent with the Attorney General's guidelines. But the reasonable suspicion standard applies across the board.

Senator TESTER. And 43,000 involved in those kind of suspicions or counterterrorism investigations?

Mr. BOYLE. I do not have the numbers in front of me, sir, but if that——

Senator TESTER. Well, that would be 5 percent of 860,000.

Mr. BOYLE. If that is the way the match works out.

Senator TESTER. A couple things, and I think the Chairman touched on one of them, and that is, in fact, does the county, city,

highway patrol, and tribal police forces all have access to this information?

Mr. BOYLE. Yes, sir.

Senator TESTER. And they are all encouraged to use it.

Mr. BOYLE. Yes, they are.

Senator TESTER. And then you talked about seven employees dealing with 500 reviews on redress. How long has that board been in existence?

Mr. BOYLE. We created the redress group after the 2005 report from the Office of Inspector General. I can get you the answer by turning around just briefly.

Senator TESTER. Well, I guess more specifically, it was created sometime in 2005.

Mr. BOYLE. Yes, sir.

Senator TESTER. So it has been in effect for a couple years?

Mr. BOYLE. That is correct, sir.

Senator TESTER. Are those 500 people, are the majority of them Americans or U.S. citizens? If you do not know that, you can give me——

Mr. BOYLE. I do not know. I am turning to our redress officer.

Senator TESTER. That would be good.

Mr. BOYLE. I do not have the answer to that.

Senator TESTER. And the other thing is you had mentioned that you felt that a majority of the people that were on that list were on that list—and make no mistake about it, mistakes can be made when you are talking about a list this size. In Mr. Fine's testimony, he said that 38 percent were errors or inconsistencies. Could you explain that, Mr. Fine? I mean, there seems to be some difference in opinion on the surface here.

Mr. FINE. Well, we are not saying that those 38-percent people should not be on the list, but when we looked at a sample of 105 that had gone through the quality assurance review, we found errors in there—for example, the date of birth was wrong, incomplete, incomplete field, other errors, which showed that it was not complete and accurate, despite the fact that it had already gone through the quality assurance program. That gave us concern about the quality assurance program, and we wanted there to be more comprehensive protocols and testing of this quality assurance program to make sure that they were completely accurate.

Senator TESTER. I understand. Mr. Rosenzweig, you said that there were inherent limitations on the name situation, and the Chairman talked about Senator Kennedy being on the list at one point in time. What about the other side of the equation and you have somebody who gets off the list and just by happenstance there is a terrorist on the list that has the same name? What are the impacts there?

Mr. ROSENZWEIG. Well, thank you for the question, Senator. Actually, what we are doing inside DHS—and it is parallel to things that TSC is doing—is we do not take the name off the list. We will, for example, issue somebody who has gone through the TRIP program a cleared number that is his kind of personal additional identification number. We leave his name on the list, but the addition of additional information means we can differentiate.

Senator TESTER. Can an individual within one of the agencies or in government place names on this watch list, or are there clear criteria, period, that are followed in every case?

Mr. BOYLE. There are clear criteria, sir. Any person who is being nominated to the Terrorist Screening Database who is suspected of being involved in international terrorism, that nomination has to be vetted through the National Counterterrorism Center, and the derogatory information regarding that nominee must meet the standards that are appropriate for inclusion on the list.

Senator TESTER. Thank you very much. Thanks for your answers.

Chairman LIEBERMAN. Thanks very much, Senator Tester. Senator Voinovich.

OPENING STATEMENT OF SENATOR VOINOVICH

Senator VOINOVICH. Thank you, Mr. Chairman.

It is interesting that we hear examples of anecdotal situations where people are on the list and somehow get through the system. We also hear similar examples of individuals that are on the list that should not be on the list and somehow have not been taken off the list. But the fact of the matter is that from what I hear today and read in the written testimony, we have made really outstanding and significant improvement in screening people and the sharing of information on the watch list, and I congratulate you.

The thing that is of concern to me is that there are still some things that need to be done. Mr. Fine, do you have a term of office?

Mr. FINE. No.

Senator VOINOVICH. Are you out with the next Administration?

Mr. FINE. I serve at the pleasure of the President. All IGs do, although if the President wanted to remove me, he would have to give the reasons why to both Houses of Congress. I would note that this Committee and Congress is considering amendments to the IG Act to create a term of office of 7 years.

Senator VOINOVICH. Well, the point is that you will be around for a while. Ms. Larence, you will be around. Mr. Boyle, you will be out, I believe. [Laughter.]

Mr. Rosenzweig, you will be out also. The real issue for me is the transformation of some really significant issues in terms of intelligence gathering for our people. And, by the way, I just recently met with the FBI Joint Terrorism Task Force in Cleveland, and they are doing a fantastic job. And the great response that I got from local government officials is that they are really sharing information, and they are sharing information well. In fact, local law enforcement is embedded at the FBI today. For a former mayor that lived in a town where the Federal agencies did not even talk to each other, the outlook is very promising. To see that kind of coordination and communications is just very exciting and comforting.

But what I am concerned about is this: Does anyone have a strategic plan on how to remedy the things that you have pointed out? And is there an agreed upon metric to determine whether or not, in fact, they have accomplished it so that a year and a half from now, or more, we are not doing the same thing but with different players? Mr. Fine or Ms. Larence, are you going to be able to tell

us whether or not they really have made changes in terms of the issues that you are concerned about?

Ms. LARENCE. No, sir. That was the major finding in our report, that even though the President tasked DHS to work with all the agencies involved in screening from soup to nuts and put a plan together, including a recommendation about a governance board for this process, that has not been completed to date. I understand from the statement from the Homeland Security Council that DHS has agreed to put that plan together and submit that to the Homeland Security Council, and they have agreed to look at that issue and take action on it. But we are as concerned as you. You mentioned the growth of the watch list. Who is managing that? Who is asking those questions? In our conversations with the National Counterterrorism Center, they are expressing the same concerns about the growth of the list and our ability to manage that.

GAO was the only organization for the first time that put together the outcomes of this process across the agencies and took a look and said what does that mean and is this process working as intended. And so unless the agencies and the White House make that happen, I am afraid not, sir; we will be back in a couple of years to discuss concerns again.

Senator VOINOVICH. Well, from the point of view of this Committee, the issue we ought to be concentrating on is that a plan be put in place to implement GAO's recommendations. We must also implement metrics to determine whether or not the plan is being instituted so that we do not lose momentum during the change of administrations.

Ms. LARENCE. Yes, sir, a plan, and also we are suggesting an entity be identified, and that could be an interagency governing council, that is given the responsibility and the accountability to watch this process from soup to nuts.

Senator VOINOVICH. Mr. Boyle, if you are not getting cooperation from someone that you think you should have cooperation from, what do you do?

Mr. BOYLE. I go to the Director of the FBI or to the Secretary of the Department of Homeland Security, and the cooperation has never been a problem, sir. And with respect to your question about the recommendations, the Office of Inspector General made 18 recommendations to the Terrorist Screening Center. We have accepted all of them. We will be meeting with Office of Inspector General staff in early December. I expect that as many as six or more of those recommendations we can close out as having been satisfied. Others are more long term, and we will be presenting the Office of Inspector General with our long-term plan to address each of those matters.

Senator VOINOVICH. Thank you. Mr. Chairman, the only thing that I would recommend is that either you and Senator Collins bring them in and see the plan or have another hearing.

Chairman LIEBERMAN. We will do one or the other, and thank you for focusing on this.

Let me mention briefly how we are going to proceed. Senator Carper has yielded to Senator Warner for one question. Then Senator Carper will proceed. I will head over to vote with Senator Warner, leaving Senator Carper with really unlimited power for a

few moments. And then he can recess the hearing, but then we will come back for a few more questions. It could take 20, 25 minutes before we come back, but hang around.

Senator Warner.

OPENING STATEMENT OF SENATOR WARNER

Senator WARNER. Thank you, Mr. Chairman. I thank my colleagues.

We are privileged in the Commonwealth of Virginia to have the National Ground Intelligence Center, and I visit quite frequently, and they are on the cutting edge of biometrics. And it has come to my attention—I am not sure of the accuracy—that the Terrorist Screening Center presently does not have a number of these capabilities, including the use of biometrics.

Are you leveraging research and capabilities from other areas to incorporate it at the Terrorist Screening Center? Are you planning to get biometrics capabilities? Or do you think it should be made a part of the program? Please answer the question for the record.[1]

Mr. BOYLE. Yes, sir.

Senator WARNER. I will ask each of the witnesses to make a contribution. Thank you.

Mr. BOYLE. Biometrics will play a key role in——

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER [presiding]. I am going to ask you to withhold your answer at this time.

Mr. BOYLE. OK. But put it in the record?

Senator CARPER. If each of you would do that, it would be much appreciated. We have a vote on the way. We are voting on whether or not to order an up or down vote on the nomination of Leslie Southwick to serve on the Fifth Circuit Court of Appeals, and we have about 6 minutes to go. I do not want to miss that vote.

I have a statement for the record. I will ask unanimous consent that it be entered into the record. Since there is no one here but me to object, I suspect it will show up in the record.

[The prepared statement of Senator Carper follows:]

PREPARED STATEMENT OF SENATOR CARPER

Thank you, Mr. Chairman.

This is a very interesting hearing for me. My staff and I have spent a great deal of time over the past year or so learning a lot about the watch list process. We were doing this to help a constituent and a friend from Delaware who was having just a terrible time getting through airports.

This gentleman has a name that I'm assuming is similar to a name that appears on one or more of the watch lists out there. Depending on who was screening him when he got to the airport, he might have to wait hours to get through security. I believe he also missed flights from time to time. I eventually had to go all the way to the TSA Administrator's office to set things right.

I found this situation troubling not because it involved someone from Delaware, but because it told me that we're probably spending a lot of our time and resources inconveniencing innocent people. And time and resources are not unlimited, so we're probably missing opportunities to catch individuals who truly are worthy of our scrutiny.

According to the GAO report that inspired this hearing, this is in fact the case. There have been a number of instances when individuals—terrorists or suspected

[1] The responses from Mr. Fine and Mr. Boyle appear in the Appendix on pages 278 and 291 respectively.

terrorists, I assume—have been able to board planes or to enter the country when they probably should not have been able to.

I'm pleased that we were able to make the watch list system work better for my constituent in Delaware. It appears, however, that we have our work cut out for us if this system is going to be as effective as it needs to be.

We need fewer false positives, of course, but it's more important that those who we rely on to make appropriate use of the terrorist watch lists—agencies like TSA, law enforcement, the airlines—are armed with the up-to-date and accurate information they need to make us safe.

Senator CARPER. I have two questions that I will ask each of you to respond to for the record. In fact, the first one, Secretary Rosenzweig, I will ask you to respond to it, and the second one, Ms. Larence, I will ask you to respond. First of all, to the Secretary, this is a question on a system called Secure Flight. I understand that the Department of Homeland Security has a system in the works called Secure Flight that at least some believe will more accurately screen individuals at the airports against terrorist watch lists. Explain to us how Secure Flight will reduce false positives and other screening issues that have been discovered over the years. And, further, I would ask when do you believe the system will be up and running and what is your Department doing to help airlines improve their screening processes in the meantime?[1]

Mr. ROSENZWEIG. It would be my pleasure.

Senator CARPER. We will give you a copy of it before you leave.

And, Ms. Larence, you note in your testimony that the decision on whether or not to place someone on the watch list is often somewhat subjective. There are individuals apparently on the watch list who are terrorists, suspected terrorists, but there are also some there who are simply being investigated for some other reason. Are there clear enough rules out there for determining who should and who should not be on the list and who ultimately makes the decision and what does he or she base his or her decision on? You are the one who made that point. I believe that would be a question, I think, for the Secretary, and if you would respond to that for the record, I would be grateful.[2]

With that having been said, we thank you for being here. We thank you for your testimony. And I am going to just say for now the hearing is in recess, but we are not adjourned, so hold on. Thanks very much.

[Recess.]

Chairman LIEBERMAN [presiding]. The hearing will reconvene. Thank you for your patience. I hope that one or two other Members will come back because they indicated to me that they had some other questions.

Let me go first to you, Ms. Larence, and this question of who has overall responsibility for, you might say, the strategic decisions related to terrorist screening in the U.S. Government. Mr. Boyle, as you heard, indicated that the Secretary of Homeland Security has that authority. There was a plan submitted, never adopted, by the Homeland Security Council. I am not clear exactly why that has not happened. Are you?

---

[1] The response from Mr. Rosenzweig appears in the Appendix on page 305.

[2] The responses from Mr. Boyle and Mr. Rosenzweig appear in the Appendix on pages 292 and 311 respectively.

Ms. LARENCE. No, sir. We actually met with each of the key players, and they gave us their perspectives on their role. The Director of National Intelligence staff obviously said they have a role in information and intelligence but not in screening operations, so they did not really think they were the appropriate person or organization to do that.

Chairman LIEBERMAN. Right.

Ms. LARENCE. Likewise, TSC explained their role. So DHS was tasked with working with the agencies to develop the plan, but DHS was not tasked with being the overall entity that we are calling for. And so it is our understanding that one possible model that was suggested would be an interagency council with representatives from each of those key players in that screening process. TSC has a council like that already in existence to advise them on their piece of the watch list process. Our point, though, is such a council would need additional authorities to be able to have responsibility for intelligence operations and outcomes.

Chairman LIEBERMAN. And those authorities would be able to do what? Spell it out a little more.

Ms. LARENCE. We think that somebody needs to be accountable, again, for really evaluating the watch list process, to make sure that, for example, they would answer questions about how are agencies making nominations, and are they doing that consistent with the right criteria. They could look at the screening across agencies to make sure that this is being done consistently. They could look at how the information is being used that is developed from the watch-listing process. And, most importantly, they could monitor the outcomes of the process to determine if it is complying with privacy issues, if we are getting the types of outcomes that we want, and how we can better manage misidentifications. And they could also help to make sure that people consistently apply new technical opportunities and tools such as new computer algorithms or more sophisticated search engines.

Chairman LIEBERMAN. Yes. Mr. Boyle, are any of those responsibilities ones that you believe that you carry out now? Or do you think that they really are in a different direction than what you have been doing every day?

Mr. BOYLE. Some of those fall pretty squarely, Senator, within what we are doing right now. For example, the algorithm project is something that we have been involved with. We are currently approaching the testing phase to try to change search algorithms so that the search engines that are being used across the communities are more finely tuned and attuned more specifically to the types of names that we are encountering in the process these days. So that is one example of a matter that we are intimately involved in. I consider that part of the tactics, if you will, of screening, the nuts and bolts that we are involved in, as is biometrics, which we are also involved with.

Chairman LIEBERMAN. Ms. Larence, do you reach a conclusion, based on all your knowledge of what is happening here, about what the best person, office, or group would be to perform this larger oversight role?

Ms. LARENCE. The potential model of an interagency council seemed to us to make sense because there are so many equities involved in this process.

Chairman LIEBERMAN. Right.

Ms. LARENCE. If I could just respond quickly, the Algorithm Working Group is a good example. It is going to be up to the agencies to voluntarily implement whatever algorithm is developed from that group, so there is really no one saying, are we going to be implementing this consistently or making sure that this happens.

So a lot of the decisions are made through consensus, working groups, or voluntary measures, and we are just wondering if that is the most effective way to manage this process.

Chairman LIEBERMAN. Yes, OK.

Commissioner Boyle, let me go to a different part of this, which is what you do to make sure that the nominating agencies—that is, agencies that suggest you put somebody on the terrorism list—are following the same criteria.

Mr. BOYLE. Again, as we noted earlier, Senator, the standard that is used is one of reasonable suspicion. In the first instance, that determination is made by the nominating agency itself.

Second, all international terrorism nominations—and about 98 to 99 percent of the database are persons who are associated with international terrorism.

Chairman LIEBERMAN. Right.

Mr. BOYLE. All of those nominations go to the National Counterterrorism Center where there is a second review or vetting of the underlying derogatory information to make sure it meets appropriate standards, and then it comes to us. So there are three phases at which the determination is made does this derogatory information meet a reasonable suspicion standard.

Chairman LIEBERMAN. Senator Levin is here, and I want to ask one more line of questions—I am glad to see him—and then I will yield to him. This, Commissioner Boyle, is on the question of what happens when there are hits found to the list. I believe I read and Ms. Larence said today that there were 53,000. Is that the right number, Ms. Larence?

Ms. LARENCE. Yes, sir.

Chairman LIEBERMAN. And I understand that GAO issued a restricted distribution version of its public report to us today which provides, I think, valuable statistics about watch list encounters and the results of those encounters. I know we cannot talk about those statistics in detail, but to the best of your ability, I wonder if you could talk a little bit about the categories of things that happen when somebody's name genuinely turns up on the list. I am leaving aside here—well, you might want to mention it—the false positives. What else happens?

Mr. BOYLE. When our call center receives a call from either a Customs and Border Protection agent or a municipal police officer who has encountered one of our watch-listed subjects, our call taker in the first instance, accessing all of the underlying information, verifies that this is or is not the watch-listed person.

Chairman LIEBERMAN. So let me interrupt you a second. When there is what I would call a hit, a match, in each case the person at the point of entry, they call that 24-hour, 7-day-a-week service?

Mr. BOYLE. They should be calling. Now, we do have instances where we do not get calls, and we are working actively to try to prevent that. But, yes, if a police officer pulls somebody over or a CBP agent encounters someone at a border, they will get a screen that tells them to call the Terrorist Screening Center.

They call the center. One of our analysts receives the call, accesses electronically all of the underlying information, and in the first instance tries to determine and does determine is the person who you are encountering the watch-listed person or is it someone who unfortunately shares a name.

Chairman LIEBERMAN. Right.

Mr. BOYLE. We can usually make that determination within 10 minutes or less. If, in fact, the person who has been encountered is the watch-listed person, we then immediately notify the FBI's Terrorist Screening Operations Unit. The TSOU then notifies the case agent who is responsible for the case that has that particular person watch-listed so that there can be an appropriate operational response.

The other things that happen are that the screen that the police officer in this example would receive tells the police officer, according to a category code, what action can be taken. Most often it is not to arrest because there has to be an active arrest warrant for that to happen, but most often it is simply to try to gather information. So that is the general procedure that happens.

Just to link back momentarily to the Ziad Jarrah case, if, in fact, the person who has found his way into the United States and is encountered as a known or suspected terrorist is not the subject of an FBI investigation, then when we notify the Terrorist Screening Operations Unit, they will set a lead to the nearest FBI office, creating an investigation to follow up on that person to make sure that the FBI monitors what he is doing.

Chairman LIEBERMAN. That is really interesting because I would guess that most people would suspect that when you have found somebody who is a known or suspected terrorist, you would take them into custody, or the law enforcement person would take them into custody. But what you are saying is that there is really not a basis for that.

Mr. BOYLE. Only if there is an active arrest warrant or a detention order or if the person has done something else that would justify an arrest. But, no, the fact that the person is on the list does not in and of itself justify an arrest.

Chairman LIEBERMAN. But the Members of the Committee and the public I presume can have some confidence that having seen that person, that person is likely then to be followed if this is really a known or suspected terrorist.

Mr. BOYLE. It is a great opportunity for law enforcement to gather intelligence about that person because if the case agent is investigating that particular suspected terrorist and that person is stopped on the highway, we can get valuable information, such as: Where he is at that particular moment; who else is in the car with him; has he been found near a critical infrastructure or some other area that is particularly sensitive. It is a tremendous intelligence tool.

Chairman LIEBERMAN. Thanks. Very interesting. Very helpful.

Senator Levin, welcome.

OPENING STATEMENT OF SENATOR LEVIN

Senator LEVIN. Thank you. Thank you, Mr. Chairman, for holding this hearing. I will try to avoid questions if they have been asked before.

The IG has found duplicate records in the Terrorist Screening Database which can slow down the screening process or even put a law enforcement officer at risk if the handling instructions are inconsistent. The IG's report says that TSC officials stated that they will review the TSDB on a weekly basis for duplicate records. Is that now going on?

Mr. BOYLE. Yes, sir, and I think it is important to identify that duplicate records in some instances are unavoidable because we have to maintain more than one record on a particular person because our downstream customers may want different fields of information. So while it appears to be duplicative because the name, date of birth, etc., is the same, we have to include some additional information.

What is of real concern and what was importantly pointed out by the Office of Inspector General is when there are inconsistencies that might result in a different sort of category code. We are reviewing that to make sure that does not occur.

Senator LEVIN. About how many inconsistencies have appeared? Is this a rare thing? Is this one out of a thousand?

Mr. BOYLE. I believe that the figure that was identified by the Office of Inspector General was 38 percent?

Mr. FINE. I think that referred to problems with the quality assurance review. I think our report said that we saw approximately 2,000 in the first instance of duplicate records. I am not sure all of them had different handling instructions, but that was the concern that we had, duplicate records with significantly different handling instructions.

Senator LEVIN. What percentage is that?

Mr. FINE. If there are approximately 800,000 records, it is a very small percentage.

Senator LEVIN. So it is less than a quarter?

Mr. FINE. Less than 1 percent, yes.[1]

Senator LEVIN. OK. The GAO report says that the Terrorist Screening Center is developing a process that would permit law enforcement and border control agencies to directly inquire of the database as opposed to contacting the TSC by telephone when there is a possible hit. What is the status of that process to allow direct access to the database?

Mr. BOYLE. Well, that is a remote query that we are in the process of putting in place. Right now the only availability of that is for certain FBI offices which we have made available so that agents at certain airports and other areas can access the database through a BlackBerry device.

I should point out, though, Senator, that even once that remote query project is in practice, we will always want the encountering agent to call our center because it is our call takers, our analysts

[1] A clarification of this response by Mr. Fine appears in the Appendix on page 279.

who have full electronic access to all of the underlying information on the watch list.

Senator LEVIN. And it is not possible for someone in the field to have that direct access to all the underlying data?

Mr. BOYLE. No, because of classification issues.

Senator LEVIN. All right. Now, the IG follow-up audit of the Screening Center found that there are two watch lists, not one. One is a Web-based system and the other is an older legacy version. They are supposed to be identical but they are not. The IG found that multiple watch list records were missing from one or the other database that was used by either visa, border, or law enforcement personnel. The Terrorist Screening Center has apparently told the IG that having two versions is necessary for technological reasons. That is troubling to me, but explain why you have to have two versions.

Mr. BOYLE. Well, we have had substantial discussions with our friends from the Office of Inspector General about that. At one point there were two separate systems. Right now we have what I would call two components of a single system. We have an ingest system through which we receive the nominations. We then have to take those nominations and export them or the export system to our downstream clients.

The short answer to the question, sir, is that sometime during the first quarter of calendar year 2008, we expect to be able to retire that export system so that everything will be done through that first component, which will satisfy the IG's understandable concern.

Second, with respect to the time between now and then, as a result of what the IG has identified, we now do a daily reconciliation of those two components so that at the end of each day, if they do not zero out, the very next day one of our analysts takes that report and his first priority, his first order of business is to ensure that those records are, in fact, properly reconciled.

Senator LEVIN. And you have the funding to achieve that goal in 2008?

Mr. BOYLE. Yes, sir.

Senator LEVIN. Thank you. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you very much, Senator Levin. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Mr. Fine, the President has directed DHS to work with other agencies and departments to identify other appropriate screening opportunities, including the use of the watch list to screen applicants for private sector jobs when it is a job involving critical infrastructure.

Now, some people who advocate this point out that if you are having an individual who is working in a chemical plant, for example, this kind of screening could be very helpful. Others, such as the Constitution Project,[1] the think tank, have said that it is inappropriate to use watch lists for employment screening. And still other people have pointed out that a person who is turned down for a job who was mistakenly listed on a watch list would not be

[1] The Constitution Project's report appears in the Appendix on page 78.

likely to conclude that was the reason, unlike a frequent traveler where it is pretty obvious that is what has occurred.

Do you have any thoughts on this issue that you could share with us?

Mr. FINE. I do think that it is an important issue to pursue, but it raises some significant concerns, particularly because of the factors that you just identified. It is not a minor inconvenience that you are going to be delayed at the airport a short period of time. When you are looking at it in the private sector, it can have very serious implications about not being able to get employment without having any reason or knowledge about why that is. It also gives us concerns because of the size of the watch list and the potential inaccuracies in the watch list about the impact of the mistakes on it.

So while I am not opposed to pursuing this, I do think that these important safeguards need to be considered and discussed. One of the things that I do think needs to be discussed is not solely how people get onto the watch list—we have had a lot of discussion about this today, and it is an important subject—but how people get off of the watch list, how people are removed. And the FBI has a process where if the case is closed, they are removed. I am not sure all the other entities have that same process or have that same standard, so I agree with the GAO that they need to look at that in terms of a high-level review and pursue these opportunities, but to ensure that there are safeguards in place.

Senator COLLINS. I think that is a very difficult issue when you start extending the watch list to matters of employment. Clearly, we do not want terrorists to have the ability to work at a nuclear power plant or chemical facility or other critical infrastructure. But if you start having a system where the personnel director of a company has access to a watch list which may not be accurate and uses that to turn someone down for a job, I think it raises a host of new questions and we need to proceed with a lot of care in that area.

Mr. Boyle, that raises an issue as well about how long it takes for an individual who is mistakenly included on a watch list to obtain redress. The IG has found that TSC on average takes about 67 days to close its review of an inquiry from an individual who believes he or she is mistakenly listed.

Now, for a busy traveler, for a business traveler who is traveling every single week, several times a month, 2 months can involve a great deal of inconvenience if they have been incorrectly identified. Could you comment on what TSC is doing to try to expedite these reviews?

Mr. BOYLE. Yes. We are monitoring on a regular basis the average time that it takes us to resolve these matters. Sometimes because we must spend a fair amount of time dealing with the nominating agency to try to find out exactly what the information is that supports the nomination and that nominating agency's view of that person's watch list status, it can take a while, obviously particularly if we are dealing with someone who is overseas. But we are monitoring that. We are trying to reduce the time.

I would also point out that, as the OIG report mentioned, although we would like to see the time that it takes reduced, the quality of the work that is being done by our redress unit is quite

remarkable. And we certainly do not want to sacrifice the quality of what those folks are doing for the sake of expediency.

Senator COLLINS. Thank you. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks very much, Senator Collins.

Commissioner Boyle, I know today the Committee did receive the Memorandum of Understanding with this new series of policies regarding redress. Is there anything more you would like to say about that. We appreciate the fact that it has come into effect. Parties to this are the various agencies involved in the various terrorism databases.

Mr. BOYLE. Yes, and thank you for the opportunity to address that, Mr. Chairman. This has been the result of a lot of hard work by a lot of folks over the past several months.

We have had in place a process whereby our redress analysts in our redress unit work with the various agencies. The Memorandum of Understanding that is being released today commits each one of those agencies to identify a high-level official who will be responsible for ensuring that each of those agencies responds appropriately and quickly to any request for information relating to redress. So we believe that this will be a help in expediting the process and will continue to help us do so in a way that produces the appropriate result.

Chairman LIEBERMAN. Good. Secretary Rosenzweig, let me come back to the question and answer you had with Senator Collins about the Mexican national with tuberculosis who came back and forth across the borders undetected. I understood your example, and it was quite perplexing in its way. I want to mention two things to you to ask you to respond now or afterward.

One, I have seen the name of the individual, and it is not a common Hispanic name.

Two, my staff has continued to talk to the folks from Customs and Border Protection, and I do not know exactly what the individual did. I must say I do not have that, and I would like to; I think the Committee should understand that, the public should, from yourself or the Customs and Border Protection people. But I gather from the CBP people, or my staff does, that this was not a switch of names, that the person did something else.

Mr. ROSENZWEIG. Thank you for the opportunity. Let me be clear. My hypothetical——

Chairman LIEBERMAN. That was a hypothetical.

Mr. ROSENZWEIG [continuing]. Was about me, and it shows the difficulty when we do not know what the mistake is. In the Hispanic culture, it is very common for transposition.

Chairman LIEBERMAN. Right.

Mr. ROSENZWEIG. It is very common for a transposition of birth dates because of the European style of 12/9 becoming 9/12.

We got a lookout, and the very first information lacked the first name and had the wrong birth date. We try within that all the other possible permutations that we can think of, given our knowledge—I mean, we are not, despite the fact that some people might think so, routinized robots who do not actually try and approach these things with creativity. We tried reversing the names. We tried reversing the birth dates. We did indeed get a corrected birth date. But we do not know if that is a correct corrected birth date.

The first one having been wrong, we do not know if the second—it is only when we actually find the person a month later that we know that it is actually a corrected birth date as opposed to another incorrect iteration.

We run all of those possibilities. In none of them, as I understand it—and, granted, this is very fact intensive—did we have a match, principally because we lacked a first name that was at all accurate.

Chairman LIEBERMAN. So you ran those at the time the person came through or afterward to see how the person got through?

Mr. ROSENZWEIG. No. We are looking for him in our records. This person is identified to us as a frequent border crosser. If that is accurate, we should have a record of this person having crossed the border, not only the 20 times between the date and afterwards, but also the 50 times that he did before we ever got a report from the Mexican health authorities, which, of course, I cannot do anything until I get a notice.

When we throw all of these iterations of possibilities at the data set and say, do you have any Hahns, do you have any Rosenzweigs, do you have any 10/31/59s or 10/8/59s or 8/10/59s, we do not get a match that matches these descriptions.

Chairman LIEBERMAN. OK. So that was just an example, and you are not sure whether he switched his name or not, the two names?

Mr. ROSENZWEIG. We have no information about what the source of the incomplete—I think the fair way to say this is incomplete information that we got.

Chairman LIEBERMAN. So at that point, you have somebody that Mexico has told you is coming back and forth with a real contagious health problem, and you are trying to find him but you cannot. I mean, that is basically——

Mr. ROSENZWEIG. That is it. And, perhaps I will just disagree with you slightly in characterization, but of the three names that we had, two of them to our eyes looked reasonably common, particularly the first name we got and one of the two latter names. Whether they are as common as Rodriguez, that is a value judgment that I——

Chairman LIEBERMAN. Right.

Mr. ROSENZWEIG. But my Rodriguez example was intended to demonstrate that the only way I can guarantee finding one is to take all three names and all the possible dates of birth and run them all separately. And that just creates lots and lots of false positives.

If we have the accurate information with the name-matching algorithm, we can find a person, but even there we are also hobbled by misspellings. One of these names is indeed a complex name, so we can try variants on that spelling. But we do not know what the error is in the information we have until roughly 40 days later when we finally get the match and say, "Ah, of course. If only we had known."

Senator COLLINS. Mr. Chairman.

Chairman LIEBERMAN. Senator Collins.

Senator COLLINS. Could I just follow up on your point?

Chairman LIEBERMAN. Sure.

Senator COLLINS. Because my information is a bit different. First of all, the agency knew that this individual was crossing at the El Paso, Texas, border crossing, so it is not as if we have a huge number of border crossings where this individual is coming through. Surely, that should have helped narrow the search.

Second, the fact is, as I understand it from Customs and Border Protection, the individual was able to cross 21 times after the agency had the correct hyphenated last name, and I agree with the Chairman that this is not like Joe Smith. This last name is a hyphenated, not common last name. And you had the correct date of birth. When you know where the individual is going to be crossing, what his last name is, and his correct date of birth, the fact that the first name is missing seems to me not a sufficient explanation for why there was not a match. You had the middle name, the hyphenated last name, and the correct date of birth, and you know where he is coming from. You know at which border crossing to be on the alert.

So I think this does not fit your example at all. Your example is a compelling one of what can happen, but it does not fit the facts of this case as they have been presented to me.

Mr. ROSENZWEIG. Again, with respect, Senator, I think we are looking at it backwards. We now know that El Paso is the place that he most frequently crossed. In fact, my information is that all of his crossings were not at El Paso but at other ports of entry as well. So, unless we know in advance that is the only place, we are obliged to look everywhere.

I would also say that El Paso is one of the three busiest crossing points in the United States on a daily basis. There are thousands and thousands of people.

It is the case that with the information we had, had we restricted ourselves to that, we could have picked out all the people with those names crossing across the border. But not knowing who he is and without the first name, that would have included everybody who has either of those two hyphens, because you and I now know that is the correct answer, that his name is Rosenzweig-Hahn—and, again, I will not use his personal name. But, with respect, it is a bit of back-seat driving. I cannot know that until I find him. So I have to look at all the Rosenzweigs and all the Hahns in order to be able to be sure that I am getting the right answer.

We try and heighten our scrutiny of those people, but that is a larger number of people than you might suspect.

Senator COLLINS. He was not using an alias. That was the first report that we got from the Department—that was the reason. That turned out not to be the case.

I am really concerned about this. This person was potentially very dangerous from a public health perspective, but what if this had been a terrorist? If a terrorist about whom we have an accurate last name and an accurate middle name and an accurate date of birth could cross 21 times, when you know it is likely where the individual is going to be crossing, that is of huge concern to me. And I say that with all due respect to the good job that is being done on this watch list. We have come a long ways. But if, in fact, with that kind of information a person can cross into our country, that really concerns me.

Mr. ROSENZWEIG. Well, I do not mean to suggest that it does not concern us as well, and certainly with this event we are going to go back and review our procedures on watch list name matching to ensure that we are doing the best that we can. But I do have to say that given the volume of people that we have crossing the land border and not knowing ex ante whether or not we actually have the accurate names—because we have already determined, at least to some degree, that there is something missing because it is not coming up on our system fully. We have to always characterize and balance the risk/benefit of who we are targeting for secondary screening in the devotion of resources.

I have to also say—and I think that this is predictive but accurate—that if the case were somebody who was a terrorist or on the terrorist watch list, which, of course, this person is not because it is a public health risk, we would probably apply a different risk calculus, especially if it were an active investigation of somebody we thought were coming immediately to do harm to the United States. We would stop all the Rosenzweigs and all the Hahns no matter what, and that would just be too bad and a difficult time for the mistakenly stopped ones who would be cleared after secondary. But we have to dial up and dial down the degree of closeness of screening and match that we seek, and at busy ports on the land side, we are disabled by the volume and by the need to process people in 10 seconds, at least as we currently stand, from doing much better.

I should add, by the way, that we have modernization money in our budget, too, $100 million. The screens my guys use are 25 years old for these things, so that is part of the answer, better software and things like that.

Chairman LIEBERMAN. OK. You understand our concern.

Mr. ROSENZWEIG. Absolutely.

Chairman LIEBERMAN. And we are going to stay on this. As one of you said earlier, a terrorism watch list which is based on names obviously has limitations. One of them is if somebody uses an alias that they have not used before. Right, Commissioner? Then we are not going to catch him.

Mr. BOYLE. Yes, sir, unless we have some reason to link that alias with that person.

Chairman LIEBERMAN. To that person. Am I correct in my recollection, surprisingly, that all or most of the September 11, 2001, terrorists actually used their own names?

Mr. BOYLE. For the most part, that is correct.

Chairman LIEBERMAN. That is what I thought, which was amazing. Now, of course, what is perplexing, to put it mildly, about this case of the Mexican national with tuberculosis is that we, our government, had his name from the Mexican health authorities, and we were still, for the reasons you said, not able to stop him. I suppose hindsight is always clearer, but I was interested in what you said, that obviously if we knew this person was a terrorist, even if we had the confusion, in your case we would have stopped everybody with those two names. It is an interesting value judgment when you have somebody with tuberculosis which could cause a real health problem here. I am sure people would have complained, but, again, what I am about to say I say with hindsight, I wish you

had stopped everybody with his two names if that is what was necessary to stop him from coming in. It would have bothered a lot of people, a lot of false positives, but I think overall public interest would have been better served.

Mr. ROSENZWEIG. If I may, sir, and this is a complete throw the ball to somebody else. But in making those kinds of determinations, we rely obviously very strongly on Health and Human Services and the Centers for Disease Control to tell us what they assess is the risk and how much or how little we need to dial up or dial down the matching process. And I am told that we actually had this discussion with HHS, and they made a judgment that they did not want to press for better identification information because that has systematic effects about discouraging people from seeking treatment. That is completely outside of my lane, and it certainly is something you should be interested in following up on. But we take the medical judgments as given to us by our partners. We do not do doctors.

Chairman LIEBERMAN. OK. So, I ask you to keep us posted on your continuing review of this because we are not satisfied yet because we do not want this to happen again, and we know that the GAO report mentions other cases in which people on a watch list earlier this year—or was it last spring—got by and got into the country. And it also reminds us that to the extent that we move to tamper-proof IDs for people to come into the country who are able to make that easily entered into an electronic system and that we move to biometrics to the extent that we have biometrics on people, that is obviously at a higher level of certainty.

But I want to come back to the beginning because I think the important thing is that the Terrorist Screening Center and the accumulation of lists and the process you have has raised our guard much higher than it was before and on September 11, 2001. For that we thank you. And I guess the other part of this clearly is that there is more to do. We have a big country, and a lot of people coming in and out of it every day, astounding numbers, really—legally I am talking about, not even illegally—and how we do our best using modern technology to filter out those who either are dangerous to us in terms of terrorism or health is critically important. So I thank you.

Senator Collins, do you want to add anything?

Senator COLLINS. No, thank you.

Chairman LIEBERMAN. Thanks very much for what you have been doing. The hearing record will be open for 15 days for Members to submit additional questions to you and for you to answer some of the questions. Senator Warner, I know, would particularly like an answer to his question for the record.

I thank you very much. The hearing is adjourned.

[Whereupon, at 12:18 p.m., the Committee was adjourned.]

APPENDIX

United States Government Accountability Office

GAO

Testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. EDT
Wednesday, October 24, 2007

TERRORIST WATCH LIST SCREENING

Recommendations to Enhance Management Oversight, Reduce Potential Screening Vulnerabilities, and Expand Use of the List

Statement of Eileen R. Larence, Director
Homeland Security and Justice Issues

GAO-08-194T

October 2007

GAO
Accountability · Integrity · Reliability
Highlights

Highlights of GAO-08-194T, a testimony before the Committee on Homeland Security and Governmental Affairs, United States Senate

TERRORIST WATCH LIST SCREENING

Recommendations to Enhance Management Oversight, Reduce Potential Screening Vulnerabilities, and Expand Use of the List

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.

This testimony discusses (1) standards for including individuals on the list, (2) the outcomes of encounters with individuals on the list, (3) potential vulnerabilities in screening processes and efforts to address them, and (4) actions taken to promote effective terrorism-related screening.

This statement is based on GAO's report (GAO-08-110) being released at this hearing. To accomplish the objectives, 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 recommends several actions 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.

The departments that provided comments on the report generally agreed with GAO's findings and recommendations.

To view the full product, including the scope and methodology, click on GAO-08-194T. For more information, contact Eileen Larence at (202) 512-8777 or larencee@gao.gov.

What GAO Found

The FBI and the intelligence community use standards of reasonableness to evaluate individuals for nomination to the consolidated terrorist 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.

Mr. Chairman and Members of the Committee:

I am pleased to be here today to discuss our report on U.S. efforts to develop and use the terrorist watch list to screen for known or suspected terrorists who pose a threat to homeland security. The list is an important tool in the government's overall efforts to combat terrorism.

The Terrorist Screening Center (TSC) is responsible for maintaining the watch list and providing for its use during agency screening processes. TSC receives the vast majority of its watch list records from the National Counterterrorism Center, which compiles information on known or suspected international terrorists from executive branch departments and agencies. In addition, the Federal Bureau of Investigation (FBI) provides TSC with information on known or suspected domestic terrorists who operate primarily within the United States, such as Ted Kaczynski (the "Unabomber"). TSC consolidates this information into its watch list database and makes records available for a variety of screening purposes, such as the screening of visa applicants and the screening of airline passengers. When an individual on the watch list is encountered during screening, several entities—TSC, the screening agency, investigative agencies, and the intelligence community—can be involved in deciding what action to take, if any.

My testimony today discusses (1) the standards agencies use for including individuals on the list, (2) the outcomes of encounters with individuals on the list, (3) potential vulnerabilities in agencies' watch list screening processes and efforts to address them, and (4) actions taken to promote effective terrorism-related screening.

This statement is based on the report we released today.[1] To accomplish our report objectives, we reviewed procedural guidance, statistics, and other relevant 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. Specifically, at the Transportation Security Administration, we examined the prescreening of airline passengers prior to their boarding a flight; at U.S. Customs and Border Protection, we examined the screening

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

of travelers entering the United States through ports of entry; and at the Department of State, we examined the screening of visa applicants. We conducted our work in accordance with generally accepted government auditing standards.

Summary

In summary, we found the following:

- The National Counterterrorism Center and the FBI rely upon standards of reasonableness in determining which individuals are appropriate for inclusion on TSC's consolidated terrorist 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, inclusion on the list does not automatically prohibit an individual from, for example, obtaining a visa or entering the United States. As of May 2007, TSC's watch list contained approximately 755,000 records.

- From December 2003 (when TSC began operations) through May 2007, agencies encountered individuals who were on the watch list about 53,000 times. Many individuals were encountered multiple times. Actions taken in response included arresting individuals and denying others entry into the United States. Most often, however, agencies questioned and then released the individuals because there was not sufficient evidence of criminal or terrorist activity to warrant further legal action. Nevertheless, such questioning allowed agencies to collect information on the individuals, which was shared with law enforcement agencies and the intelligence community.

- Screening agencies do not check against all records in the consolidated watch list, partly because screening against certain records (1) may not be needed to support the respective agency's mission or (2) may not be possible due to the requirements of computer programs used to check individuals against watch list records. Not checking against all records may pose a security risk. 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. Federal agencies have ongoing initiatives to help reduce these potential vulnerabilities.

- The federal government has made progress in using the consolidated watch list for screening purposes, but it has not (1) finalized guidelines for using watch list records within critical infrastructure components of the private sector or (2) identified all appropriate opportunities for

which terrorist-related screening should be applied. Further, the government lacks an up-to-date strategy and implementation plan—supported by a clearly defined leadership or governance structure—which are important for enhancing the effectiveness of terrorist-related screening.

We have recommended several actions to promote a more 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. The Department of Homeland Security and the FBI, which provided the Department of Justice's comments on a draft of the report, generally agreed with our findings and recommendations. The Homeland Security Council was provided a draft of the report but did not provide comments.[2]

Background

Pursuant to Homeland Security Presidential Directive 6, the Attorney General established TSC in September 2003 to consolidate the government's approach to terrorism screening and provide for the appropriate and lawful use of terrorist information in screening processes. TSC's consolidated watch list is the U.S. government's master repository for all records of known or appropriately suspected international and domestic terrorists used for watch list-related screening.

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

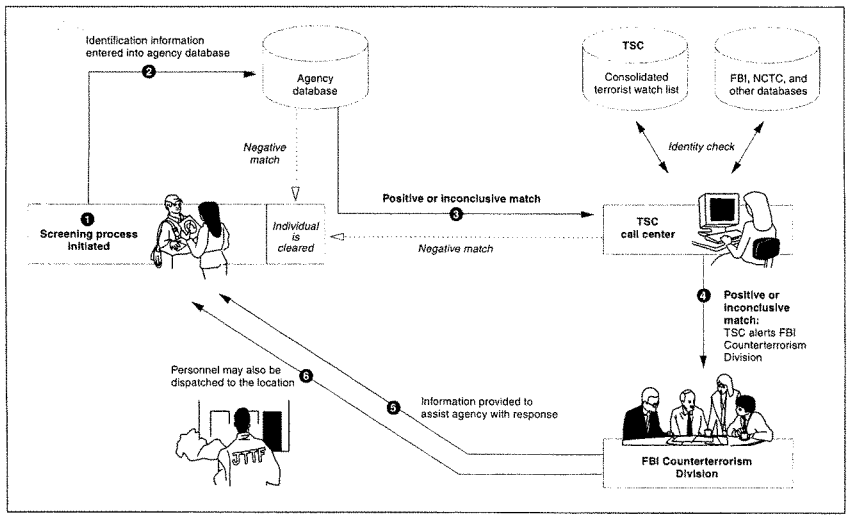
[2]The Homeland Security Council was established to ensure coordination of all homeland security-related activities among executive departments and agencies and promote the effective development and implementation of all homeland security policies. See The White House, *Homeland Security Presidential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

report on terrorist watch list screening.[3] However, clearly positive or exact matches and matches that are inconclusive (difficult to verify) generally are to be referred to TSC to confirm whether the individual is a match to the watch list record. TSC is to refer positive and inconclusive matches to the FBI to provide an opportunity for a counterterrorism response. Deciding what action to take, if any, can involve collaboration among the frontline screening agency, the National Counterterrorism Center or other intelligence community members, and the FBI or other investigative agencies. 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.[4] 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.

[3]Terrorist 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).

[4]Joint 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 Homeland Security Presidential Directive 6, in August 2004, the President signed Homeland Security Presidential Directive 11. 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 screening. 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.

Agencies Rely upon Standards of Reasonableness in Assessing Individuals for Inclusion on TSC's Watch List

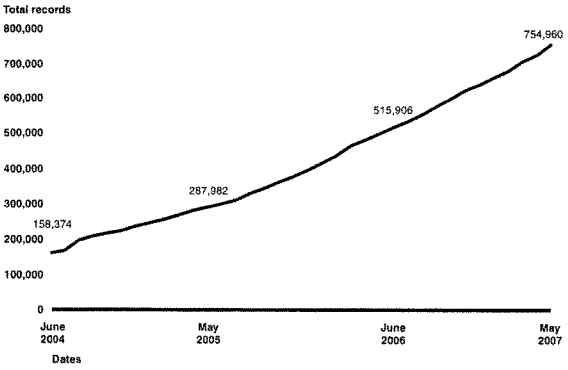
The National Counterterrorism Center and the FBI rely upon standards of reasonableness in determining which individuals are appropriate for inclusion on TSC's consolidated watch list.[5] In accordance with Homeland Security Presidential Directive 6, TSC's watch list is to contain information about individuals "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, the National Counterterrorism Center 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. 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 TSC for inclusion on the watch list, including persons who are being preliminarily investigated to determine if they have links to terrorism. In determining whether to open an investigation, the FBI uses guidelines established by the Attorney General. These guidelines contain specific standards for opening investigations, including formal review and approval processes. 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. If an investigation does not establish a terrorism link, the FBI generally is to

[5]In 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).

close the investigation and request that TSC remove the person from the watch list. Based on these standards, the number of records in TSC's consolidated watch list has increased from about 158,000 records in June 2004 to about 755,000 records as of May 2007 (see fig. 2). It is important to note that the total number of records in 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.

Figure 2: Increase in Terrorist Watch List Records, June 2004 through May 2007



Source: GAO analysis of TSC data.

TSC's watch list database is updated daily with new nominations, modifications to existing records, and deletions. 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 when the person is identified by a screening agency. 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.

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

From December 2003 (when TSC 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 TSC data. A breakdown of these encounters shows that the number of matches has increased each year—from 4,876 during the first 10-month period of TSC's operations 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. Our analysis of TSC data also indicates that many individuals 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 involved screening within the United States by a state or local law enforcement agency, U.S. government investigative agency, or other governmental entity. The next highest percentage involved border-related encounters, such as passengers on airline flights inbound from outside the United States or individuals screened at land ports of entry. The lowest percentage of encounters occurred outside of the United States.

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 on 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.

- 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.[6]

- Transportation Security Administration 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.[7] 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. Additional information on individuals on the watch list passing undetected through agency screening is presented later in this statement.

- U.S. Customs and Border Protection 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, the agency determined there was sufficient information related to watch list records to preclude admission under terrorism grounds. However, for most of the encounters, the agency determined that there was not sufficient 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 released, unless there were reasons other than terrorism-related grounds for arresting or detaining the individuals, such as the individual having an outstanding arrest warrant.

Also, 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

[6]In this context, ineligibility waived refers to individuals who were ineligible for a visa based on terrorism grounds, but the Department of Homeland Security 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.

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

opportunity to collect additional information about the individual. The information collected 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.

Potential Vulnerabilities in Agency Screening Processes and Agency Efforts to Address Them

The principal screening agencies whose missions most frequently and directly involve interactions with travelers do not check against all records in TSC's consolidated watch list because screening against certain records (1) may not be needed to support the 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. Rather, each day, TSC 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 records on U.S. citizens and lawful permanent residents because these individuals would not apply for U.S. visas.

The FBI database that state and local law enforcement agencies use for screening contained the third highest percentage of watch list records. According to the FBI, the remaining records were not included in this database primarily because they did not contain sufficient identifying information on the individual, 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 the nomination criteria for the No Fly or Selectee list or (2) did not contain

sufficient identifying information on the individual.[8] 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. While we understand the FBI's and the Department of Homeland Security's concerns about misidentifications, we still believe it is important that federal officials assess the extent to which security risks exist by not screening against certain watch list records and what actions, if any, should be taken in response.

Also, Department of Homeland Security component agencies are taking steps to address instances of individuals on the watch list passing undetected through agency screening. For example, U.S. Customs and Border Protection has encountered situations where it identified the subject of a watch list record after the individual had been processed at a port of entry and admitted into the United States. U.S. Customs and Border Protection has created a working group within the agency to study the causes of this vulnerability and 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 to determine the cause, with appropriate follow-up and corrective action taken, if needed. The agency is also working with TSC 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 checks passenger names 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

[8]Of all of the screening 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 Homeland Security Presidential Directive 6.

some instances resulted in diverting the aircraft to a new location.[9] 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.[10] For domestic flights within the United States, there is no second screening opportunity—like the one U.S. Customs and Border Protection conducts for international 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. Also, TSC has ongoing initiatives to help reduce instances of individuals on the watch list passing undetected through agency screening, including efforts to improve computerized name-matching programs.

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

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

[9]In 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).

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

have a substantial bearing on homeland security. Finalizing such guidelines would help both the private sector and the Department of Homeland Security ensure that private sector entities are using watch list records consistently, appropriately, and effectively to protect their workers, visitors, and key critical assets. Further, federal departments and agencies have not identified all appropriate opportunities for which terrorist-related screening will 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 directives. Without an up-to-date strategy and plan, agencies and organizations that conduct 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 presidential directives, 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.

Although all elements of a strategy and implementation plan cited in presidential directives 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. 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. Thus, it is important that the Assistant to the President for Homeland Security and Counterterrorism address these deficiencies by ensuring that an appropriate governance structure has 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.

Conclusions and Recommendations for Executive Action

Managed by TSC, the consolidated 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, expanding use of the watch list, and enhancing management oversight. Thus, we have made several recommendations to the heads of relevant departments and agencies. Our recommendations are intended to help (1) mitigate security vulnerabilities in terrorist watch list screening processes that arise when screening agencies do not use certain watch list records and (2) optimize the use and effectiveness of the watch list as a counterterrorism tool. Such optimization should include development of guidelines to support private sector screening processes that have a substantial bearing on homeland security, as well as development of an up-to-date strategy and implementation plan for using terrorist-related information. Further, to help ensure that governmentwide terrorist-related screening efforts are effectively coordinated, we have also recommended that the Assistant to the President for Homeland Security and Counterterrorism ensure that an appropriate leadership or governance structure has clear lines of responsibility and authority.

Agency Comments and Our Evaluation

In commenting on a draft of our report, which provides the basis for my statement at today's hearing, the Department of Homeland Security 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 FBI noted that the database state and local law enforcement agencies use for screening does not contain certain watch list records primarily to minimize instances of individuals being misidentified as subjects of watch list records. Because of this operational concern, the FBI noted that our recommendation to assess the extent of vulnerabilities in current screening processes 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 security risks are raised by not screening against certain watch list records and what actions, if any,

should be taken in response. Also, the FBI noted that TSC'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 our report, TSC's governance board is 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. The Homeland Security Council was provided a draft of the report but did not provide comments.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members have at this time.

GAO Contacts and Staff Acknowledgments

For questions regarding this testimony, please contact me at (202) 512-8777 or larencee@gao.gov. Other key contributors to this statement 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, and Ronald J. Salo.

Office of the Inspector General
United States Department of Justice

Statement of Glenn A. Fine
Inspector General, U.S. Department of Justice

before the

Senate Committee on Homeland Security and
Governmental Affairs

concerning

Watching the Watchlist:
Building an Effective Terrorist Screening System

October 24, 2007

Statement of Glenn A. Fine
Inspector General, U.S. Department of Justice
before the
Senate Committee on Homeland Security and Governmental Affairs
concerning
"Watching the Watchlist:
Building an Effective Terrorist Screening System"

I. Introduction

Mr. Chairman, Senator Collins, and Members of the Committee on Homeland Security and Governmental Affairs:

I appreciate the opportunity to testify before the Committee on the development and status of the terrorist watchlist screening system. For the past several years, the Department of Justice Office of the Inspector General (OIG) has examined the work of the Terrorist Screening Center (TSC), which is a multi-agency effort administered by the Federal Bureau of Investigation (FBI). Created in 2003, the TSC integrates U.S. government terrorist watchlists into a consolidated database and provides 24-hour, 7-day a week responses to federal, state, and local governments to assist in screening for individuals with possible ties to terrorism. Prior to the establishment of the TSC, the federal government's terrorist screening system was fragmented, relying on at least a dozen separate watchlists maintained by different federal agencies.

In June 2005, the OIG issued its first audit of the TSC's operations. Our 2005 audit found that the TSC had made significant strides in becoming the government's single point-of-contact for law enforcement authorities requesting assistance in identifying individuals with possible ties to terrorism. However, we also found weaknesses in various areas of TSC operations, including that the TSC had not ensured that the information in the consolidated terrorist watchlist database was complete and accurate.

In September of this year, we completed a follow-up review examining the TSC's progress in improving its operations and addressing certain recommendations in our 2005 audit. Our follow-up review found that the TSC had continued to make progress in several important areas. For example, the TSC had enhanced its efforts to ensure the quality of watchlist data, had increased staff assigned to data quality management, and had developed a process and a separate office to address complaints filed by persons complaining that they are included on the terrorist watchlist by mistake.

Yet, we also determined that the TSC's management of the watchlist continues to have significant weaknesses, and that the data in the watchlist database was not complete or fully accurate.

Thus, while the TSC is a critical participant in the government's counterterrorism effort and TSC employees deserve credit for creating a consolidated watchlist, weaknesses remain in the TSC's operations and watchlisting process. These weaknesses can have enormous consequences. Inaccurate, incomplete, and obsolete watchlist information can increase the risk of not identifying known or suspected terrorists, and it can also increase the risk that innocent persons will be stopped or detained. For these reasons, we believe it critical for the TSC, and the agencies providing information for inclusion in the consolidated watchlist database, to further improve the accuracy of the data and their efforts to remove inaccurate information.

In this statement, I provide further details on these conclusions. First, I briefly provide background on the operation of the TSC. I then summarize the findings of the two OIG reports on the TSC's operations. Finally, I note for the Committee ongoing reviews by our office and other Inspectors General in the Intelligence Community that are further examining the watchlist nomination process.

II. Background

A. Creation of the TSC

Prior to the establishment of the TSC, the federal government relied on many separate watchlists maintained by different federal agencies for screening individuals who, for example, apply for a visa, attempt to enter the United States through a port-of-entry, attempt to travel internationally on a commercial airline, or are stopped by a local law enforcement officer for a traffic violation.

Homeland Security Presidential Directive-6 (HSPD-6), signed on September 16, 2003, required the creation of the TSC to integrate the existing U.S. government terrorist watchlists and provide 24-hour, 7-day a week responses for agencies that use the watchlisting process to screen individuals. HSPD-6 mandated that the TSC achieve initial operating capability by December 1, 2003.

Following the issuance of HSPD-6, the Attorney General, the Director of Central Intelligence, and the Secretaries of the Department of Homeland Security (DHS) and the Department of State entered into a Memorandum of Understanding (MOU) describing the new TSC organization and the level of necessary cooperation, including the sharing of staff and information from the four participating agencies. The MOU stipulated that the Director of the TSC would report to the Attorney General through the FBI. As a result, the FBI administers the TSC, although the Principal Deputy Director of the TSC must be an employee of the DHS.

Since fiscal year (FY) 2004, the participating agencies have shared responsibility for funding and staffing the TSC. For FY 2007, the TSC had a budget of approximately $83 million and a staffing level of 408 positions.

B. The TSC's Role in the Watchlist Process

When a law enforcement or intelligence agency identifies an individual as a potential terrorist threat to the United States and wants that individual watchlisted, the source agency nominates that person for inclusion in the consolidated watchlist maintained by the TSC. As additional information is obtained that either enhances the identifying information or indicates that the individual has no nexus to terrorism, the record should be updated or deleted.

The TSC shares the information contained in its Terrorist Screening Database by exporting or sending data "downstream" to other screening systems, such as the State Department's Consular Lookout and Support System (CLASS), DHS's Interagency Border Inspection System (IBIS), the Transportation Security Administration's (TSA) No Fly list, the FBI's Violent Gang and Terrorist Organization File (VGTOF) within its National Crime Information Center (NCIC) system, and others. Watchlist information is then available for use by U.S. law enforcement and intelligence officials across the country and around the world.

Law enforcement or intelligence personnel routinely encounter individuals as part of their regular duties. For example: (1) DHS agents of the U.S. Customs and Border Protection agency examine individuals at various U.S. ports-of-entry and search IBIS to determine if a person can be granted access to the United States, (2) State Department officials process visa applications from non-U.S. citizens wishing to visit the United States and search CLASS to determine if the individual should be granted a U.S. visa, and (3) state and local law enforcement officers query the FBI's NCIC system to review information about individuals encountered through the criminal justice system. These databases and lists contain terrorist watchlist records to assist screening agents in identifying persons that the U.S. government has determined are known or suspected terrorists.

When a name appears to be a match against the terrorist watchlist, requestors receive a return message through their database informing them of the preliminary match and directing them to call the TSC. When a call is received, TSC staff in the 24-hour call center assist in confirming the subject's identity.

These matches may be actual watchlist subjects, individuals misidentified to a terrorist identity, or someone mistakenly included on the watchlist. In responding to such a call, TSC Call Center staff search the consolidated database and other databases to determine if a terrorist watchlist identity match exists.

Records within the consolidated watchlist database also contain information about the law enforcement action to be taken when encountering the individual. This information is conveyed through "handling codes" or instructions – one handling code for the FBI and one for the DHS. The FBI's handling codes are based on whether there is an active arrest warrant, a basis to detain the individual, or an interest in obtaining additional intelligence information regarding the individual. DHS handling instructions provide screeners with information on how to proceed with secondary screening of the individual.

Between the TSC's inception in December 2003 and May 2007, the TSC has documented more than 99,000 encounters for which its call center was contacted. TSC data shows that 53.4 percent of these calls were determined to be a positive match to a terrorist watchlist identity in the consolidated database. In those cases, the TSC contacted the FBI, which is responsible for initiating any necessary law enforcement action. In 43.4 percent of the encounters, it was determined that the individual did not match the watchlisted identity. In the remaining 3.2 percent of the encounters, the TSC Call Center staff could not definitively determine if the match was positive or negative and therefore forwarded these calls to the FBI.

Since creation of the TSC in December 2003, the number of records in the consolidated watchlist database of known or suspected terrorists has significantly increased. According to TSC officials, in April 2004 the consolidated database contained approximately 150,000 records. It is important to note that because multiple records may pertain to one individual, the number of individuals in the database is fewer than the total number of records.

TSC data indicate that by July 2004 the number of records in the consolidated database had increased to about 225,000, representing approximately 170,000 individuals. In February 2006, the TSC reported that the database contained approximately 400,000 records. Most recently, information we obtained from the TSC indicates that the consolidated database contained 724,442 records as of April 30, 2007. According to the TSC, these records relate to approximately 300,000 individuals.

III. The OIG's June 2005 Audit of the TSC

In June 2005, the OIG issued an audit of the TSC's operations. As mentioned previously, the OIG review found that the TSC had made significant strides in becoming the government's single point-of-contact for assistance in identifying individuals with possible ties to terrorism. The TSC began operating as the nation's centralized terrorist screening center by the mandated December 1, 2003, date. Several months later, the TSC began

using a terrorist screening database that contained consolidated information from a variety of existing watchlist systems.

Yet, while the TSC had deployed a consolidated watchlist database, the OIG report found that the TSC had not ensured that the information in that database was complete and accurate. For example, the OIG found that the consolidated database did not contain names that should have been included on the watchlist. In addition, the OIG found inaccurate or inconsistent information related to persons included in the database.

Due to its rapid start-up and the need for personnel with adjudicated security clearances, the TSC had been heavily dependent upon staff and supervisors detailed from participating agencies who generally worked at the TSC for only 60 to 90 days. Moreover, due to the temporary assignments of call center supervisors, the TSC had difficulty developing and implementing standard oversight procedures for call center personnel, and at times provided incorrect instructions to call center staff. This lack of sufficient training, oversight, and general management of the call screeners left the call center vulnerable to errors, poor data entry, and untimely responses to callers. We also found problems with the TSC's management of its information technology, a crucial facet of the terrorist screening process.

The OIG report also concluded that the TSC needed to better address instances when individuals were mistakenly identified as a "hit" against the consolidated database (also referred to as misidentifications). Finally, the audit found that the TSC would benefit from formalizing its strategic planning efforts, enhancing its outreach efforts to inform the law enforcement and intelligence communities of its role and functions, and expanding its ability to assess the effectiveness and performance of the organization. The OIG report provided 40 recommendations to the TSC to address areas such as database improvements, data accuracy and completeness, call center management, and staffing. The TSC generally agreed with the recommendations and said it had, or would, take corrective actions.

IV. The OIG's September 2007 Follow-up Audit on TSC Operations

In September 2007, the OIG issued a follow-up audit assessing the progress of the TSC in improving its operations. Our audit examined the TSC's efforts to ensure that accurate and complete records were disseminated to and from the watchlist database in a timely fashion and the TSC's efforts to ensure the quality of the information in the watchlist database. The review also examined the TSC's process to respond to complaints raised by individuals who believe they have been incorrectly identified as watchlist subjects.

In conducting this audit, we interviewed more than 45 officials and reviewed numerous TSC documents. To evaluate the accuracy and completeness of the consolidated watchlist, we analyzed the consolidated

database as a whole, and reviewed the number of records in the database and any duplication that existed within those records. We also tested individual records for accuracy and completeness, as well as the timeliness of any related quality assurance activities.

Overall, our follow-up audit found that the TSC had enhanced its efforts to ensure the quality of watchlist data, had increased staff assigned to data quality management, and had developed a process and a separate office to address complaints filed by persons seeking relief from adverse effects related to terrorist watchlist screening. In these areas, we credited the TSC for significant progress in improving its operations.

However, we also determined that the TSC's management of the watchlist has significant continuing weaknesses. For example, our review revealed instances where known or suspected terrorists were not appropriately watchlisted on screening databases that frontline screening agents (such as border patrol officers, visa application reviewers, or local police officers) use to identify terrorists and obtain instruction on how to appropriately handle these subjects.

Even a single omission of a terrorist identity or an inaccuracy in the identifying information contained in a watchlist record can have enormous consequences. Inaccuracies in watchlist data increase the possibility that reliable information will not be available to frontline screening agents, which could prevent them from successfully identifying a known or suspected terrorist during an encounter or place their safety at greater risk by providing inappropriate handling instructions for a suspected terrorist. Furthermore, inaccurate, incomplete, and obsolete watchlist information increases the chances of innocent persons being stopped or detained during an encounter because of being misidentified as a watchlist identity.

Our review also found that, due to technological differences and capabilities of the various systems used in the watchlist process, the TSC still maintains two interconnected versions of the watchlist database. The TSC is developing an upgraded consolidated database that will eliminate the need to maintain parallel systems. However, in the meantime these two databases should be identical in content and therefore should contain the same number of records. Yet, we discovered during our review that these two systems had differing record counts.

We also found that the number of duplicate records in the TSC database has significantly increased. Multiple records containing the same unique combination of basic identifying information can needlessly increase the number of records that a call screener must review when researching a specific individual. In addition, when multiple records for a single identity exist, it is essential that the identifying information and handling instructions for contact with the individual be consistent in each record. Otherwise, the screener may

mistakenly rely on one record while a second more complete or accurate record may be ignored. Furthermore, inconsistent handling instructions contained in duplicate records may pose a safety risk for law enforcement officers or screeners.

In addition, we found that not all watchlist records were being sent to downstream screening databases. Our testing of a sample of 105 watchlist records revealed 7 watchlist records that were not exported to all appropriate screening databases. As a result of the TSC's failure to export all terrorist watchlist records to screening databases, watchlisted individuals could be inappropriately handled during an encounter. For example, a known or suspected terrorist could be erroneously issued a U.S. visa or unknowingly allowed to enter the United States through a port-of-entry. We discussed these records with TSC officials who agreed with our findings and began correcting these omissions.

Our review also found that the TSC did not have a process for regularly reviewing the contents of the consolidated database to ensure that only appropriate records were included on the watchlist. TSC officials told us that they would perform a monthly review of the database to identify records that are being stored in the database that are not being exported to downstream systems. We also believe it is essential that the TSC regularly review the database to ensure that all outdated information is removed, as well as to affirm that all appropriate records are watchlisted.

Our review determined that because of internal FBI watchlisting processes, the FBI bypasses the normal terrorist watchlist nomination process for international terrorist nominations and instead enters international nominations directly into a downstream screening system. This process is not only cumbersome for the TSC, but it also results in the TSC being unable to ensure that consistent, accurate, and complete terrorist information from the FBI is disseminated to frontline screening agents in a timely manner. As a result, in our report we recommended that the FBI and TSC work together to design a more consistent and reliable process by which FBI-originated international terrorist information is provided for inclusion in the consolidated watchlist.

We concluded that the TSC needs to further improve its efforts for ensuring the quality and accuracy of the watchlist records. We found that since our last report the TSC had increased its quality assurance efforts and implemented a data quality improvement plan. In general, we believe the actions the TSC has taken to improve quality assurance are positive steps. We also recognize that it is impossible to completely eliminate the potential for errors in such a large database. However, continuing inaccuracies that we identified in watchlist records that had undergone the TSC's quality assurance processes underscore the need for additional actions to ensure the accuracy of the database.

For example, the TSC completed a special quality assurance review of the TSA's No Fly list, which reduced the number of records on the list. Our review of a sample of records examined during of this special review process identified virtually no errors. In contrast, our examination of the TSC's routine quality assurance reviews revealed continued problems. Specifically, we examined 105 records subjected to the TSC's routine quality assurance review and found that 38 percent of the records we tested continued to contain errors or inconsistencies that were not identified through the TSC's routine quality assurance efforts. Thus, although the TSC had clearly increased its quality assurance efforts since our last review, it continues to lack important safeguards for ensuring data integrity, including a comprehensive protocol outlining the TSC's quality assurance procedures and a method for regularly reviewing the work of its staff to ensure consistency.

Our audit also expressed concerns that the TSC's ongoing quality assurance review of the consolidated watchlist will take longer than projected by the TSC. At the time of our audit field work in April 2007, the TSC was continuing its efforts to conduct a record-by-record review of the consolidated watchlist and anticipated that all watchlist records would be reviewed by the end of 2007. However, the watchlist database continues to increase by more than 20,000 records per month and as of April 2007 contained over 700,000 records. Given this growth and the time it takes for the TSC's quality assurance process, we believe the TSC may be underestimating the time required to sufficiently review all watchlist records for accuracy.

With regard to addressing complaints from individuals about their possible inclusion on the watchlist, we found that the TSC's efforts to resolve complaints have improved since our previous audit. In 2005, the TSC created a dedicated unit to handle such matters. The TSC also helped to spearhead the creation of a multi-agency Memorandum of Understanding (MOU) focusing on watchlist redress (Redress MOU) and developed comprehensive redress procedures. Currently, frontline screening agencies such as the DHS and the State Department receive complaints from persons seeking relief related to the terrorist watchlist screening process. Matters believed to be related to a terrorist watchlist identity or to an encounter involving the watchlist are forwarded to the TSC. The TSC Redress Office conducts an examination of the watchlist records, reviews other screening and intelligence databases, and coordinates with partner agencies for additional information and clarification. The TSC determines if any records need to be modified or removed from the watchlist, ensures these changes are made, and notifies the referring frontline screening agency of the resolution. The frontline screening agency is then responsible for responding to the complainant.

To test the TSC's redress procedures, we selected 20 redress complaints received by the TSC between January 2006 and February 2007 and reviewed the corresponding files to determine if the TSC followed its redress procedures.

We found that in each of the sampled cases the TSC complied with its redress procedures, including reviewing the applicable screening and intelligence databases, coordinating with partner agencies, and reaching appropriate resolutions.

However, we also noted that the TSC's redress activities identified a high rate of error in watchlist records. The high percentage of records in the redress process requiring modification or removal points to deficiencies in the terrorist watchlisting process. We believe that the results of the TSC's redress reviews are a further indicator that watchlist data needs continuous monitoring and attention.

In addition, we believe the TSC needs to address the timeliness of redress complaint resolutions. We reviewed TSC files and statistics for closed redress matters to examine the efficiency of redress reviews. This data revealed that it took the TSC, on average, 67 days to close its review of a redress inquiry. Our review of redress files indicated that delays were primarily caused by three factors: (1) the TSC took a long time to finalize its determination before coordinating with other agencies for additional information or comment, (2) nominating agencies did not provide timely feedback to the TSC or did not process watchlist paperwork in a timely manner, and (3) certain screening agencies were slow to update their databases with accurate and current information.

TSC officials acknowledged that it has not developed response timeframes for redress matters with its partner agencies. While the Redress MOU states that one of the goals of the redress process is to provide a timely review, the MOU does not define what constitutes a reasonable timeframe. Because the TSC is central to resolving any complaint regarding the content of the consolidated terrorist watchlist, we recommended that the TSC organize the U.S. government's effort to develop timeliness measures for the entire watchlist redress process.

In addition, we found the TSC does not have any policy or procedures to proactively use information from encounters to reduce the incidence and impact of watchlist misidentifications. For example, the TSC could program its tracking system to automatically generate a quality assurance lead for the TSC to perform a review of watchlist records that have been the subject of a certain number of encounters with individuals that were not a positive match to the watchlist record. Moreover, the TSC's strategic plan does not include goals or actions associated with reducing the incidence of misidentifications or the impact on misidentified persons other than that covered by a formal redress process. Considering that nearly half of all encounters referred to the TSC Call Center are negative for a watchlist match, we recommended that the TSC consider misidentifications a priority and develop strategic goals and policy for mitigating the adverse impact of the terrorist screening process on non-

watchlist subjects, particularly for individuals who are repeatedly misidentified as watchlist identities.

In total, our report made 18 recommendations to further improve the TSC's watchlisting process and the quality of the watchlist data. These recommendations include making further improvements to increase the quality of watchlist data; revising the FBI's watchlist nominations process; and developing goals, measures, and timeliness standards related to the redress process. In response, the TSC agreed with the recommendations and stated that it would take corrective action.

V. Ongoing Reviews of Watchlist Nomination Process

The OIG is currently conducting a separate audit examining the watchlist nominations processes in the Department of Justice. This audit is examining the specific policies and procedures of Department components for nominating individuals to the consolidated watchlist. The audit also is reviewing the training provided to the individuals who are involved in the nominating process. The Department components we are reviewing include the FBI, the Drug Enforcement Administration, the Bureau of Alcohol, Tobacco, Firearms and Explosives, and the United States Marshals Service.

We are conducting this review in conjunction with other Intelligence Community OIGs, who are examining the watchlist nomination process in their agencies. The OIG reviews, which are being coordinated by the OIG for the Office of the Director of National Intelligence, include OIGs in the Departments of State, Treasury, Energy, Homeland Security, and others.

VI. Conclusion

In conclusion, the TSC deserves credit for creating and implementing a consolidated watchlist and for making significant progress in improving the watchlist and screening processes. However, our reviews have found continuing weaknesses in some of those processes and in the quality of the data in the consolidated database. We believe it is critical that the TSC further improve the quality of its watchlist data and its redress procedures. Inaccurate, incomplete, and obsolete watchlist information can increase the risk of not identifying known or suspected terrorists, and it can also increase the risk that innocent persons will be repeatedly stopped or detained. While the TSC has a difficult task and has made significant progress, we believe it needs to make additional improvements.

That concludes my statement and I would be pleased to answer any questions.

Statement of Leonard Boyle,
Director,
Terrorist Screening Center,
Before the Senate Homeland Security and Governmental Affairs Committee,
24 October 2007

Good morning Chairman Lieberman, Ranking Member Collins, and members of the Committee. Thank you for the opportunity to discuss the Government Accountability Office (GAO) report, its findings and the watchlisting process at large.

Since its inception on December 1, 2003, the Terrorist Screening Center (TSC) has assumed a critical role in securing our borders and the safety of the American people by providing to the nation's entire screening and law enforcement communities the identities of known and suspected terrorists. As directed by Homeland Security Presidential Directive 6 (Integration and Use of Screening Information), the TSC has combined the 12 previously existing terrorist watchlists and created the United States Government's single consolidated Terrorist Screening Data Base (TSDB). Every day, the TSC provides an updated list of known and suspected terrorists to screeners and law enforcement personnel. The TSC also provides:

(1) A single coordination point for terrorist screening data;
(2) A 24/7 call center to provide identification assistance to screening agencies;
(3) Access to a coordinated law enforcement response for any encounter with a watchlisted person;
(4) A formal process for tracking all positive encounters;
(5) Feedback to the appropriate entities;

(6) A redress process for any individual who believes they have been improperly delayed or otherwise inconvenienced because of the watchlist; and
(7) A process for removing names from the watchlist when it has been conclusively determined they do not have a nexus to terrorism.

The TSC has significantly enhanced interagency cooperation in the post-9/11 culture where information sharing is a MUST. In fact, as the GAO report cites, "The TSC plays a central role in the real-time sharing of information, creating a bridge among screening agencies." The TSC has not only assisted in eliminating historical cultural boundaries between and among the intelligence and law enforcement communities, but also has provided a physical mechanism to ensure information sharing is done in an efficient manner.

As the GAO report correctly notes, while great strides have been made there is still room for improvement in the terrorist screening process. I must echo what my colleagues have said many times: In order to be successful in the war on terrorism, we must constantly improve, determining our weaknesses from within, and correcting them. The TSC's unique position as the U.S. Government's hub for all terrorist identification information allows the TSC to play a critical role regarding the GAO Executive Recommendations, especially with respect to identifying further screening opportunities while serving in a leadership role for the screening community.

TSC Initiatives

In fact, the TSC has already moved forward in a number of areas, which will result in a more complete and efficient screening process.

- TSC is working hand-in-hand with the Transportation Security Administration (TSA) regarding its "Secure Flight" initiative.
- TSC participates in an interagency working group to identify how to better use biometric data to enhance the screening process.

- While maintaining all privacy rules and policies, TSC is undertaking information technology improvements on several fronts, including ways to increase the ease with which our screening and law enforcement customers are able to access the TSDB.
- TSC has partnered with the Directorate of National Intelligence (DNI) to initiate a working group to evaluate the different name match algorithms currently in use by different agencies during the screening process. This effort will result in the TSC developing a search engine to improve name matching, and allowing screening and law enforcement agencies direct query access to the TSDB.

TSC Achievements

One of the TSC's most recent accomplishments is the September 19, 2007 execution of a multi-agency agreement on the terrorist watchlist redress process. The TSC terrorist watchlist redress process, established in January 2005, provides a full and fair review of any watchlist record that is the cause of an individual's complaint. The redress process seeks to identify any data errors and correct them, including errors in the watchlist itself. The TSC worked with the Privacy and Civil Liberties Board, and obtained cabinet-level commitments from participating agencies, to include the Attorney General, Secretaries of State, Treasury, Defense and Homeland Security, the Director of National Intelligence, and the Directors of the National Counterterorrism Center, Central Intelligence Agency, and Federal Bureau of Investigation, to support the redress process with appropriate resources and oversight from senior agency officials. Furthermore, this agreement ensures uniformity in the handling of watchlist related complaints and demonstrates the United States Government's commitment to protecting national security consistent with privacy and civil liberties.

The TSC has also become a premier entity on the forefront of the global war on terrorism by establishing formal information sharing partnerships with our allies. The TSC has thus far signed agreements with six nations. These agreements provide our allies with access to the world's most comprehensive tool to identify terrorists, and we

are the beneficiaries of their terrorist identity information. We continue to work with our allies to share information more efficiently, and those information gaps are shrinking rapidly. As a result, it is becoming much more difficult for terrorists and their supporters to hide. By teaming up with our foreign counterparts, we have effectively broadened the net with which known and suspected terrorists are identified and caught.

GAO Report

The recent GAO review of Terrorist Watchlist Screening provided some critical feedback to all agencies involved in the watchlisting process. The TSC is working with our partners in DHS and the FBI to:

- Identify a systemic approach to capitalize on all watchlisting opportunities, including in the private sector and with current and potential international partners;
- Continually review and update terrorist screening strategies; and
- Identify clear lines of responsibility and authority for terrorist screening.

GAO Report - Private Sector Screening

Terrorist screening is currently conducted by an array of agencies protecting our nation's borders and our people from another terrorist attack. HSPD-6, HSPD-11 (Comprehensive Terror Related Screening Procedures) and their resulting initiatives, including the creation of the TSC, have greatly enhanced security at our borders. But simply enhancing border screening is not enough to identify those who may have already successfully assimilated into our culture, become established within our society and placed themselves in positions of trust in the private sector. Such persons would have the ability to carry out attacks on our critical infrastructure that could harm large numbers of persons or cause immense economic damage. Private sector screening is therefore critical to ensuring we identify watchlisted persons working as, or who have access to, critical infrastructure facilities that could be used to harm the American public. HSPD-6 mandates that the terrorist watchlist be made available to support private sector screening

processes that have a substantial bearing on homeland security. The TSC is working closely with DHS to finalize guidelines to support private sector screening and to fulfill the mandate of HSPD-6.

GAO Report - Use of the Watchlist

As the GAO report states, TSC customers receive TSDB data that suits their individual agency needs. Which TSDB records are exported to a particular customer depends on that customer's mission, legal authority, resources, and other considerations. For example, U.S. Customs and Border Protection (CBP) receives over 98% of the records in the TSDB to screen against threats at our borders. CBP has by far the broadest criteria concerning TSDB data, and therefore receives the greatest number of TSDB records. Other TSC customers, such as the Department of State (which screens applicants for visas and passports), have different criteria tailored to their mission and screening needs and therefore receive slightly less data. The State Department's visa screening process, for example, does not check against TSDB records on American citizens or Legal Permanent Residents, because they are not required to have a visa to enter the U.S. The TSC also exports nearly two-thirds of the TSDB to the National Crime Information Center (NCIC), where it is made available to federal, state, county, tribal, and municipal law enforcement officers. The TSC also sends a portion of the TSDB to the Transportation Security Administration as the "selectee" and "no fly" lists for use in air passenger screening.

In FY 2006, as indicated in the GAO Report, 269 foreign persons were denied entry to our nation because they were determined to present an unacceptable risk of committing a terrorist act. Thousands of other individuals listed in the TSDB were encountered at our borders, or within the United States, and their whereabouts were made known to the FBI and other law enforcement agencies. These encounters often yield valuable information not only about the subject's whereabouts, but also his or her associates, interests, and intentions.

These, and all matches to the watchlist, significantly enhance the FBI's ability to accurately assess current threats, to identify intelligence gaps and opportunities, and to further existing investigations. In sum, they help to "connect the dots" and make safer those whom we are sworn to protect. Through data quality assurance methods, an extensive nominations process and the redress process, the TSC continues to work to ensure that its data remains accurate, current and comprehensive, thus efficiently meeting our customers' screening needs.

Conclusion

In the four short years since its inception, the TSC has significantly enhanced the safety of the nation and has become a critical player in the war on terrorism. We are committed to achieving new heights, and continuing to make America a safer place through balancing terrorist screening and the rights of our fellow citizens. This can only be accomplished through a continuous process of internal and external review, and eternal vigilance. Chairman Lieberman, Ranking Member Collins, and members of the Committee, thank you again for the opportunity to address this esteemed body, and I look forward to answering your questions.

UNITED STATES DEPARTMENT OF HOMELAND SECURITY

STATEMENT OF PAUL ROSENZWEIG
DEPUTY ASSISTANT SECRETARY FOR POLICY

BEFORE THE SENATE COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

OCTOBER 24, 2007

INTRODUCTION

Thank you, Chairman Lieberman, Ranking Member Collins, and Members of the Committee for the invitation to appear today. I appreciate this Committee's steadfast support of the Department and your many actions to improve our effectiveness.

At the outset, I would like to acknowledge the strong working relationships we share with the Director of National Intelligence (DNI), the Federal Bureau of Investigation (FBI), the Terrorist Screening Center (TSC), and the National Counterterrorism Center (NCTC), as well as many other federal, state, and local partners working around the clock to protect our country and the American people from terrorist attacks.

None of us alone can keep our nation safe from the threat of terrorism. Protecting the United States is a mission we all share and one that requires joint planning and execution of our counterterrorism responsibilities; effective information collection, analysis, and exchange; and the development of integrated national capabilities.

One of the most important tools in the fight against terrorism is the U.S. Government's consolidated Terrorist Watchlist. The implementation and use of the Terrorist Watchlist 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. DHS works closely with the FBI and the Office of the DNI to review screening opportunities, implement watchlist enhancements and address potential vulnerabilities. As the largest screening agency, DHS has a significant interest in ensuring the effective and appropriate application of the watchlist in screening programs. This is an iterative process of continual review and improvement. As one example, the Screening Community is focused today on aligning biometric watchlist information in a more automated fashion with biographic records to provide even more efficient screening capabilities.

DHS as a Screening Agency

As you know, U.S. screening efforts start well before individuals arrive in the U.S. Most important, we have a number of information sharing activities with our international allies in the War on Terror. The international community has put significant resources into detecting and tracking terrorist travel across the globe.

Our overseas layers of security related to screening of individuals prior to arrival in the United States include: Department of State (DOS) visa application processing, the Immigration and Customs Enforcement (ICE) Visa Security Units that support DOS screening, and the new Immigration Advisory Program that involves screening of travelers by U.S. Customs and Border Protection (CBP) at airports of departure. Watchlist information supports all of these front line officers in their mission to keep dangerous people out of the U.S.

Information-based screening represents the next and most intensive opportunity for screening to prevent terrorists and terrorist weapons from entering the U.S. Leveraging passenger information from both Advance Passenger Information and Passenger Name Record (PNR) data in advance of arrival allows us to check the terrorist watchlist, criminal wants and warrants, and travel history as well as search for connections between known and unknown terrorists. This year we reached an important agreement with the European Union that will allow us to continue accessing PNR data while protecting passenger privacy. We will also continue to collect PNR data from flights originating in other regions around the world that are destined for the United States.

While we are conducting these checks prior to arrival, DHS is moving toward its Advance Passenger Information System (APIS) pre-departure requirement to perform watchlist checks in advance of boarding. In August 2007, DHS issued the final rule requiring commercial air and vessel carriers to provide manifest information for flights to and from the U.S. prior to boarding and for vessels departing from the U.S. prior to departure.

APIS pre-departure is a first step to taking over the No Fly and Selectee list matching responsibility from air carriers. As you know, since 9/11, the U.S. Government has been making the No Fly and Selectee lists available to commercial air carriers flying into, out of, or within the U.S. for passenger prescreening. Any nominating agency can recommend that a known or suspected terrorist (KST) be placed on the No Fly or Selectee list if the individual meets specific criteria for inclusion on either list. TSC has released the No Fly and Selectee Lists Implementation Guidance which was revised in July 2006 to provide the Screening Community with direction on appropriate nominations. According to the Implementation Guidance, TSC is ultimately responsible for placing individuals nominated to the No Fly or Selectee Lists, which are subsets of Terrorist Screening Data Base.

Today, commercial air carriers are responsible for conducting checks in advance of boarding pass issuance, and they must notify the Transportation Security Administration (TSA) where there is a match to the No Fly list. TSA then notifies the TSC and the FBI, which coordinate the operational response with law enforcement and other agencies and foreign partners as appropriate. The air carriers must also ensure that a match to the Selectee list is subject to secondary screening prior to boarding an aircraft. As outlined in the passenger screening sections below, the government is preparing to assume the responsibility for No Fly and Selectee screening in both the international and domestic air passenger processing venues.

In August 2007, DHS published the Secure Flight Notice of Proposed Rulemaking, which outlined DHS plans to assume watchlist matching responsibilities from air carriers for domestic flights and align domestic and international passenger pre-screening. Secure Flight, as

envisioned in the proposed rule, will make watchlist matching more effective, efficient, and consistent, offering improvements in both security and customer service for the traveling public. DHS expects Secure Flight to add a vital layer of security to our nation's commercial air transportation system while maintaining the privacy of passenger information.

The most significant benefit to initiating the Secure Flight program is the government's ability to take over watchlist-matching responsibility from the air carriers. DHS will be able to more effectively and consistently perform the watchlist-matching function than air carriers for several reasons to include the following:

- DHS will utilize real-time watchlist information;
- Matching will be uniformly conducted by one process with consistent results applied across airlines;
- The system can be effectively and swiftly calibrated to meet the current threat – for example by increasing the number of potential matches that are generated for an intelligence analyst's review, based on an elevated threat level;
- Distribution of the watchlists themselves will be more limited – protecting that sensitive information; and
- DHS will have identifying passenger information sooner and will be able to adjudicate potential matches prior to the individual's arrival at the airport, thereby reducing the impact of false matches on the traveling public, or providing more time to coordinate an appropriate law enforcement response to potential threats, if necessary.

Secure Flight will establish a more consistent and uniform prescreening process, enhancing the ability of DHS to stop KSTs before they get to the passenger screening checkpoints while simultaneously reducing potential misidentification issues.

Once inside the U.S., terrorist-related screening opportunities increase exponentially, requiring the greatest application of discipline for risk-based screening measures to ensure that resources are focused accordingly, meeting the threats while simultaneously ensuring our civil liberties and privacy. DHS screens immigration benefits applicants and critical infrastructure sector workers, consistent with its legal authority through programs such as the Transportation Workers Identification Credential program.

With our current security layers, we have prevented thousands of dangerous people from entering the United States, including individuals suspected of terrorism, murderers, rapists, drug smugglers, and human traffickers. In Fiscal Year 2007, CBP alone encountered 5,953 positive watchlist matches.

I should also dispel some myths about DHS's screening programs. A person's union membership, sexual orientation, eating habits and reading choices are irrelevant to DHS's screening programs. All of DHS's screening systems are designed to match travelers against intelligence and/or enforcement information only. Accordingly, DHS only actively seeks data pertinent to screening. However, we may, at times, receive ancillary information from an air carrier or from the individual concerned that could be considered "sensitive." For example, a carrier may note in reservation data that a traveler is blind and will need help finding his seat or

that the travel agency that booked the ticket was UnionPlus. From this ancillary information a person could deduce facts about the traveler. However, very pertinent information may also be stored in the same record – including names and passport data. When DHS does receive sensitive data it is because of the need to collect this other information. In these instances, special, stringent protections are put in place to prevent DHS users from viewing any sensitive information unless there is a specific case-related necessity that has been verified by a senior official. DHS is transparent about the rules it has put in place to prevent sensitive information from being used for screening. We have published them in our System of Records Notice for the Automated Targeting System and have made similar public representations to the European Union.

Factors Relevant to Watchlist Matching Effectiveness

Not only is it important to ensure that the watchlist itself is accurate and appropriate to the screening opportunity, but the robustness of the information that is matched against the watchlist is a key factor in effective screening. What level of assurance do we have in the individual's presented identity? What information is provided? As Director Boyle notes in his testimony, different screening opportunities present different challenges. At the border, CBP has many tools at its disposal to identify and screen individuals entering the U.S. – whereas in the domestic aviation context, we are currently reliant upon the name matching capabilities of the air carriers.

The use of biographic information in screening including reliance on names to identify KSTs, has its limitations. For that reason, DHS is pursuing efforts to enhance the effectiveness of the screening conducted at all opportunities by promoting secure identification and the use of biometrics, where appropriate and feasible. US-VISIT biometrics collection that starts overseas during the visa application process provides a significant layer of security. As we move to 10-print collection, our ability to match that information against latent prints from the battlefield to identify unknown terrorists increases substantially.

Secure identification also enhances our ability to screen effectively. Identification documents often provide the baseline information for conducting screening. For that reason, DHS is pursuing implementation of the Western Hemisphere Travel Initiative (WHTI) and REAL ID. Both programs are recommendations of the 9/11 Commission, who so aptly noted that "[f]or terrorists, travel documents are as important as weapons." By requiring secure documents to enter the United States, or board commercial aircraft, we will make it harder for people to use fraudulent credentials to travel or cross our borders, and we will make it easier for our inspectors to separate real documents from fake, enhancing our security and ultimately speeding up processing.

Misidentification and Redress

Recognizing the impact of screening on the public, particularly where only name-based checks are conducted, agencies have incorporated redress into their screening programs. DHS has implemented the DHS Traveler Redress Inquiry Program (DHS TRIP), which provides a central gateway for travelers to obtain information about screening and redress as well as a central contact to DHS regarding their adverse screening experiences. Travelers, regardless of their

nationality, citizenship or residency, can submit inquiries via website, email, or postal mail. The DHS TRIP Program Office then ensures that the cases are resolved, to the extent possible, and that travelers receive an official response from the screening agency. The DHS TRIP Program Office, using the DHS TRIP system, assigns redress requests to the appropriate DHS agencies, ensures coordination of responses, and institutes performance metrics to track progress, giving leadership visibility into the types of complaints DHS receives and the status of response.

Once a redress request associated with No Fly and Selectee matching is processed, the cleared individual is added to the TSA Cleared List and is provided to air carriers. The Cleared List is currently used by the airlines to distinguish false matches from actual matches as they perform No Fly and Selectee list matching.

For international travel, CBP has implemented a process that automatically suppresses specific lookout matches, including terrorist watchlist matches, in its screening systems when a CBP Officer at a port of entry encounters an individual that CBP has previously determined to be a false positive match. Primary Lookout Override (PLOR) is an automated function for situations where a traveler is repeatedly stopped because his or her biographical information is the same or similar to a lookout or watchlist record, but when the traveler is not the actual subject of the record. When the passenger is positively identified and determined not to be a match to a lookout or watchlist record, CBP can create a PLOR record that automatically suppresses that specific hit the next time that person is encountered, unless new derogatory information has become available. As a result, CBP does not have to resolve the false match each time the person travels.

When DHS TRIP is unable to determine whether an individual is a positive or false match, the redress request is referred to the TSC pursuant to the formal watchlist redress process established in January 2005. Director Boyle describes this process in his testimony.

Between February 20, 2007, and October 17, 2007, DHS TRIP received approximately 21,942 requests for redress and 11,870 cases have been resolved. The majority of TRIP requests that remain in process are awaiting submission of supporting documentation by the traveler. From program inception through September 2007, CBP has approved 71,487 PLOR requests at the border.

Quality Assurance of the Watchlist

In addition to the efforts described above, TSC analysts also conduct various proactive quality assurance projects with support from DHS. We recently completed a review of all records on the No Fly List and are near completion of a record-by-record review of the Selectee List. Quality assurance projects like the No Fly and Selectee list reviews ensure that the most current, accurate, and thorough watchlist information is made available to DHS and other screening agencies, and that records are updated in a timely fashion. Such regular updates both improve the quality of the screening being conducted and decrease the instances of screening misidentifications.

The U.S. Government is doing much to ensure travelers have the opportunity to seek redress and to enhance the effectiveness of the watchlisting process itself. At the same time, it is worth noting what GAO described in its September 2006 report (GAO-06-1031) – that although the total number of misidentifications is significant, they represent a tiny fraction of the total screening transactions that are conducted on the hundreds of millions of travelers DHS encounters each year.

The DHS Screening Coordination Office (SCO), the DHS TRIP Office, and the screening agencies responsible for addressing redress requests continue to refine the concept of operations for DHS TRIP as well as to consider next phases for enhancing the Department's redress capabilities.

Response to GAO Audit

DHS agrees with many of the findings in the GAO Terrorist Watch List Screening report. DHS takes GAO's recommendations seriously and, in fact, has had ongoing efforts to address them.

GAO recommended that the Secretary of Homeland Security "...develop guidelines to govern the use of watchlist records to support private-sector screening processes that have a substantial bearing on homeland security."

In response to this recommendation, DHS is drafting guidelines to establish and support private sector screening for those respective private sector entities that have a substantial bearing on homeland security. These guidelines will prioritize private sector entities by critical infrastructure sector that are necessary for the functioning of our society. For these purposes, critical infrastructure may include, but is not limited to, agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry and hazardous materials, postal and shipping, and national monuments and icons. In addition to the draft guidelines, DHS anticipates preparing an information collection request under the Paperwork Reduction Act, Privacy Impact Assessment, and System of Records Notice, which would address any DHS private sector screening program.

GAO also recommends that the Secretary of Homeland Security "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" as well as "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." The updated HSPD-11 report is under development and is forthcoming.

The Screening Community has taken extensive steps since 2004 to enhance terrorist screening and many of those efforts that are specific to the watchlist have been outlined in this testimony. Additionally, at the request of the Assistant to the President for Homeland Security and Counterterrorism, DHS is providing such an update to the Homeland Security Council.

CONCLUSION

On September 11, 2001, no one would have predicted the passage of six years without another terrorist attack on U.S. soil. Some believe our country hasn't suffered another attack because we've been lucky. Others contend the terrorist threat has diminished and we are no longer in danger.

I disagree. Over the past six years, we have disrupted terrorist plots within our own country and we've turned away thousands of dangerous people at our borders. We've also witnessed damaging terrorist attacks against some of our staunchest allies in the war on terror.

I believe the reason there have been no additional attacks against our homeland is because we've successfully raised our level of protection and we've succeeded in frustrating the aims of our enemies. That's not to say our efforts have been flawless or that our work is done. On the contrary, we must move forward aggressively to build on our success to keep pace with our enemies.

Our improvements to passenger and cargo screening, critical infrastructure protection, and intelligence fusion and sharing must continue. While no one can guarantee we will not face another terrorist attack in the next six years, if we allow ourselves to step back from this fight, if we allow our progress to halt, if we don't continue to build the necessary tools to stay ahead of terrorist threats, then we will most certainly suffer the consequences.

I'd like to thank this Committee for your ongoing support for our Department. We look forward to working with you and with our federal, state, local, and private sector partners as we continue to keep our nation safe and meet our responsibility to the American people.

Promoting Accuracy and Fairness in the Use of Government Watch Lists

Statement of the Constitution Project's Liberty and Security Initiative

December 5, 2006

The Constitution Project
1025 Vermont Avenue, NW
Washington, DC 20005

202-580-6920 (phone)
202-580-6929 (fax)

info@constitutionproject.org
www.constitutionproject.org

Promoting Accuracy and Fairness in the Use of Government Watch Lists

Statement of the Constitution Project's Liberty and Security Initiative*

Introduction

United States intelligence and law enforcement agencies have long relied upon "watch lists" to help identify individuals who pose potential threats to national security. In light of widespread press coverage and personal experience, most Americans are now familiar with the watch lists used to screen airline passengers. As we have come to understand, these lists contain names of people who may be subjected to additional screening and review or even prohibited from boarding an airplane. Press reports have also made clear that the use of such lists extends well beyond airport security, and we have recently learned of the existence of an "Automated Targeting System (ATS)" that gathers data on travelers and assigns computer-generated risk scores. Therefore, we, the undersigned members of the Constitution Project's Liberty and Security Initiative, are issuing this statement to urge policymakers to promptly restrict the use of such watch lists, and adopt important reforms to govern the situations in which they are used.

The Constitution Project is an independent think tank that promotes and defends constitutional safeguards by bringing together liberals and conservatives who share a common concern about preserving civil liberties. By forging consensus positions that bring together "unlikely allies" from both sides of the aisle, the Project broadens support for constitutional protections both within government and in the public at large. The Project launched its Liberty and Security Initiative in the aftermath of September 11th. Guided by an ideologically diverse committee of prominent Americans, the Initiative is committed to developing and advancing proposals to protect civil liberties even as our country works to make Americans safe. We, the committee's members, are Democrats, Republicans, and independents, conservatives and liberals. We are united in our belief that the use of watch lists must be strictly limited, and in our concern that procedural safeguards and other measures to promote fairness are needed to protect us from the dangers posed by the use of watch lists. Even in situations where watch lists may be appropriate, the use of such lists may harm innocent persons either because they share a name with another individual who is appropriately included, or because such people are placed on lists despite a lack of evidence to warrant such treatment.

Although watch lists may serve as a valuable tool in our government's efforts to combat terrorism, they also pose serious threats to Americans' civil liberties. First and foremost, watch lists must not be used as "blacklists," to prevent certain people even from being considered for various jobs or government benefits. Moreover, watch lists continue to be plagued with errors, and the press has reported numerous accounts of individuals – even children – being mistakenly

* The Constitution Project sincerely thanks Peter M. Shane, Joseph S. Platt - Porter, Wright, Morris & Arthur Professor of Law and Director, Center for Interdisciplinary Law and Policy Studies, Ohio State University Moritz College of Law, for his extensive researching and drafting work on this statement and a background report for the Liberty and Security Initiative. In addition, we are grateful to the Public Welfare Foundation and the Community Foundation for their support of the Liberty and Security Initiative's work on the issue of watch lists. We also thank the Open Society Institute, the Wallace Global Fund, and an anonymous donor for their support of the Constitution Project in all its work.

stopped at airports. In order for watch lists to be both effective and fair, it is critically important that they be accurate. Mistaken targeting wastes government resources and harms innocent individuals who are included on lists without justification or who simply share a name with an appropriately listed person. To the extent watch lists impede travel or immigration by non-citizens who present no actual threat to the United States, they can exact substantial cultural, political, and economic costs, in both the short and long term. For individuals wrongly included, costs may range from surveillance or minor inconvenience to serious reputational damage or substantial limitations on privacy and freedom of action.

I. When Watch Lists Are Appropriate

Since September 11, 2001, federal law enforcement and intelligence agencies have vastly expanded the scope of, and their reliance upon, watch lists. In late 2003, the government began consolidating these various lists under the aegis of the Terrorist Screening Center (TSC). The Terrorist Screening Data Base (TSDB), subsequently established by the TSC, now serves as a central repository for records and as a coordinating hub for information that moves between government watch lists.

The history of governmental use of watch lists is a checkered one. In some contexts, watch lists have been used inappropriately to deny people jobs and government contracts on unjustified and discriminatory bases. On the other hand, we recognize that in certain circumstances watch lists may be a useful tool because the opportunity does not exist for more careful real-time investigation.

We recommend that watch lists be used only in situations in which decisions must be made quickly and grave consequences would follow from failure to screen out a listed person. The obvious case occurs when individuals present themselves for immediate access to sensitive sites or facilities, such as airplanes. Thus, it is appropriate to use a watch list to determine who may merit additional screening before boarding an airplane, and for the "no fly" list, subject to the recommendations we make in Section II below. Similarly, under the same conditions, we approve of the use of a watch list to determine which foreigners residing overseas should be denied visas to come to the United States. Such watch lists must only be used, however, for the specific and limited purpose for which the list is authorized.

By contrast, watch lists should not be used in such contexts as employment, where the burdens on individuals are substantial and the government can protect national security effectively through careful contemporaneous investigation. The Constitution Project's Liberty and Security Initiative disapproves of the practice of compiling watch lists of suspected persons to be used for screening for employment purposes or in connection with applications for contracts or licenses related to employment. We are concerned by current discussions of whether to use the Terrorist Screening Database watch list in such contexts. We note that many members of the Initiative have long fought against the use of criminal history records, particularly arrest records, to deny persons employment, as leading to discrimination and other unlawful practices.

At the same time, we recognize that there are positions that require security clearances or other types of background checks for national security or other legitimate reasons. The security clearance system, for example, has evolved over time to address both the criteria for denying persons clearances and the due process rights of those denied clearances, including how to deal with the classified information in making such determinations. Given the systems in place to assure appropriately qualified applicants obtain clearances for employment and contracts, a watch list of suspected persons is unnecessary and inconsistent with constitutional protections against discrimination and for due process.

Finally, we disapprove of the use of watch lists to determine which non-citizens living in the United States should be subjected to arrest or detention, with the exception of a watch list for individuals for whom outstanding arrest warrants have been issued.

II. Recommended Reforms to Watch Lists to Promote Fairness and Accuracy

For situations in which watch lists are appropriate, the Constitution Project's Liberty and Security Initiative has formulated a set of recommended procedures to promote accuracy as well as fairness in their maintenance and use. Specifically, we propose implementation of "front-end" procedures to enhance the accuracy and uniformity of watch lists, as well as a "back-end" redress system for individuals seeking to clear their names. This combination of measures should not only vastly improve the quality and fairness of watch lists, but also provide clear channels for individuals seeking to remove their names from watch lists. We recommend that Congress enact legislation to implement these procedures.

A. A Front-End Fairness System for Government Watch Lists

Promoting accuracy at the "front-end" will improve the efficiency and effectiveness of watch lists, and provide greater fairness to individuals. This approach will enable the TSC to avoid – and remedy – significantly more cases of potential error than would a system that relied only on a "back-end" redress system.

To achieve these goals, we recommend four kinds of protection in the front-end maintenance of watch lists:

1. *Clear Written Standards:* Agencies maintaining watch lists need clear written standards that specify the general criteria for inclusion, the kinds of information regarded as relevant evidence that the criteria have been met, and the standards of proof appropriate for including individuals when information is received.

2. *Rigorous Nominating Process:* Agencies maintaining watch lists should follow a rigorous nominating process, structured to promote reliability across agents and across agencies in order to make certain that decisions are being made as objectively as possible. The process should be designed so that the decision to include or exclude names is relatively uniform no matter who makes the nomination. Reliability is critical not only to the accuracy of the system, but also as a guarantee of equality in

the treatment of all people.

3. *Internal Monitoring for Accuracy:* Agencies maintaining watch lists should pursue rigorous programs of internal monitoring to insure the completeness, timeliness, and accuracy of all records, including the completeness, timeliness, and accuracy of error correction. This should include regular sampling of records on a random basis. Each agency should appoint a Records Integrity Officer to oversee the implementation of these processes.

4. *Maintaining Accuracy in Interagency Sharing of Records:* Agencies maintaining watch lists should employ a system architecture to protect the accuracy and completeness of records that are shared, with the particular goal of insuring that error correction in any database results in error correction in every other database containing the same foundational record. In addition, watch lists must be maintained under fully secure conditions, to protect against the risks of both inadvertent tampering and computer hacking.

B. A Back-End Redress System for Listed Individuals

To be complete, a fairness system must also include some mechanism for redressing errors in individual cases. At bottom, individuals must be afforded a fundamentally fair opportunity to challenge their inclusion on a watch list, on grounds of either mistaken identity or inadequate justification for inclusion. The specific procedural details that constitute a "fundamentally fair opportunity" will vary with the circumstances, including the nature of the challenge and the degree to which agencies implement protective "front-end" procedures.

In mistaken identity cases, a well-managed front-end process should greatly reduce the number of cases requiring redress, and entitle the government to establish a less exacting "back-end" system at the administrative level. The level of procedural formality might also be expected to vary with the nature of the burden that an individual faces because of challenged watch list inclusion. If, however, the government assembles all or a group of watch lists from a single database serving many functions, it may make sense to have a process tailored to the most burdensome consequence that inclusion in the central database might portend. Acknowledging that variations are inevitable, we offer the following as an example of an appropriate approach.

1. *A Different Approach to Notice*

Most redress systems begin when the government provides an individual with notice of an official action, which the individual may then challenge. In the watch list context, however, providing notice that a person has been added to a list would likely undermine the purposes of the program, and could entail substantial risks to ongoing investigations. Thus, provided that the front-end protections outlined above are implemented, we recommend that the government should be compelled to offer redress only in those cases when an individual suffers a real burden by his or her inclusion on a watch list.

There remain two special types of cases where elimination of the notice requirement becomes more troubling: (1) when individuals are proposed for inclusion on watch lists based solely upon anonymous or uncorroborated tips, and (2) when individuals have been proposed for inclusion on watch lists solely through the operation of pattern recognition techniques. Even with a front-end fairness system in place, the risks of error under either of these scenarios would be substantial.

We therefore recommend that because uncorroborated or anonymous tips are especially unreliable, but giving notice is likely an impracticable solution, government agencies should simply be prohibited from using tip information, without corroboration, as a basis for including any individual on an "operational" watch list that may result in the denial of any right, privilege, or benefit. Thus, such information should not be used as a basis for including a person on the "no fly" list. Uncorroborated tip information might be kept in a separate "pre-operational" list, as individuals potentially subject to watch list inclusion remain subject to investigation. Further, on a time-limited basis, it might be appropriate to rely upon such tips as the basis for further investigation, such as by placing the person on a list requiring additional screening at airports. However, any such use to target individuals for more thorough screening should be strictly limited to a follow-up period of no more than 120 days. After that time, absent corroboration or authentication of the original tip, the individual should be removed from any list of persons to be targeted for more rigorous screening.

We similarly recommend that agencies be precluded from relying solely upon pattern recognition techniques to include persons on operational watch lists. Such techniques involve the compilation of several characteristics or behaviors, each of which may itself be innocuous, but the combination of which is considered suspicious. Although pattern recognition may be a valuable tool, this kind of statistical profiling is subject to high rates of error, and could lead to inclusion of individuals on watch lists despite the lack of any direct evidence of a suspicious act or behavior. Therefore, individuals identified solely through pattern recognition techniques should not be included on any *operational* watch lists, but only on *pre-operational* lists or time-limited lists for additional screening, as described above for uncorroborated or anonymous tips. To the extent that the recently disclosed "Automated Targeting System (ATS)" is such a pattern recognition system, that system should only be operated in compliance with these recommendations.

As an alternative for pattern recognition cases, the government could create a process that would provide independent review of proposed pattern recognition algorithms. Specifically, the government might provide for an independent arbiter to determine whether a particular statistical profile creates a justifiable belief that persons identified are reasonably suspected of involvement in terrorism. The agency proposing use of the particular algorithm would make a confidential *ex parte* showing to the independent arbiter that (a) the government was justified in associating the behavioral pattern with suspected terrorism and (b) the algorithm was accurately deployed in identifying the subjects involved. The required showing should include a demonstration that the targeted behavioral pattern characterizes a substantial number of terrorist suspects

identified through other means. Only after such an independent arbiter approves the profile analysis could the government rely upon it to nominate individuals for inclusion on an operational watch list.

2. *A Proposed System of Redress*

For situations in which watch lists are appropriate, as outlined in Section I above, the government must also design improved "back-end" redress procedures. Although adoption of the recommended "front-end" procedures outlined in Section II.A. above will reduce the number of cases in which redress may be needed, there will still be situations in which individuals seek to clear their names from watch lists.

We recommend that the government develop two different back-end procedures, one informal and one formal. The choice of which procedure to apply in any specific case should depend on whether the government actually implements the recommended front-end protections, and on whether the individual is alleging mistaken identity – that he or she simply shares a name with someone on the list but is not that person – or is alleging that there is not sufficient evidence to warrant his or her inclusion on the list.

a. Informal: The informal process should consist solely of written procedures without an oral hearing. Individuals would have a right to appeal in court, but the decision would be reviewed only for arbitrariness. If the government implements the recommended front-end fairness protections, the informal process should be applicable for all mistaken identity cases in which the decision maker determines that the front-end standards and processes were followed.

b. Formal: The formal system would involve an oral administrative hearing and judicial review under a *de novo* evidentiary standard with the government bearing the burden of proof. If the government declines to adopt the recommended front-end fairness protections, then the formal procedure should be available whenever an individual challenges his or her inclusion on a watch list. Otherwise, the formal process would be available only for cases alleging insufficient evidence to warrant inclusion on a watch list and for those mistaken identity cases in which the agency failed to follow the required front-end safeguards.

In addition to these two tracks, another category is needed for individuals who are non-United States persons* outside the borders of America. These individuals should be entitled to submit a written complaint for review by the agency maintaining the watch list, but the government should not be compelled to grant hearings outside of the United States for those dissatisfied with the results of the written review process.

* The term "United States person" refers to both United States citizens and legal residents of the United States. A "non-United States person" would not be entitled to the same protections under the United States' constitution and laws.

For purposes of hearings under the formal system and appeals under the informal system, the government should employ government attorneys to serve as public advocates, who will have security clearances at a level adequate to insure that they can review classified material.

3. *Audits and Recordkeeping*

Whatever redress procedures the government follows, it should preserve the records from any complaints. Information regarding the nature of the complaint and its resolution should be promptly recorded in the Terrorist Screening Data Base (TSDB) and circulated to all agencies using watch lists.

In addition, the TSC should conduct regular routine audits of how the TSDB has been used. The TSDB purports to contain names of people with known or suspected links to terrorism. Those with "suspected links" are included in this database because government officials want to watch them further, to assess whether they are in fact participating in any terrorist plot. The audit process should document each occasion on which use of a watch list has resulted in a match, and describe what occurred during the encounter with the listed individual. This should include whether or not the individual was arrested, and the nature and extent of any follow-up investigation that was conducted to assess whether the watch-listed individual is in fact participating in any terrorist plot. Audit reports should then be reviewed to assess the efficacy of the watch list, and to determine whether any particular individuals should be purged from the list.

C. Reports to Congress

Despite procedures to ensure fairness and proper redress, the lack of transparency built into the watch list program may undermine the public's support. In order to improve accountability and monitoring of watch lists, Congress should further require regular reporting by the agencies employing watch lists, including submission of the audit reports recommended above.

Members of the Liberty and Security Initiative Endorsing the Constitution Project's *Promoting Accuracy and Fairness in the Use of Government Watch Lists*[*]

Co-Chairs

David Cole- Professor of Law, Georgetown University Law Center

David Keene- Chairman, American Conservative Union

Members

Dr. Azizah Y. al-Hibri- Professor, The T.C. Williams School of Law, University of Richmond; President, Karamah: Muslim Women Lawyers for Human Rights

Hon. Bob Barr- former Member of Congress (R-GA); CEO, Liberty Strategies, LLC; the 21st Century Liberties Chair for Freedom and Privacy at the American Conservative Union; Chairman of Patriots to Restore Checks and Balances; practicing attorney; Consultant on Privacy Matters for the ACLU

John Curtin- Bingham McCutchen LLP; former President, American Bar Association

Hon. Mickey Edwards- Director, Aspen Institute-Rodel Fellowships in Public Leadership; Lecturer, Woodrow Wilson School of Public and International Affairs, Princeton; former Member of Congress (R-OK): former Chairman, House of Representatives Republican Policy Committee

Dr. Morton H. Halperin- Director of U.S. Advocacy, Open Society Institute; Senior Vice President, Center for American Progress

David Lawrence, Jr.- President, Early Childhood Initiative Foundation; former Publisher, *Miami Herald* and *Detroit Free Press*

Thomas R. Pickering- former Undersecretary of State for Political Affairs; former United States Ambassador and Representative to the United Nations

John Podesta- President and CEO, Center for American Progress; White House Chief of Staff, Clinton Administration

Hon. William S. Sessions- Partner, Holland + Knight, former Director, Federal Bureau of Investigation; former Chief Judge, United States District Court for the Western District of Texas

John Shore- Founder and President, noborg LLC; former Senior Advisor for Science and Technology to Senator Patrick Leahy

John F. Terzano- President, The Justice Project

Hon. Patricia Wald- former Chief Judge of the U.S. Court of Appeals for the D.C. Circuit

John W. Whitehead- President, The Rutherford Institute

Lawrence B. Wilkerson, Col, USA (Ret)- Visiting Pamela C. Harriman Professor of Government at the College of William and Mary; Professorial Lecturer in the University Honors Program at the George Washington University; former Chief of Staff to Secretary of State Colin Powell

Roger Wilkins- Clarence J. Robinson Professor of History and American Culture, George Mason University

[*] *Affiliations listed for identification purposes only*

United States Government Accountability Office

GAO

Report to Congressional Requesters

October 2007

TERRORIST WATCH LIST SCREENING

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

GAO
Accountability * Integrity * Reliability

GAO-08-110

October 2007

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-08-110, a report to congressional requesters

TERRORIST WATCH LIST SCREENING

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

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.

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

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

[1]There 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.

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

[3]The 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

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

[5]As 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.

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

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

[7]See 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—

[8]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. 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

[9]The 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

[10]The 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.

[11]The 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

[12] Also, 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.

[13]In 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).

[14]See 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.

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

[16]The 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

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

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

[19]See 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

[20]TSA 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).

[21]CBP'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.

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

[23]Terrorist 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).

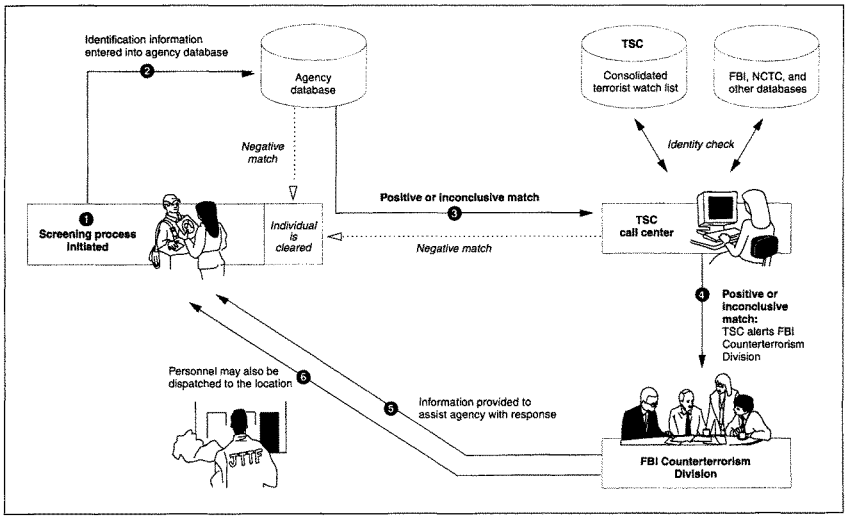
CBP's National Targeting Center; and Department of State consular officers who process visa applications are to submit a request for a security advisory opinion to Department of State headquarters.[24] The intelligence or operations center is to refer exact matches and inconclusive matches to TSC. State 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.

[24]Regarding 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.

[25]Joint 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

[26]The 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

[27]In 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.

[28]In 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

[29]The 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.

[30]According 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.

[31]See 8 U.S.C. § 1733.

[32]See 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-

[33]In 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.

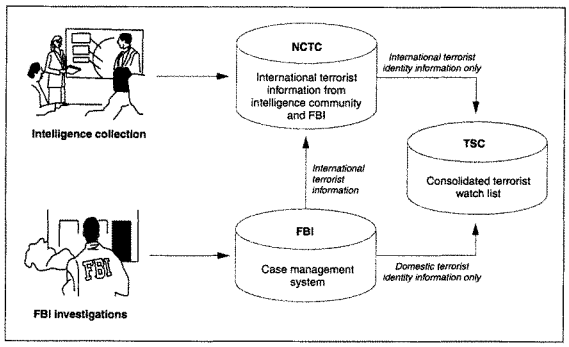
TSC's Watch List Is the Master Repository for Watch List Records

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.

[34]TSC 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.

[35]In 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

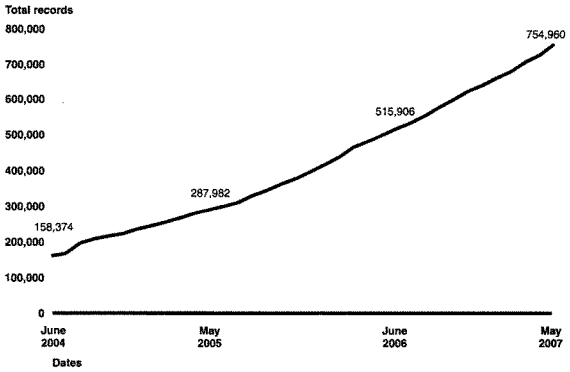


Source: GAO analysis of TSC information.

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.

[36]TSC 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

[37]Passengers 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

[38]In 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.

[a]According 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

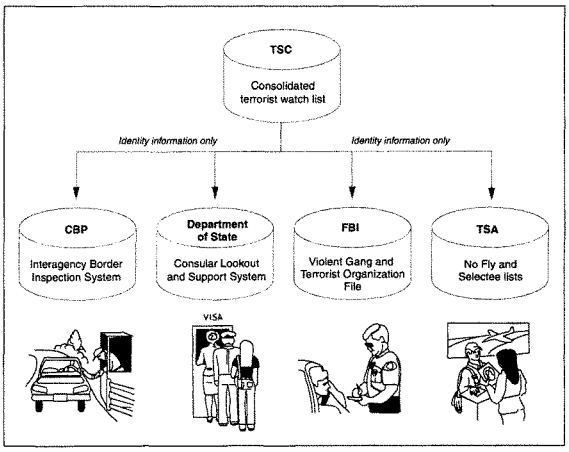
[39] As discussed previously in this report, sensitive but unclassified identifying information from NCTC's database is provided to TSC for inclusion on the consolidated terrorist watch list.

[40] The 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.

[41] In 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.

[42]The 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

[43]The 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.

[44]Also, 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

[45]The 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

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

[47]Pursuant 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).

[48]See 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

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

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.

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

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

[50]In 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

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

[52]CBP 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.

[53]For 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

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.

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

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

[54]See 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).

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

[56]An 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.

[57]The 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.

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

Improving Data Quality

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

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

[59]Department 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.

[60]Redress 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).

[61]In 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

[62]National 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

[63]Foreign 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).

[64]According 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.

[65]The 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.

[66]National 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.

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

[68]Additional 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

[70]DHS 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.

[71]The 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.

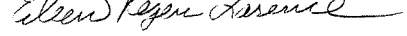
We recognize that TSC and its governance board have played and will continue to play a central role in coordinating watch list-related activities governmentwide. However, as discussed in this report, TSC's governance board is currently responsible for providing guidance concerning issues within TSC's 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

[1]Results 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.

[2]The 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.

[3]The 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.

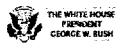
This directive does not alter existing authorities or responsibilities of department and agency heads to carry out operational activities or provide or receive information. This directive is intended only to improve the internal management of the executive branch and is not intended to, and does not, 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.

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 assess-ment 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;

(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 imple-menta-tion 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.

(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

[1]Department 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.

[2]In 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.

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

[4]See 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.

[5]See 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

[6]The 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.

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

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

2

REDACTED FOR PUBLIC RELEASE

FOLLOW-UP AUDIT OF THE TERRORIST SCREENING CENTER

U.S. Department of Justice
Office of the Inspector General
Audit Division

Audit Report 07-41
September 2007

REDACTED FOR PUBLIC RELEASE

FOLLOW-UP AUDIT OF THE TERRORIST SCREENING CENTER*

EXECUTIVE SUMMARY

The Terrorist Screening Center (TSC) is a multi-agency organization administered by the Federal Bureau of Investigation (FBI) that consolidates terrorist watchlist information and provides 24-hour, 7-day a week operational support for federal, state, local, and foreign governments.[1] The TSC was created by the September 16, 2003, Homeland Security Presidential Directive-6 (HSPD-6), which directed the TSC to integrate all existing U.S. government terrorist watchlists and assist in the screening of individuals who, for example, apply for a visa, attempt to enter the United States through a port-of-entry, attempt to travel internationally on a commercial airline, or are stopped by a local law enforcement officer for a traffic violation. Prior to the establishment of the TSC, the federal government relied on at least a dozen separate terrorist watchlists maintained by different federal agencies.

In June 2005, the Department of Justice Office of the Inspector General (OIG) issued an audit of the TSC's operations from the time of its inception in 2003.[2] The OIG reported that although the TSC had made significant strides in becoming the government's single point-of-contact for law enforcement authorities requesting assistance in identifying individuals with possible ties to terrorism and had developed a consolidated terrorist watchlist database, the TSC had not done enough to ensure that the information in that database was complete and accurate. For example, we reported instances where the consolidated database did not contain names that should have been included on the watchlist. Additionally, we found inaccurate or inconsistent information related to persons included in the database. In this prior review, we also found problems with the TSC's management of its information technology, a crucial facet of the terrorist screening process. Our June 2005 report included 40 recommendations to

---

* The full version of this report includes information that the FBI considered to be law enforcement sensitive and therefore could not be publicly released. To create this public version of the report, the OIG redacted (deleted) the portions of the full report that were considered sensitive by the FBI, and we indicated where those redactions were made.

[1] The participating agencies include the FBI, Central Intelligence Agency (CIA), and the Departments of Homeland Security (DHS) and State (State Department).

[2] Department of Justice, Office of the Inspector General, *Review of the Terrorist Screening Center*, Audit Report 05-27, June 2005.

the TSC addressing areas, such as database improvements, data accuracy and completeness, and staffing.

The objectives of this follow-up audit were to: (1) determine if accurate and complete records are disseminated to and from the watchlist database in a timely fashion; (2) review the TSC's efforts to ensure the quality of the information in the watchlist database; and (3) assess the TSC's efforts to address complaints raised by individuals who believe they have been incorrectly identified as watchlist subjects.

To accomplish these objectives, we interviewed more than 45 officials and reviewed TSC documents and databases. To evaluate the accuracy and completeness of the consolidated watchlist, we analyzed the consolidated database as a whole, including a review of the number of records in the database, any duplication that existed within those records, and the associated watchlist processes. We also tested individual records within the database for accuracy and completeness, as well as the timeliness of any related quality assurance activities. Finally, we assessed the TSC's activities related to individuals who raised complaints following their involvement in a screening encounter. This included examining the TSC's coordination with other participating agencies and reviewing a sample of such cases to determine if the actions taken were timely and conformed to TSC policy.[3]

Results in Brief

Overall, this follow-up audit found that the TSC has enhanced its efforts to ensure the quality of watchlist data, has increased staff assigned to data quality management, and has developed a process and a separate office to address complaints filed by persons seeking relief from adverse effects related to terrorist watchlist screening. However, we also determined that the TSC's management of the watchlist continues to have weaknesses. For example, the TSC is relying on two interconnected versions of the watchlist database. As a result of this and other conditions, we identified several known or suspected terrorists who were not watchlisted appropriately. Specifically, we identified 20 watchlist records on suspected or known terrorists that were not made available to the frontline screening agents (such as a border patrol officer, visa application reviewer, or local police officer) for use during watchlist screening encounters (such as at a border crossing, through the visa application process, or during a routine traffic stop). We also found that the number of duplicate records in the database has significantly increased since our last review.

---

[3] Detailed information regarding the audit objectives, scope, and methodology is contained in Appendix I.

In addition, because of internal FBI watchlisting processes, we found that the FBI bypasses the normal international terrorist watchlist nomination process and enters these nominations directly into a downstream screening system. This process is cumbersome for the TSC and, as a result, the TSC is unable to ensure that consistent, accurate, and complete terrorist information is disseminated to frontline screening agents in a timely manner.

We also concluded that the TSC needs to further improve its efforts for ensuring the accuracy of the watchlist records. We found that, in general, the TSC's actions to review records as part of a targeted special project successfully ensured the quality of the data. In contrast, our examination of the routine quality assurance reviews revealed continued problems. We examined 105 records subject to the routine quality assurance review and found that 38 percent of the records we tested continued to contain errors or inconsistencies that were not identified through the TSC's quality assurance efforts. Although the TSC had clearly increased its quality assurance efforts since our last review, it continues to lack important safeguards for ensuring data integrity, including a comprehensive protocol outlining the agency's quality assurance procedures and a method for regularly reviewing the work of its staff. Additionally, the TSC needs to work with partner agencies to develop clearly defined areas of responsibility and timeframes for quality assurance matters.

A single omission of a terrorist identity or an inaccuracy in the identifying information contained in a watchlist record can have enormous consequences. Deficiencies in the accuracy of watchlist data increase the possibility that reliable information will not be available to frontline screening agents, which could prevent them from successfully identifying a known or suspected terrorist during an encounter or place their safety at greater risk by providing inappropriate handling instructions for a suspected terrorist. Furthermore, inaccurate, incomplete, and obsolete watchlist information increases the chances of innocent persons being stopped or detained during an encounter because of being misidentified as a watchlist identity.

We are also concerned that the TSC's ongoing review of the watchlist will take longer than projected. At the time of our audit field work in April 2007, the TSC was continuing its efforts to conduct a record-by-record review of the consolidated watchlist and anticipated that all watchlist records would be reviewed by the end of 2007. However, the watchlist database continues to increase by an average of over 20,000 records per month and contained over 700,000 records as of April 2007. Given this growth and the TSC's weak quality assurance process, we believe the TSC is

underestimating the time required to sufficiently review all watchlist records for accuracy.

Our audit further determined that the TSC was following its procedures and reaching appropriate resolutions in its review of complaints filed by individuals seeking redress from further adverse experiences that they believed were the result of terrorist watchlist screening. However, we found that the redress reviews were not always completed in a timely manner, and we recommend that the TSC and partner agencies develop timeliness measures for each phase in the redress process.

Additionally, the TSC's redress reviews have identified that the database contains records for individuals that should not be watchlisted and that some watchlist records are inaccurate or incomplete. We believe that these results provide a further indicator that watchlist data needs continuous monitoring and attention. We also believe that the TSC should use information related to terrorist watchlist identities that are frequently the subject of watchlist encounters to proactively initiate redress reviews before complaints are filed.

Our report contains detailed information on the full results of our follow-up review of the TSC and contains recommendations to help the TSC carry out its important role in the terrorist watchlisting process.

Summary of Watchlist Nomination, Screening, and Redress Processes

Agencies that conduct counterintelligence, counterterrorism, and law enforcement activities provide information to the FBI and the National Counterterrorism Center (NCTC) on suspected or known terrorists who are nominated for inclusion on the consolidated terrorist watchlist maintained by the TSC.[4] The FBI is responsible for submitting to the TSC all domestic terrorist identity nominations, and NCTC is responsible for submitting international terrorist identity nominations.[5] These two agencies employ analysts who review the information on the known or suspected terrorist identity and forward an unclassified subset of information to TSC analysts, who then review the information to ensure that all required criteria are met

[4] NCTC was established on May 1, 2003, to develop comprehensive threat assessments through the integration and analysis of terrorist information collected domestically and abroad by the U.S. government. NCTC is a component of the Office of the Director of National Intelligence and was formerly known as the Terrorist Threat Integration Center.

[5] The FBI is a source agency for domestic and international terrorist information; it forwards relevant information to NCTC on suspected or known international terrorists.

to incorporate the identity record in the TSC's consolidated terrorist screening database (TSDB). As additional information is obtained that either enhances the identifying information or indicates that the individual has no nexus to terrorism, source agencies must also submit this information through the nominating process to effect watchlist record modifications and deletions, as appropriate.

The review performed by analysts at NCTC, the FBI, and the TSC includes an analysis of information supporting the watchlist nomination, as well as an examination of the quality, accuracy, and sufficiency of the identity information.[6] Thus, all identity records undergo a two-stage review before inclusion in the TSDB: (1) at NCTC and then at the TSC for international terrorist identities, or (2) at the FBI and then at the TSC for domestic terrorist identities.

The TSC shares the terrorist information contained in the TSDB by sending it "downstream" to other government screening systems where frontline screening agents can use the information to identify individuals against TSDB records.[7] The following are examples of three databases that contain information from the TSC's consolidated watchlist: (1) an employee of the U.S. Customs and Border Protection (CBP) agency at a U.S. port-of-entry searches the DHS's Interagency Border Inspection System (IBIS) to determine if a person should be granted access to the United States, (2) a state police officer stops a vehicle for a traffic violation and queries the driver's name in the FBI's National Crime Information Center (NCIC) system, and (3) a State Department consular affairs official searches the Consular Lookout and Support System to determine if a foreign national should be granted a visa to visit the United States. The TSC reported that approximately 270 million individuals are screened by frontline screening agents and law enforcement officers each month.[8]

When a name appears to be a match against the terrorist watchlist, frontline screening and law enforcement personnel contact the TSC's

---

[6] The TSC's general criterion for including a record in the consolidated watchlist database is that the nominating agency must have provided evidence of a nexus to terrorism. From a data perspective, the minimum criteria for inclusion of a terrorist identity into the TSDB are that the record contains at least a partial name (e.g., given name, surname, or both) and at least one additional piece of identifying information (e.g., date of birth).

[7] A description of each of the downstream screening systems is contained in Appendix II.

[8] The TSC provided data on screening agency encounters from February through April 2007. We reported the average of these 3 months.

24-hour call center for assistance in confirming the subject's identity. In responding to such a call, the TSC Call Center staff searches the TSDB and other databases to determine if a terrorist watchlist identity match exists. Between the TSC's inception in December 2003 and May 2007, the TSC has documented more than 99,000 encounters for which its call center was contacted. TSC data shows that 53.4 percent of these calls were determined to be a positive match to a terrorist watchlist identity in the TSDB. In those cases, the TSC contacted the FBI, which is responsible for initiating any necessary law enforcement action. In 43.4 percent of these calls, it was determined that the encountered individual did not match the watchlisted identity, and the TSC Call Center staff instructed the frontline screening agent of this resolution. In the remaining 3.2 percent of the encounters, the TSC Call Center staff could not definitively determine if the match was positive or negative and therefore forwarded these calls to the FBI.

The nature of the U.S. government's actions to screen individuals against the consolidated terrorist watchlist can result in individuals being delayed or detained during security screenings. This can range from an individual being subjected to enhanced security screening and slight delays to missing a flight or being detained for a long period of time. Persons stopped may be actual watchlist subjects, individuals misidentified to a terrorist identity, or someone mistakenly included on the watchlist.

In 2005, the TSC created a process for resolving complaints from individuals who were adversely affected by terrorist watchlist-related screenings and who were seeking relief or "redress." Since the creation of a unit dedicated to processing such complaints in 2005, the TSC Redress Office has received 438 terrorist watchlist-related redress complaints.

Known or Suspected Terrorists Missing from Watchlist

Our review revealed continued instances where known or suspected terrorists were not appropriately watchlisted on screening databases that frontline screening agents use to identify terrorists and obtain instruction on how to appropriately handle the subjects. Even a single omission of a suspected or known terrorist from the watchlist is a serious matter. We found at least 20 watchlist records that were not appropriately watchlisted to downstream screening databases. These watchlisting errors are discussed in detail below.

Due to technological differences and capabilities of the various systems used in the watchlist process, the TSC maintains two interconnected versions of the TSDB to allow for the electronic import and export of data. Although the TSC is developing an upgraded TSDB to eliminate the need for the two

systems, in the meantime TSC officials informed us that these two databases should be identical in content and therefore should contain the same number of records. However, we discovered during our review that these two systems had differing record counts. Specifically, on one day that we tested the databases the difference was 18 records, and on a subsequent day the difference was 38 records.

On March 26, 2007, the TSC informed us that the differing record counts were due, in part, to five watchlist records that were missing from the TSC database responsible for exporting watchlist records to most downstream screening databases. Therefore, the associated terrorist identities were not included in downstream databases used to screen individuals against the terrorist watchlist. Further, our testing of a sample of 105 watchlist records revealed 7 additional watchlist identities that were not being exported to all appropriate screening databases. As a result of the TSC's failure to export all terrorist watchlist records to screening databases, these 12 watchlisted individuals could be inappropriately handled during an encounter. For instance, a suspected or known terrorist could be erroneously issued a U.S. visa or unknowingly allowed to enter the United States through a port-of-entry. We discussed these records with TSC officials who agreed with our findings and began correcting these omissions.

During the course of our review, we were also informed by TSC officials that in September 2006 they had identified 2,682 records in the TSDB that were not being exported to any screening database. Working with NCTC, the TSC determined that 2,118 of these records should not have been watchlisted in any system and needed to be removed from the TSDB.[9] TSC officials conducted a manual review of the remaining 564 records and determined that 8 had not been appropriately watchlisted and needed to be renominated to the TSDB.

However, despite being responsible for removing outdated or obsolete data from the TSDB, the TSC did not have a process for regularly reviewing the contents of the TSDB to ensure that only appropriate records were included on the watchlist. TSC officials told us that they intend to begin performing a monthly review of the database to identify any records that are being stored in the TSDB that are not being exported to any downstream systems. We believe it is essential that the TSC regularly review the TSDB to ensure that all outdated information is removed, as well as to affirm that all records are appropriately watchlisted.

---

[9] On April 27, 2007, the TSC implemented an information technology solution to delete these records.

Inconsistent FBI Procedure for Processing Watchlist Data

The FBI's Terrorist Review and Examination Unit (TREX) receives requests from FBI agents to include an individual with known or suspected ties to terrorism on the terrorist watchlist. These requests are provided on nomination forms, which are also used to modify previous submissions or remove records from the watchlist. Analysts at TREX review the nomination information for accuracy and completeness. Once verified, nomination forms for known or suspected *domestic* terrorists are electronically forwarded to the TSC where a TSC analyst manually enters the information into the TSDB. This information is electronically distributed to the downstream screening agency data systems, including the FBI's Violent Gang and Terrorist Organization File (VGTOF), which is part of the NCIC system.

By contrast, once the TREX analyst verifies an FBI-generated *international* terrorist nomination, the analyst enters the information into VGTOF directly and then submits the nomination form to NCTC. Following its review and vetting, the NCTC analyst manually enters the information into its database – the Terrorist Identities Datamart Environment (TIDE) – that in turn feeds the information to the TSDB. Because TREX has already entered the record into VGTOF, it is not necessary for the TSC to export the record it receives from TIDE to VGTOF. Therefore, these records are not exported from the TSDB to VGTOF.[10] Because these VGTOF records will not receive electronic modifications or deletions from the TSDB, the TSC and TREX have agreed that TREX will be responsible for ensuring FBI-originated international watchlist records in VGTOF are accurate, complete, and current.

The FBI's direct entry of international terrorist watchlist nomination data into a downstream screening database bypasses NCTC and the TSC and makes it difficult for the NCTC and the TSC to carry out their responsibilities related to watchlist nominations and records. In our opinion, this process does not comport with the nomination and data flow procedures agreed to by the partner agencies, which requires agencies to provide to NCTC, rather than directly into a downstream database, information related to known or suspected international terrorists. Additionally, we believe the FBI's practice is cumbersome for the TSC and creates unnecessary data errors, anomalies, and inconsistencies as described below.

---

[10] To alert the TSC of this non-standard entry of records into the TSDB, the TSC implemented a special flag, referred to as "FBI sole source," for FBI-originated international records. This designation precludes all future electronic transactions, including related modifications and deletions, from being exported from the TSDB to VGTOF.

To test for data accuracy and consistency, we reviewed a judgmental sample of 50 FBI-originated additions or modifications to the watchlist.[11] We found that while the records for the domestic terrorist nominations were generally accurate, the international terrorist nominations were not. We identified 16 records with 28 instances in which the identifying information related to international terrorists was inconsistent between the nomination form, VGTOF, TIDE, TSDB, or other screening systems. According to TSC officials, TREX analysts frequently augment the data on the nomination forms with information they glean from FBI case files and enter this additional information into the VGTOF system. However, this supplemental case information is not forwarded to NCTC and as a result the information is not included in TIDE, not sent to the TSDB, and not made available, if appropriate, to downstream screening systems. Further, because TREX enters the record into VGTOF before the addition of any other existing information from other government databases to which NCTC has access, this additional information is often not included in VGTOF. As a result, vital information on watchlist subjects is not being shared with all appropriate screening agencies.

In addition, we found that the FBI's procedures for processing international terrorist watchlist nominations are cumbersome for the TSC and can inadvertently create an incomplete watchlist. The difference in procedures between the FBI's and other agencies' watchlist nominations requires TSC analysts to review every incoming international terrorist nomination and indicate within the record whether it is an FBI source record. If a terrorist watchlist record is improperly designated as an FBI source record, the subset of terrorist watchlist records in VGTOF will be incomplete because that record will not be exported to or modified within VGTOF. TSC staff told us that they were concerned about this because, when reviewing nominations from NCTC, it is often difficult to distinguish between FBI source records and nominations received from other agencies. In fact, TSC staff stated that there was a period of time (possibly as long as a year) in which many records had been improperly designated as FBI-originated records and vice versa. In March 2007, the TSC and NCTC addressed this problem by developing a method to permit TSC analysts to more easily identify FBI source records.

FBI officials responded to our concerns by stating that they had implemented their nomination procedures to ensure that FBI international terrorist information was entered into VGTOF in a more efficient manner. Yet, our review of 70 FBI record transactions (50 nominations previously

[11] The total sample of 50 records consisted of 25 each for domestic and internationally known or suspected terrorists. These 50 records were part of our 156 watchlist record sample that we selected for testing.

mentioned and 20 deletions) revealed that although the transactions were entered into VGTOF in a timely manner, the transactions were not incorporated into the TSDB in a timely fashion.[12] Specifically, 18 of the 70 transactions took more than 5 days for TREX to process, with one transaction taking 35 days. In addition, we identified 2 instances in which TREX erroneously delivered nomination forms for domestic terrorists to NCTC that resulted in delays of 6 and 16 days, respectively.

Delays in including terrorist information in the consolidated database present a significant vulnerability to the integrity of the consolidated watchlist. Further, the FBI's current practice of bypassing NCTC and the TSC and entering international terrorist-related data directly into VGTOF increases the likelihood that watchlist information within the TSDB, TIDE, VGTOF, and other downstream databases is inaccurate and incomplete. As a result, we recommend that the FBI, NCTC, and TSC work together to design a more consistent and reliable process by which FBI-originated international terrorist information is provided to NCTC for inclusion in TIDE and disseminated to the TSDB and downstream screening systems, including VGTOF.

Duplicate Terrorist Watchlist Records

Multiple records containing the same unique combination of basic identifying information can needlessly increase the number of records that a call screener must review when researching a specific individual. In addition, when multiple records for a single identity exist, it is essential that the identifying information and handling instructions for contact with the individual be consistent in each record. Otherwise, the screener may mistakenly rely on one record while a second, more complete record may be ignored. This can result in important information being missed. Further, inconsistent handling instructions contained in duplicate records may pose a significant safety risk for law enforcement officers or screeners.

In reviewing the TSDB for duplicate records, we defined duplicate records as those records that contain the same identifying information for five primary identifying fields – [SENSITIVE INFORMATION REDACTED].[13] In our June 2005 TSC report, we identified 31 such instances of duplicate records in the TSDB and recommended that the TSC implement corrective

[12] Officials from NCTC, the TSC, and TREX stated that each agency attempts to process nominations to the watchlist within 1 day.

[13] For each terrorist watchlist record in the consolidated database, only these five fields are exported to downstream systems for use in identifying suspected or known terrorists during the watchlist screening phase.

action. For our current audit, we again determined that duplicate records existed within the TSDB and that the occurrence of duplicates had increased significantly. In March 2007, we found that the TSDB contained 2,533 repeated combinations in the 5 core fields involving 6,262 watchlist records. For example, one unique combination of the 5 core fields had 19 associated records. Further, our analysis of the 6,262 duplicate TSDB records indicated that at least 20 percent had some discrepancy in handling instruction, identifying information, or watchlist export designation. For example, we identified one individual with duplicate identity records in the consolidated watchlist. Because both records pertained to the same individual, the instructions for handling the subject should be consistent. However, we identified significant differences between the records regarding handling instructions and additional warnings related to the individual. Specifically, one record noted that the individual was "armed and dangerous with violent tendencies" and also had a valid arrest warrant. The other record did not contain this important information. These types of inconsistencies place screeners and law enforcement officers at undue risk and could potentially result in the admittance of a dangerous individual into the United States.

According to the TSC Chief Information Officer (CIO), the TSC does not have an ongoing process to review the TSDB for duplicate records. Based on our findings, however, the TSC CIO stated that the TSC plans to implement a procedure to conduct weekly reviews of the TSDB for duplicate records and forward any issues to the TSC's internal quality assurance unit for review.

The TSC's Watchlist Quality Efforts

Our June 2005 audit report identified weaknesses in the completeness and accuracy of the consolidated watchlist. At that time, TSC management acknowledged that it needed to focus more attention on ensuring the quality of the watchlist. We recommended that the TSC regularly review and test the information contained in the consolidated watchlist database to ensure the data is complete, accurate, and non-duplicative. We also recommended that the TSC coordinate with participating agencies and establish procedures to identify and resolve missing and conflicting record information.

In response to our recommendations, the TSC increased its quality assurance efforts and implemented a data quality improvement plan. Additionally, in November 2006, the TSC's consolidated terrorist watchlist database was upgraded to incorporate a tracking feature for quality assurance activities. As a result of this upgrade, individual watchlist records in the database now contain a record (referred to as a QA ticket) in which

TSC staff can record all quality assurance work that has been performed on that record.

The Nominations and Data Integrity Unit (NDIU) is responsible for performing the TSC's activities related to ensuring the quality and accuracy of the watchlist. The NDIU's activities for ensuring the quality of watchlist information can be categorized into three areas: (1) reviewing incoming watchlist data (referred to as the single review queue); (2) performing reviews of historical records following an encounter where the TSC identifies a potential discrepancy in watchlist records; and (3) conducting special quality assurance projects, such as performing a targeted review of the Transportation Security Administration (TSA) No Fly list.[14] As of March 2007, the TSC had assigned 34 staff to this unit. In comparison, as of September 2004 the TSC had 12 staff assigned responsibility for nominations and data integrity tasks, including 1 staff member that was dedicated solely to quality assurance matters.

To examine the TSC's efforts to ensure the quality of the information in the TSDB, we examined 156 TSDB records that had been subjected to the TSC's quality assurance procedures. Of these 156 records, 36 involved record deletions and we found that each had been handled appropriately. Using the remaining sample of 120 records, we performed tests to determine if the watchlist records were accurate. We found that, in general, the TSC's actions to review records as part of a targeted special project successfully ensured the quality of the data, and we identified virtually no errors in the 15 records we tested in connection with special project reviews. In contrast, our examination of 105 records subjected to the single review queue or post-encounter quality assurance reviews revealed that 38 percent of these tested records continued to contain errors or inconsistencies that were not identified through the TSC's quality assurance efforts.

In general, we believe the actions the TSC has taken to improve quality assurance since our last audit are positive steps. We also recognize that it is impossible to completely eliminate the potential for errors. However, the inaccuracies that we identified in TSDB records that had undergone the TSC's quality assurance processes underscore the need for additional actions to ensure that the TSDB is a reliable source of information about known or suspected terrorists. The results of our testing and analysis of the TSC's quality assurance efforts are summarized below.

---

[14] [SENSITIVE INFORMATION REDACTED]

The TSC's Review of the No Fly List

In July 2006, the Homeland Security Council Deputies Committee issued guidance on how to correctly apply its criteria for including individuals on the No Fly list. Subsequently, the TSC submitted all TSDB records associated with individuals who were on the No Fly list to a comprehensive quality assurance review using this guidance. When the TSC began its review in July 2006, the No Fly list contained 71,872 records. The TSC completed its special review of the No Fly list on January 31, 2007, determining that the No Fly list should be reduced to 34,230 records.[15] The TSC recommended 22,412 records for removal from the No Fly list and placement on the TSA's Selectee list.[16] For another 5,086 records, the TSC determined that the individual did not require inclusion on either the No Fly or Selectee list.

We selected and reviewed 15 records that were part of the TSC's review of the No Fly list. We did not find any data inaccuracies or inconsistencies in these records. Each record's basic identifiers [SENSITIVE INFORMATION REDACTED] were shown consistently in all of the affected databases and each record remained the same or was downgraded from the No Fly list in accordance with the final recommendation of the TSC.

Data Inaccuracies and Inconsistencies Exist After Quality Assurance Review

Unlike our review of the No Fly list special project, however, our examination of records passed through the TSC's single review queue or encounter-driven quality assurance processes revealed that records were still likely to contain errors or inconsistencies. We examined 105 records to determine if basic information [SENSITIVE INFORMATION REDACTED] was shown consistently in all of the affected databases. We also verified that correct handling codes were included on watchlist records. In short, our testing revealed that records the TSC reviewed through its routine quality assurance processes frequently continued to contain errors, which indicates weaknesses in the TSC's practices for verifying the integrity of the original watchlist data.

As previously reported, we found that 7 of the 105 records we tested were not exported to appropriate downstream databases. In addition, our

---

[15] During its review of the No Fly list, the TSC continued to receive routine No Fly list additions, modifications, and deletions through the watchlist nomination process. As a result, it is not possible to subtract the special project-driven No Fly list changes from the starting point of 71,872 records and obtain the correct number of No Fly records as of January 31, 2007.

[16] [SENSITIVE INFORMATION REDACTED]

review of the 105 watchlist records that had been subjected to the TSC's single review queue or encounter-driven quality assurance processes revealed that 35 records had inconsistent identifying information when comparing one or more fields in the TSC's consolidated watchlist records with the source or screening agencies' database records. Identifying information related to terrorist watchlist identities must be accurate and consistent across all systems involved in the watchlisting process, namely the TSDB, the downstream systems, and the nominating agencies' systems. Inconsistent data can confuse or delay TSC Call Center operators in their efforts to determine whether an encountered individual is a positive match to a known or suspected terrorist. Further, inconsistent information among databases involved in terrorism screening indicates that at least one record may be incorrect. Incorrect records can also misinform frontline screening agents and contribute to the misidentification of a person not on the watchlist or the inappropriate release or admittance of a dangerous individual. Finally, our testing of the 105 sample watchlist records also revealed that 5 records contained incorrect handling instructions.

During our review, it became apparent that both the TSC's quality assurance efforts and our reviews of watchlist records identified errors and inconsistencies in incoming records from the source agencies – NCTC and the FBI. We discussed the watchlist nomination process with NCTC and FBI officials, and both agency representatives stated that records are reviewed for accuracy, completeness, and consistency before the records are forwarded to the TSC. However, these efforts are failing to identify a significant number of deficiencies in the nominated records. The TSC's quality assurance efforts, therefore, are hampered by the inaccurate and incomplete source material.

Untimely Resolution of Quality Assurance Issues

Delays in the closure of quality assurance matters directly affects the accuracy of the consolidated watchlist database because records can contain inaccurate and incomplete information for extended periods of time while the matter is being resolved. We examined a sample of 51 quality assurance matters opened between February 2006 and February 2007. We found that these matters were open from 0 days (matter was closed the same day as it was opened) to 329 days. On average, the quality assurance matters examined in our sample were open for 80 days.

The TSC has not established a performance measure identifying what it believes to be an acceptable duration for its analysts to complete a quality assurance review. According to TSC personnel, NDIU analysts were supposed to follow up on all quality assurance matters every 30 days.

However, the TSC does not have a mechanism such as a standardized report or digital dashboard that catalogs all outstanding quality assurance matters.[17] In concert with the development of timeframes for resolving quality assurance matters, we believe the TSC should develop a system, including an aging schedule, to track its quality assurance work.

Weaknesses in TSC Quality Assurance Policy and Oversight

We also found that the TSC has implemented necessary enhancements in its quality assurance resources and processes since our last audit. Our examination of records submitted to the TSC's No Fly list special project showed that the TSC's review was generally successful in ensuring the quality of watchlist records. However, the inaccuracies we found in our review of watchlist records that were subjected to the TSC's single review queue and post-encounter quality assurance reviews – examinations that are less comprehensive than the No Fly list review – indicate a need for further enhancements to these quality assurance processes.

During our audit, we performed a physical observation of TSC analysts conducting quality assurance reviews of watchlist records. We noted that the analysts' method of performing their reviews was not always consistent. For example, some analysts inspected all of the documents supporting a TSDB record while other analysts relied solely upon summary information. We also found that the analysts were not consistently documenting their quality assurance work.

We believe that this situation was caused by inadequate standard operating procedures (SOP) detailing the TSC's quality assurance processes and by insufficient training. The TSC has an SOP for its quality assurance efforts, but the document was last revised on August 16, 2005. Moreover, the document provides incomplete guidance to analysts on the processing of quality assurance matters and did not mention the existence of special quality assurance projects and encounter-based quality assurance reviews. Further, while the SOP informs the analysts performing standard quality assurance reviews how to examine watchlist records, it fails to detail what fields, supporting information, and other aspects of the records the analysts should be verifying and comparing. In addition, these procedures do not instruct the analysts on the necessary actions to take when inaccurate or incomplete information is identified.

[17] A digital dashboard is a business management tool that visually displays the status of a business project. The dashboard can provide warnings, next steps, action notices, and summaries of a project.

Additionally, the TSC provides its quality assurance analysts only a few days of training before allowing them to work independently, and no supplemental training is required. Moreover, the TSC does not have a mechanism for regularly evaluating the work of its quality assurance analysts to help ensure that the analysts are performing appropriate reviews and keeping abreast of any process changes. We believe that the TSC should develop a more detailed and comprehensive quality assurance SOP to better guide NDIU analysts through their work. In addition, the TSC should develop a mechanism to routinely review its analysts' work to identify processing deficiencies and areas requiring additional training.

Insufficient Process to Comprehensively Review Watchlist Data Quality

In response to our previous TSC audit that identified errors and inconsistencies in the watchlist records, the TSC stated that it intended to conduct a record-by-record review of the approximately 400,000 records in the TSDB. The TSC later estimated that this review would not be complete until 2012. In February 2007, TSC officials stated that the review was being performed through its three-pronged quality assurance strategy – the single review queue, encounter-driven quality assurance reviews, and special projects. TSC officials told us that they plan to examine the TSDB following the completion of the ongoing special projects and determine how many TSDB records have not yet been reviewed. The TSC then plans to review any previously unexamined TSDB records.

In February 2007, TSC officials told us that since the inception of the single review queue in March 2006 over 670,000 TSDB records had been reviewed and the agency had revised its estimated completion date. TSC officials now project that the record-by-record review will be complete by the end of 2007. However, we believe that the TSC may have overstated the number of records reviewed and is underestimating the amount of time and effort that it will take to complete its review of the entire TSDB. We base these conclusions on the following factors:

- As previously discussed, the TSC's single review queue and encounter-driven quality assurance processes do not sufficiently ensure the quality of the watchlist records. Therefore, the TSC should reconsider records examined in these processes in its count of records reviewed.

- The number of records reviewed is not limited to the review of unique records. Rather, the TSC's quality assurance process allows for one record to be reviewed multiple times: through the single review queue, following each request to modify or delete

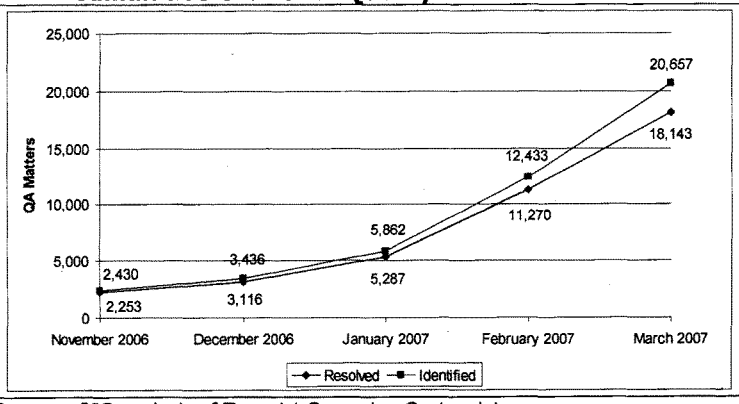
the record, in accordance with one or more special projects, and subsequent to each encounter. Therefore, we believe that the TSC's cumulative tally of records reviewed can include records counted multiple times.

- Between September 2006 and April 2007, the TSDB grew at an average rate of over 20,000 records per month. This growth adds to the analysts' workload. Since April 2004, the TSDB has more than quadrupled in size, growing from 150,000 to 724,442 records in April 2007.

- As of February 2007, there were about 3,000 open quality assurance matters that required follow-up.

As part of this review, we obtained TSC data for the number of quality assurance matters identified and resolved between November 2006 and March 2007.[18] These data show that the TSC is identifying incomplete or inaccurate information in TSDB records faster than the matters are being resolved by source agencies. As the following graph shows, cumulative differences between identified quality assurance matters and addressed quality assurance matters increased from 177 in November 2006 to 2,514 in March 2007. This differential also shows that the TSC is regularly identifying errors or concerns with known or suspected terrorist records.

Cumulative Growth in Quality Assurance Matters



Source: OIG analysis of Terrorist Screening Center data

[18] The TSC only could provide historical data on quality assurance matters since November 2006 when the latest version of the TSDB was deployed.

We believe that if the number of watchlist records and the associated quality assurance matters in the TSDB continue to grow, the TSC will not complete the record-by-record review of the TSDB by the end of 2007 as anticipated. The TSC needs to accurately determine the magnitude of the unexamined portion of the TSDB so that the TSC can implement a sound plan for examining those records and develop a realistic completion date for the project. Further, the TSC should establish benchmarks against which it can measure its progress.

Watchlist Redress

We found that the TSC's efforts to resolve terrorist watchlist redress matters since our previous audit have improved. For example, in 2005 the TSC created a dedicated unit for redress matters. The TSC also helped to spearhead the creation of a multi-agency Memorandum of Understanding (MOU) focusing on watchlist redress (Redress MOU) and developed a comprehensive Redress SOP to ensure watchlist information for redress complainants is accurate, complete, and current.

The frontline screening agencies, such as DHS and the State Department, receive complaints from persons seeking relief, or "redress," related to the terrorist watchlist screening process. Matters believed to be related to a terrorist watchlist identity or an encounter involving the watchlist are forwarded to and reviewed by the TSC.[19] The TSC Redress Office conducts an examination of the watchlist records, reviews other screening and intelligence databases, and coordinates with partner agencies for additional information and clarification. The TSC determines if any watchlist records need to be modified or even removed from the watchlist, ensures these identified changes are made, and notifies the referring frontline screening agency of its resolution. The frontline screening agency is then responsible for responding to the complainant. TSC policy requires that responses to complainants neither confirm nor deny the existence of watchlist records relating to the complainant. According to TSC officials, this nondisclosure policy protects U.S. counterterrorism operations and intelligence objectives and safeguards the personnel involved in these sensitive activities.

We judgmentally selected 20 redress complaints received by the TSC between January 2006 and February 2007 and reviewed the corresponding files to determine if the TSC followed its Redress SOP for resolving

[19] On occasion, the TSC receives a redress complaint referral from a screening agency and determines that the complaint does not relate to a terrorist watchlist identity or an encounter involving the watchlist. The TSC returns such complaints to the referring agency for resolution.

complaints. We found that in each of the sampled cases the TSC complied with its Redress SOP, including reviewing the applicable screening and intelligence databases, coordinating with partner agencies, and reaching appropriate resolutions. However, the TSC's redress activities identified a high rate of error in watchlist records. In addition, we believe the TSC needs to address the timeliness of redress complaint resolutions.

Significant Watchlist Record Changes Following TSC Redress Review

As part of our review, we analyzed TSC data on the resolution of terrorist watchlist redress complaints. Between January 2005 and February 2007, the TSC closed 388 of the 438 redress complaints it received. Through its comprehensive redress review process, the TSC concluded that 45 percent of the watchlist records related to redress complaints required modification or deletion from the watchlist. In some instances, the TSC stated that redress resolution may have been simultaneous to current watchlist record updates. We also found instances where the TSC Redress Office found inaccuracies in the watchlist record or discovered additional, relevant information that had not been passed to the TSC.

The Privacy Officer acknowledged that the high percentage of records requiring modification or removal may point to deficiencies in the terrorist watchlist nomination process and with nominating agencies not providing the TSC additional information important for appropriately updating terrorist records. We believe that the results of the TSC's redress reviews are a further indicator that watchlist data needs continuous monitoring and attention.

Untimely Resolution of Redress Complaints

The TSC is responsible for adjudicating watchlist-related complaints through its review process and working with nominating and screening agencies to resolve the matters in a timely fashion. The Redress MOU states that one of the goals of the redress process is to provide a timely review, which ensures any required changes to the watchlist are implemented efficiently so that watchlist records do not continue to be inaccurate.

We reviewed TSC files and statistics for closed redress matters to determine the efficiency of redress reviews. This data revealed that it took the TSC, on average, 67 days to close its review of a redress inquiry. For redress matters referred to the TSC during the last semiannual period in our review (July through December 2006), it took the TSC an average of 57 days to finalize its review. In addition to these closed matters, we also

analyzed the 50 open redress complaints as of February 27, 2007, and determined that these matters had been open an average of 61 days. Of these complaints, 38 percent were open over 60 days, including 2 inquiries that were pending over 180 days.

Open TSC Redress Matters
(as of February 27, 2007)

Number of Days Open	Number of Open Redress Matters	Percentage of Total Open Redress Matters
180 days or more	2	4%
90-179 days	12	24%
60-89 days	5	10%
30-59 days	11	22%
less than 30 days	20	40%
Total	**50**	**100%**

Source: The Terrorist Screening Center Redress Office

Our review of redress files indicated that delays were primarily caused by three factors: (1) the TSC took a long time to finalize its determination before coordinating with other agencies for additional information or comment, (2) nominating agencies (the FBI and NCTC) did not provide timely feedback to the TSC or did not process watchlist paperwork in a timely manner, and (3) certain screening agencies were slow to update their databases with accurate and current information. For example, our file review found that the State Department and the DHS's Customs and Border Protection did not revise encounter records in a screening database in a timely fashion to reflect modified or removed terrorist identities.

TSC officials acknowledged that it has not developed response timeframes for redress matters with its partner agencies. While the Redress MOU states that one of the goals of the redress process is to provide a timely review, the MOU does not define what constitutes a reasonable timeframe. We believe that timeliness measures could be used as standards to evaluate the U.S. government's efficiency in resolving terrorist watchlist redress inquiries and responding to complainants. Because the TSC is central to resolving any complaint regarding the content of the consolidated terrorist watchlist, we encourage the TSC to organize the U.S. government's effort to develop timeliness measures for the entire watchlist redress process.

More Proactive Efforts Needed to Mitigate Incidence and Effect of Watchlist Misidentifications

The TSC does not have any policy or procedures to proactively use information from encounters to reduce the incidence and impact of terrorist watchlist misidentifications. For example, the TSC could program its encounter tracking system to automatically generate a quality assurance lead for the TSC to perform a comprehensive review of watchlist records that have been the subject of a certain number of encounters. Moreover, the TSC's strategic plan does not include goals or actions associated with reducing the incidence of misidentifications or the impact on misidentified persons other than that covered by a formal redress process. Considering that nearly half of all encounters referred to the TSC Call Center are negative for a watchlist match, we believe the TSC should consider misidentifications a priority and develop strategic goals and policy specific to mitigating the adverse impact of the terrorist screening process on non-watchlist subjects, particularly for individuals who are repeatedly misidentified as watchlist identities.

Conclusion and Recommendations

We found that since our June 2005 report the TSC has enhanced its staffing and implemented practices to handle redress matters and help ensure the quality of terrorist watchlist information. Our review also found that the TSC's processes for examining watchlist records as part of its special project (the No Fly list examination) and redress complaint reviews were comprehensive and improved watchlist data quality.

However, we found continued weaknesses in other watchlist processes and significant deficiencies in watchlist data. We determined that the FBI's fragmented international terrorism nomination process caused many terrorist identity records to be inaccurate, incomplete, and inconsistent across watchlist systems. Additionally, the TSC's single review queue and encounter-driven quality assurance processes were not successful in ensuring the quality of watchlist records. We also found that TSC quality assurance analysts employed disparate procedures in their reviews, and the TSC did not have a mechanism for conducting oversight of its quality assurance efforts.

We believe the TSC should consider incorporating elements from its more comprehensive reviews in its other quality assurance processes to help better ensure the quality of watchlist data. Further, the TSC should develop detailed, comprehensive standard operating procedures and an oversight function for quality assurance matters.

In addition to these process deficiencies, we found suspected or known terrorists still missing from the watchlist or downstream screening systems, incorrect terrorist handling codes on watchlist records, and duplicate identity records within the TSDB. Moreover, our testing of specific watchlist records revealed that records submitted to a TSC quality assurance review contained significant errors –38 percent of the records tested contained data that was inaccurate, incomplete, inconsistent, or not current. Further, our examination of TSC redress data for positive-match encounters showed that the TSC determined that 45 percent of the watchlist records referred for review required modification or removal. In addition, watchlist agencies, including the TSC and nominating and screening agencies sometimes caused unnecessary delays in closing redress inquiry reviews.

The results of our testing of watchlist records, as well as the TSC finding that many records involved in its redress reviews required modification or removal, indicate a deficiency in the integrity of watchlist information. We recommend that the TSC resolve current process weaknesses – within the TSC and at nominating agencies – that are contributing to the weaknesses we identified in the watchlist data. The TSC also needs to develop and implement a plan to complete a sufficient analysis of all watchlist records in a timely fashion.

This report contains 18 recommendations to help the TSC improve its operations and the quality of watchlist data. These recommendations include two recommendations to the FBI directly for matters pertaining to its operations outside the TSC.

REDACTED FOR PUBLIC RELEASE

FOLLOW-UP AUDIT OF THE TERRORIST SCREENING CENTER

TABLE OF CONTENTS

INTRODUCTION **1**

Purpose of the Consolidated Watchlist 2
Overview of Watchlist Nomination and Screening Processes 3
TSC Encounter Management 6
Number of Terrorist Watchlist Records 7
Handling Instructions 8
OIG's Audit Approach 10

FINDINGS AND RECOMMENDATIONS **12**

I. DATA ACCURACY AND TIMELINESS **12**

Structure of the TSDB 12
Records Not Designated for Any Watchlisting 17
FBI Procedure for Processing Watchlist Data 18
Duplicate Records 20
Inclusion of Known Terrorists in the TSDB 24
Conclusion 24
Recommendations 25

II. QUALITY ASSURANCE **27**

Overview of the TSC's Quality Assurance Process 27
OIG Analysis of TSC Quality Assurance Efforts 31
Quality Assurance Management and Oversight 35
TSC Efforts to Enhance Terrorist Watchlisting 41
Conclusion 42
Recommendations 43

III. TERRORIST WATCHLIST REDRESS **45**

Overview of the TSC's Redress Efforts 45
Multi-agency Redress Agreement 47
Overview of the Terrorist Watchlist Redress Process 47
Disposition of Redress Complaints 51
Timeliness of Processing Redress Complaints 53
Response to Redress Complainants 56
Appeal of Redress Disposition 57
Proactive Redress 57
Conclusion 59
Recommendations 60

STATEMENT ON INTERNAL CONTROLS 61
STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS 62
APPENDIX I: OBJECTIVES, SCOPE, AND METHODOLOGY 63
APPENDIX II: SYSTEMS USED IN THE TERRORIST WATCHLIST PROCESS 67
APPENDIX III: DIAGRAM OF TERRORIST WATCHLIST DATAFLOW ... 69
APPENDIX IV: ACRONYMS 70
APPENDIX V: TERRORIST SCREENING CENTER RESPONSE 71
APPENDIX VI: OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT 77

INTRODUCTION

Prior to the establishment of the Terrorist Screening Center (TSC), the federal government relied on at least a dozen separate terrorist watchlists maintained by different federal agencies. The TSC was created by Homeland Security Presidential Directive-6 (HSPD-6), signed on September 16, 2003. In that directive, the TSC was required to integrate the existing U.S. government terrorist watchlists and provide 24-hour, 7-day a week responses for agencies that use the watchlisting process to screen individuals who, for example, apply for a visa, attempt to enter the United States through a port-of-entry, attempt to travel internationally on a commercial airline, or are stopped by a local law enforcement officer for a traffic violation. HSPD-6 mandated that the TSC achieve initial operating capability by December 1, 2003.

The TSC is a multi-agency organization administered by the Federal Bureau of Investigation (FBI). Following the issuance of HSPD-6, the Attorney General, the Director of Central Intelligence, and the Secretaries of the Department of Homeland Security (DHS) and the Department of State (State Department) entered into a Memorandum of Understanding (MOU) describing the new organization and the level of necessary cooperation, including the sharing of staff and information from the four participating agencies. The MOU stipulated that the Director of the TSC would report to the Attorney General through the FBI and required that the Principal Deputy of the TSC be an employee of DHS. Since fiscal year (FY) 2004, the participating agencies have shared responsibility for funding and staffing the TSC, and for FY 2007 the TSC has a budget of approximately $83 million and 408 positions.[20]

In June 2005, the Department of Justice (DOJ) Office of the Inspector General (OIG) issued an audit report that examined the TSC's operations from the time of its inception.[21] The OIG reported that although the TSC had made significant strides in becoming the government's single point-of-contact for law enforcement authorities requesting assistance in identifying individuals with possible ties to terrorism and had developed a consolidated terrorist watchlist database, the TSC had not ensured that the information in that database was complete and accurate. For example, we found instances where the consolidated database did not contain names that should have been

---

[20] As of June 2007, the TSC had 323 personnel on board.

[21] Department of Justice, Office of the Inspector General, *Review of the Terrorist Screening Center*, Audit Report 05-27, June 2005.

included on the watchlist. In addition, we found inaccurate or inconsistent information related to persons included in the database. In that review, we also found problems with the TSC's management of its information technology (IT), an integral part of the terrorist screening process.

TSC officials attributed some of these deficiencies to the immediate need during the earliest days of the TSC to develop a comprehensive database of potentially high-risk suspects. TSC officials explained that blending different types of data in various formats from multiple sources with varying technological infrastructures had resulted in data inconsistencies and inaccuracies. In addition, technology challenges and frequent record additions, deletions, and modifications affected the TSC's ability to ensure the quality of the watchlist data. Our report included 40 recommendations to the TSC addressing areas such as database improvements, data accuracy and completeness, and staffing.

The purpose of our current follow-up review of the TSC was to determine if accurate and complete records are disseminated to and from the watchlist database in a timely fashion, as well as to assess the TSC's current processes for ensuring the quality of the known or suspected terrorist information. Further, we examined the TSC's efforts to minimize the impact on individuals misidentified as watchlist subjects.

Purpose of the Consolidated Watchlist

One goal of the nation's counterterrorism efforts is to identify suspected terrorists and keep them out of the United States and from harming U.S. citizens both at home and abroad. An essential element of these efforts is the maintenance of a consolidated watchlist containing the names of known and suspected terrorists. This consolidated watchlist should include the most current and complete information and not contain inaccurate, inconsistent, or inappropriate information. Further, similar names and limited information in the watchlist can impair a frontline screening agent (such as a border patrol officer, visa application reviewer, or local police officer) from distinguishing between a suspected terrorist and a mistakenly identified individual. Deficiencies in the terrorist watchlist information also increase the opportunity for a terrorist to go unnoticed or not be properly handled when encountered. Additionally, inadequate information increases the possibility of individuals being misidentified as terrorist watchlist subjects and thereby being detained for more rigorous screening procedures.

Overview of Watchlist Nomination and Screening Processes

When a law enforcement or intelligence agency has identified an individual as a potential terrorist threat to the United States and wants that individual watchlisted, the source agency must nominate that person for inclusion in the consolidated watchlist maintained by the TSC. Similarly, as additional information is obtained that either enhances the identifying information or indicates that the individual has no nexus to terrorism, the record should be either updated or deleted.

All nominations from source agencies to the consolidated watchlist are vetted through the FBI or the National Counterterrorism Center (NCTC).[22] Analysts at NCTC or the FBI review the nomination information and decide whether or not the person is an appropriate candidate for inclusion on the consolidated watchlist. This review includes an evaluation of the information supporting the nomination, an examination of the quality and accuracy of the identifying information, and an examination of whether sufficient identifying information is available.[23] The FBI and NCTC are responsible for providing the TSC an unclassified subset of identifying information for individuals known or suspected to be or have been involved in activities related to terrorism.[24]

---

[22] As stated in the TSC MOU, source agencies responsible for U.S. counterintelligence, counterterrorism, and law enforcement provide information to the FBI and NCTC on suspected or known terrorists who are nominated for inclusion on the consolidated terrorist watchlist maintained by the TSC. The FBI is responsible for submitting to the TSC all domestic terrorist identity nominations, and NCTC is responsible for international terrorist identity nominations. While the FBI is a source agency for domestic and international terrorist information; it forwards relevant information to NCTC on suspected or known international terrorists. Domestic terrorist information is defined as information about U.S. persons that has been determined to be purely domestic terrorism information with no link to foreign intelligence, counterintelligence, or international terrorism.

[23] The TSC's general criterion for including a record on the consolidated watchlist is that the nominating agency must have provided evidence of a nexus to terrorism. From a data perspective, the minimum criteria for inclusion of a terrorist identity into the TSDB are that the record contains at least a partial name (e.g., given name, surname, or both) and at least one additional piece of identifying information (e.g., date of birth).

[24] The TSC also has an emergency nomination process, which is used when there is an imminent threat and a watchlist record needs to be highlighted or created quickly. Under the emergency process, a requesting agency informs the TSC directly and the TSC adds the individual to the consolidated watchlist. The TSC then forwards all the information gathered on the subject to NCTC for subsequent additional vetting and creation of a record at NCTC.

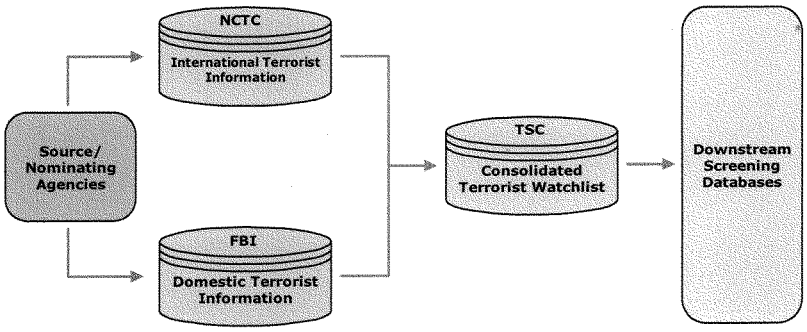
The TSC shares the terrorist information contained in its Terrorist Screening Database (TSDB) by exporting or sending data "downstream" to other screening systems, such as the State Department's Consular Lookout and Support System (CLASS), DHS's Interagency Border Inspection System (IBIS), the Transportation Security Administration's (TSA) No Fly list, the FBI's Violent Gang and Terrorist Organization File (VGTOF) within its National Crime Information Center (NCIC) system, and others.[25] Watchlist information is then available for use by U.S. law enforcement and intelligence officials across the country and around the world.

Personnel working for these organizations routinely encounter individuals as part of their regular duties during various government processes. For example: (1) DHS agents of the U.S. Customs and Border Protection (CBP) agency examine individuals at various U.S. ports-of-entry and search IBIS to determine if a person can be granted access to the United States, (2) State Department officials process visa applications from non-U.S. citizens wishing to visit the United States and search CLASS to determine if the individual should be granted a U.S. visa, and (3) state and local law enforcement officers review the identifying information of individuals encountered through the criminal justice system and query the FBI's NCIC system. In turn, these databases contain terrorist watchlist records so that the federal, state, and local law enforcement screening agents can identify persons that the U.S. government has determined are known or suspected terrorists.

An overview of the flow of watchlist information from nominating agencies to the TSC and ultimate distribution to downstream screening databases is displayed in Exhibit 1-1.

[25] NCIC is a nationwide information system maintained by the FBI that provides the criminal justice community with immediate access to information on various law enforcement data, such as criminal history records and missing persons. The FBI's Criminal Justice Information Services Division is responsible for managing the NCIC database. A description of each of the downstream screening systems is contained in Appendix II.

EXHIBIT 1-1
Terrorist Watchlist Dataflow Diagram[26]



Source: The National Counterterrorism Center

Screening Activities and Hits Against the Terrorist Watchlist

When a name appears to be a match against the terrorist watchlist, requestors receive a return message through their database informing them of the preliminary match and directing them to call the TSC. When a call is received, TSC staff in the 24-hour call center assist in confirming the subject's identity.

To do this, the TSC Call Center staff search the TSDB and supporting databases to locate any additional information that may assist in making a conclusive identification. The caller is immediately informed of any negative search result – such as the subject of the inquiry does not match the identity of an individual on the watchlist.

In general, if the subject is positively identified as a watchlist hit or the match attempt is inconclusive, the TSC call screener forwards the call to the FBI's Terrorist Screening Operations Unit (TSOU), the FBI's 24-hour global command center for terrorism prevention operations. The TSOU is then responsible for making further attempts to confirm the subject's identity and, if necessary, coordinating the law enforcement response to the encounter, including deploying agents to take appropriate action.

[26] A diagram providing a more detailed look at the flow of data in the U.S. government's terrorist watchlisting process is located in Appendix III.

Not all encounters are face-to-face. According to State Department officials at the TSC, when a person located overseas submits an application for a visa, State Department officials search the CLASS database, which receives watchlist information from the TSC. If the search reveals a possible identity match with an individual recorded in the TSDB, the official sends the TSC a cable (a secure, electronic communication). A State Department representative at the TSC reviews the cable along with information from supporting agency databases to determine if the person requesting a visa is an individual with ties to terrorism. This information is then used by U.S. government officials overseas to either process or deny the application.

TSC Encounter Management

To manage information related to "hits" or possible matches against the watchlist, called "encounters," the TSC uses a software application, called the Encounter Management Application (EMA). This system was implemented in July 2004 and includes a record of all encounters since the inception of the TSC. EMA contains the details of all incoming calls, including information about the inquiring law enforcement agency, the databases the TSC staff searched and the information obtained from these systems, the status of the TSC's efforts to confirm an identity match against a watchlist record (i.e., positive, negative, or inconclusive), whether the caller was forwarded to TSOU for further action, and the final disposition of the call. For every inquiry that TSC call screeners refer to the TSOU, the TSC screeners are responsible for obtaining feedback on the disposition of the encounter, such as whether the subject was arrested, questioned, or denied entry into the United States.

EMA provides the TSC with the ability to generate detailed statistics and prepare reports for analysis. Daily status reports are generated from EMA identifying the specific call information, which is reviewed by the TSC's Tactical Analytical Team to identify patterns or threatening circumstances. If any such patterns are identified, the TSC forwards this information to the appropriate intelligence and law enforcement agencies for further review.

As of April 2007, the TSC Call Center had recorded nearly 97,000 watchlist encounters referred by screening agencies since its creation in December 2003. More than 50 percent of this total resulted in a positive identity match. As shown in Exhibit 1-2, 60 percent of the total calls received by the TSC Call Center originated from the U.S. Customs and Border Protection agency.

EXHIBIT 1-2
Watchlist Encounters Referred to the TSC Call Center by Organization
(December 1, 2003, through April 30, 2007)

Referring Agency	Number of Referrals	Percent of Referrals
DHS – CBP	58,266	60
Other Federal	19,965	21
State and Local	17,967	19
Foreign Government	513	<1
Total	**96,711**	**100%**

Source: The Terrorist Screening Center

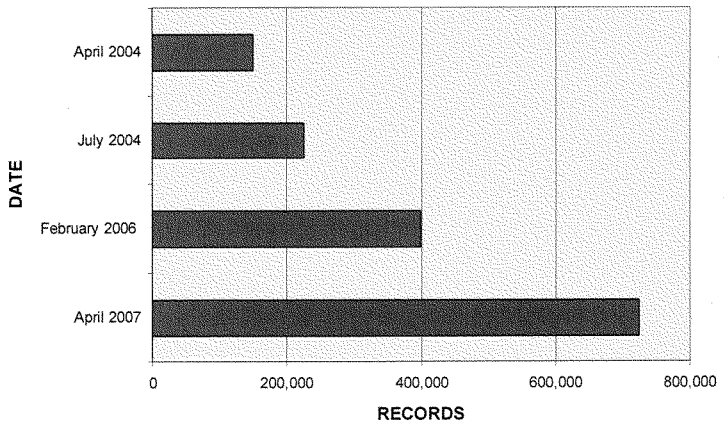
Number of Terrorist Watchlist Records

Since the creation of the TSC in December 2003, the number of records in the consolidated U.S. government watchlist of known or suspected terrorists has significantly increased. We compiled a summary of available database size information, which illustrates the continued growth of the watchlist.

According to TSC officials, there were approximately 150,000 records in the TSDB in April 2004.[27] TSC data indicate that by July 2004 the number of records had increased to about 225,000 records, representing approximately 170,000 unique terrorist identities. Eighteen months later, in February 2006, the TSC reported that the database contained approximately 400,000 records. Most recently, information we obtained from the TSC indicates that the TSDB contained a total of 724,442 records as of April 30, 2007. The vast majority of these records are international terrorist records – less than 1 percent of records related to the identities of suspected domestic terrorists. As shown in Exhibit 1-3, the number of watchlist records contained in the TSDB has more than quadrupled since its inception in 2004.

[27] The reported figure represents the number of *records* in the system. This does not equate to the number of known or suspected terrorists in the system as a single person may have multiple records to account for the use of aliases, alternate identities, and multiple identifying documents. As such, the number of records generally will be larger than the number of suspected or known terrorists on the watchlist.

EXHIBIT 1-3
Number of Terrorist Watchlist Records



Source: OIG analysis of Terrorist Screening Center data

Handling Instructions

Each record within the consolidated watchlist database is designed to contain information about the law enforcement action to be taken when encountering an individual on the watchlist. This information is conveyed through two separate "handling codes" or instructions – one handling code for the FBI and one for the DHS.

FBI Handling Codes - each individual nominated for inclusion in the FBI's screening database, National Crime Information Center's (NCIC) Violent Gang and Terrorist Organization File (VGTOF), is assigned a code used to provide instruction for handling the individual. These codes are assigned based on whether there is an active arrest warrant, a basis to detain the individual, or an interest in obtaining additional intelligence information regarding the individual.[28] Following are the definitions for each code.

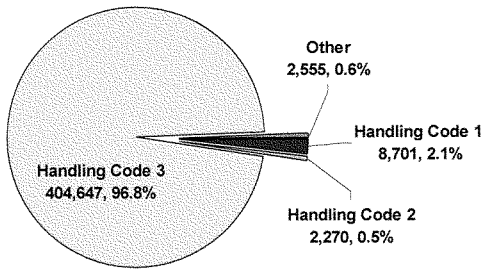
- Handling Code 1 - [SENSITIVE INFORMATION REDACTED]
- Handling Code 2 - [SENSITIVE INFORMATION REDACTED]

[28] Practices and procedures regarding one handling code are classified Secret, and are not, therefore, discussed here.

- Handling Code 3 - [SENSITIVE INFORMATION REDACTED].

All records in the consolidated watchlist database that are eligible for export to VGTOF should have a handling code assigned. Based on our review, we determined that all eligible records contained in the TSDB contained a VGTOF handling code. As depicted in Exhibit 1-4, the majority of the records in the TSDB are designated as Handling Code 3.

EXHIBIT 1-4
Distribution of VGTOF Handling Codes
(as of March 6, 2007)[29]

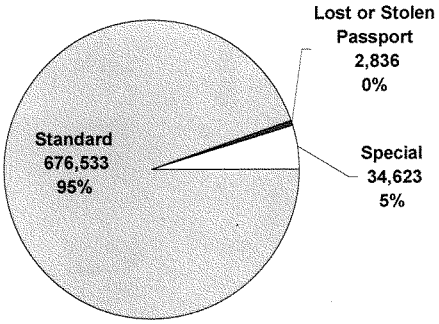


Source: The Terrorist Screening Center

DHS Handling Instructions – each individual nominated for inclusion in the DHS's screening database is assigned one of three codes that provide instructions to law enforcement officials at ports-of-entry. According to TSC officials, each instruction requires the individual to receive additional screening. However, one code provides a less intrusive method for handling known or suspected terrorists because the law enforcement officer is directed to not meet the individual at the arriving plane and not alert the subject of his or her possible watchlist status. Based on our review, we determined that all eligible records in the TSDB contained an IBIS handling instruction. As shown in Exhibit 1-5, approximately 5 percent of the records in the TSDB that are eligible for export to IBIS are designated with this special handling instruction.

[29] The other category relates to the handling code practices and procedures that are classified at the Secret level.

EXHIBIT 1-5
Distribution of IBIS Handling Instructions
(as of April 30, 2007)



Source: The Terrorist Screening Center

OIG's Audit Approach

The objectives of this OIG audit were to: (1) determine if accurate and complete records are disseminated to and from the watchlist database in a timely fashion; (2) review the TSC's efforts to ensure the quality of the information in the watchlist database; and (3) assess the TSC's efforts to address complaints raised by individuals who believe they have been incorrectly identified as watchlist subjects.

To accomplish these objectives, we interviewed more than 45 TSC officials, including the Director, the former Acting Director and Deputy Directors, as well as officials at NCTC, the FBI, and DHS. In addition, we interviewed participating agency representatives and toured facilities to ensure that we obtained a detailed understanding of the working relationships utilized, assistance provided, and communication flow during the terrorist screening process.

To evaluate the accuracy and completeness of the consolidated watchlist, we divided our review into two separate tracks. First, we analyzed the consolidated database as a whole, including a review of the number of records in the database, any duplication that existed within those records, and the associated watchlist processes. Second, we tested individual records within the database for accuracy and completeness. This included reviewing a sample of FBI and other government agency nominated domestic and international terrorist records and tracing these records to the TSDB to determine if the individuals were included in the database and that

the information was accurate, complete, and consistent. In addition, we also checked whether known terrorist names were in the database.

To assess the TSC's efforts to ensure the quality of the information in the watchlist database, we examined the TSC's quality assurance activities and reviewed records subjected to these processes. We also examined the timeliness of the TSC's efforts to resolve matters arising from its review of the accuracy and completeness of the data. This included an evaluation of the TSC's progress to conduct a system-wide, record-by-record review and to improve its quality control processes as a result of recommendations in our previous audit.

To fulfill our third objective, we examined the TSC's policies and procedures for handling inquiries related to individuals who raised complaints following their involvement in a screening encounter. This process is referred to as redress. We evaluated the TSC's efforts to coordinate redress response efforts with other participating agencies, reviewed a sample of redress inquiries, and assessed the timeliness of the TSC's responses to redress inquiries.

Detailed information regarding our audit objectives, scope, and methodology is contained in Appendix I.

FINDINGS AND RECOMMENDATIONS

I. DATA ACCURACY AND TIMELINESS

Our prior audit in June 2005 found that the TSC was operating two vastly different versions of the TSDB and the TSC lacked sufficient internal controls to ensure the integrity of the databases, resulting in names excluded from the watchlist and inaccurate and incomplete records. In our current review, we found that the TSC was operating two versions of the TSDB in tandem and the TSC had not taken adequate steps to ensure that the content of the two databases was identical. Further, we found significant numbers of duplicate records. In addition, because of internal FBI watchlisting processes, we found that the FBI bypasses NCTC and the TSC and enters a nomination into a downstream screening system prior to submitting the nomination to NCTC. As a result, the TSC is unable to ensure that consistent, accurate, and complete terrorist information is disseminated to frontline screening agents in a timely manner. Moreover, the TSC had determined that the TSDB contained over 2,000 watchlist records that did not belong in the database. This TSC review also identified at least eight records that were missing from the downstream databases and were therefore not available to frontline screening agents. While we recognize that no process will be perfect, omissions of a terrorist identity, as well as the existence of inaccurate, incomplete, or outdated watchlist records can have significant ramifications. Our findings indicate that the TSC needs to further improve its controls over the TSDB to help ensure the integrity and effectiveness of the watchlist.

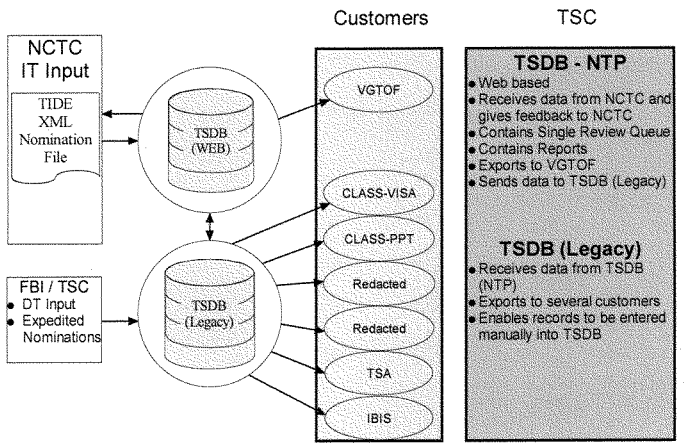
Structure of the TSDB

In concert with NCTC's implementation of its Terrorist Identities Datamart Environment (TIDE) database, the TSC developed a web-based version of the TSDB called the Nomination Tracking Processor (TSDB NTP) in March 2005. As shown in Exhibit 2-1, the TSDB NTP facilitates the receipt of data from NCTC, provides direct connectivity to the NCIC VGTOF data system, and enables the initiation and monitoring of data quality assurance efforts of the TSC.[30] However, the TSDB NTP system is unable to export watchlist data to most screening agencies or process expedited and domestic

[30] Direct connectivity to the NCIC VGTOF system and quality assurance functionality were established in May 2005 and March 2006, respectively.

terrorist nominations into the TSDB. As a result, the TSC has retained a legacy version of the TSDB to accommodate these processes.[31] These two versions of the TSDB are interconnected to help ensure that nominations are properly exported to downstream watchlist agencies.

EXHIBIT 2-1
TSDB Operating Environment



Source: The Terrorist Screening Center

TSC officials stated that while this operating environment is not optimal, they needed to maintain the legacy version of the TSDB because the TSDB NTP is unable to process expedited nominations or connect electronically with all of the related downstream screening databases. With two versions of the TSDB, however, it is critical that the TSC maintain strong controls to ensure that each name nominated for inclusion in the TSDB NTP is appropriately included in the legacy version and accurately marked for export to the relevant downstream supporting systems in a timely manner.

However, we determined that the TSC did not implement the necessary controls to ensure that both databases contained a complete and accurate version of the terrorist watchlist. Specifically, the NTP and legacy databases were not synchronized, which caused inconsistent record counts between the two systems. As a result, names were omitted from the downstream screening databases. In addition, we noted that records had

[31] In June 2004, the TSC upgraded its original watchlist, which facilitated the electronic exchange of data with participating agencies' systems.

been inappropriately maintained in the TSDB without any watchlist designation. These findings are discussed in detail below.

Inconsistent Record Counts

At the beginning of this audit, we were informed by the TSC Chief Information Officer (CIO) that the NTP and legacy versions of the TSDB were interconnected to help ensure that the watchlist was properly exported to frontline screening agencies. Therefore, the two databases should be identical in content and should contain the same number of records. However, on March 16, 2007, we found that the TSDB legacy database had 689,631 records while the NTP had 689,613 records – a difference of 18 records. Although the difference is a small portion of the universe of records, omitted records can result in a missed opportunity to identify a known or suspected terrorist.

We brought the record discrepancy to the attention of the TSC CIO, who said he was surprised to learn that the systems were not in balance. Upon further review, the CIO learned and reported to us that the IT staff at the TSC was aware that the record counts sometimes varied. Despite the increased risk created by continual transactions between the two databases as well as recent system modifications, the TSC IT staff did not appear to have examined the differences, researched a valid explanation for the discrepancies, or sought a correction for whatever condition was causing the record counts to be out of balance.

Through subsequent analysis, on March 26, 2007, the TSC determined that the record difference between the two databases had increased to 38 records – 5 records were missing from the TSDB legacy system while at the same time it contained an additional 33 records that were not in the TSDB NTP system. These omissions and inaccuracies resulted from problems in a number of different areas.

Records Missing from the TSDB Legacy Database

Because the TSDB legacy database facilitates the export of data to downstream screening databases, any information that is missing from the system is not made available to all appropriate law enforcement and intelligence officials for screening of persons against the watchlist. As a result of our review, the TSC identified five records that were missing from the TSDB legacy system, which caused the exported watchlist to be incomplete.

- One record, nominated on December 22, 2006, was never transmitted from the TSDB NTP system. As a result, this known

or suspected terrorist record was not watchlisted for over 3 months. TSC officials were unable to determine why the record was not sent. However, as a result of our review, the TSC subsequently added this record to the watchlist.

- Three records nominated on March 5, 2007, were transmitted by the TSDB NTP system but were never imported into the TSDB legacy system. According to TSC officials, the import process for the file containing these records was interrupted. The individual processing the file should have received a notification that the process failed. However, because multiple files are processed each day, TSC officials could not readily identify who processed the file nor provide an explanation as to why corrective action had not been taken. The TSC CIO stated that as a result of our review, the TSC has taken corrective action by modifying the software so that if the transfer process is interrupted again and the user restarts the program, the application returns to the last successfully imported identity and restarts the process to ensure that no records are lost by the interruption.

- On December 20, 2006, the NTP system appropriately processed a request for the deletion of one record. However, the record was not deleted from the TSDB legacy system at the same time. As a result, this name continued to be inappropriately exported to downstream screening databases for nearly 2 months. On February 6, 2007, the individual was re-nominated by NCTC through the TSDB NTP, resulting in the two systems being synchronized for this record. On February 21, 2007, the original request for deletion was inappropriately processed in the TSDB legacy system resulting in the name not being watchlisted for approximately 1 month until we brought it to the TSC's attention in early March 2007.

  TSC officials explained that earlier versions of the TSDB legacy database could not process multiple actions for a single record, such as both a modification and a deletion, within one daily import file. TSC officials also theorized that for this record it appears that the December 20, 2006, file contained both a modification and a deletion. Because the TSDB legacy system processed the modification first, the deletion did not process, remained within the queue, and was processed 2 months after it was submitted. TSC officials stated that they have modified the processing order of the queue to prevent this anomaly from occurring again.

Additional Records in the TSDB Legacy Database

As a result of our review, the TSC identified 33 additional records contained within the TSDB legacy system that were omitted from the TSDB NTP system. According to TSC officials, the errors associated with each of the 33 records resulted from deficient historical data and technological complications.[32] TSC officials agreed that none of the records should have been included in either database. TSC officials stated that they have now ensured that these records have been submitted to the internal quality assurance unit for corrective action.

Inaccurate Display of Watchlist Designation

The State Department's Consular Lookout and Support System (CLASS) is one of the downstream screening systems that receives watchlist information from the TSDB. CLASS consists of two modules – CLASS/Visa and CLASS/Passport, which are used for processing visa and passport applications. According to State Department policies, individuals who are designated as a U.S. citizen or a U.S. person are ineligible for inclusion in the CLASS/Visa module.[33] Non-U.S. persons are eligible for inclusion in both CLASS/Visa and CLASS/Passport. Therefore, an individual's TSDB record can be exported to CLASS/Visa, CLASS/Passport, or both data systems based upon their status as a non-U.S. person. The TSC has included these criteria in the TSDB legacy software to ensure that watchlist records are correctly nominated and exported to the appropriate CLASS module during the data transfer process.

TSC users viewing the TSDB NTP system see check boxes that clearly identify the downstream screening systems to which each record is disseminated. However, the series of check boxes includes only one CLASS box that does not delineate between CLASS/Visa and CLASS/Passport and has the generic label "CLASS."

The TSC plans to correct the CLASS designation in the TSDB NTP system to appropriately reflect that U.S. persons are not eligible for export to CLASS/Visa. In addition, as part of its planned system upgrades, the TSC

---

[32] Many of these deficiencies are attributable to data inconsistencies and inaccuracies that resulted from the TSC's immediate need during its earliest days to develop a comprehensive database of known or suspected terrorists.

[33] According to TSC standard operating procedures, a U.S. person is defined as either: (1) a citizen of the United States; (2) an alien lawfully admitted for permanent residence; (3) an unincorporated association with a substantial number of members who are U.S. citizens or are aliens lawfully admitted for permanent residence; or (4) a corporation that is incorporated in the United States.

intends to modify the TSDB NTP to accommodate designations for both CLASS/Visa and CLASS/Passport. This will help ensure that once the TSC begins to use the NTP system to export watchlist records to the downstream databases, the appropriate records are sent to each of the CLASS modules and individuals are watchlisted in the correct systems.

Future of the TSDB

We were told by TSC officials that they intend to streamline the TSDB by incorporating the functionality of the legacy system into the TSDB NTP and eliminating the legacy version. To minimize the impact on operations, the TSC plans to implement the changes in an incremental and phased approach. TSC officials anticipate that the project will be completed by the end of calendar year 2007.

It is essential that the TSC maintain and distribute to frontline screening agents a complete subset of known or suspected terrorist identity information. Therefore, the TSC should work aggressively to implement its plan to consolidate the TSDB NTP and legacy systems. Further, we believe that for as long as the TSC must maintain its current operating environment, the TSC must closely monitor the content of each to ensure that the record counts agree and that all watchlist records are accounted for and disseminated as appropriate. As a result of our audit, the TSC CIO stated that he had implemented a policy whereby the contents of the two systems are reconciled manually on a daily basis.

Records Not Designated for Any Watchlisting

According to its governing MOU, the TSC is responsible for regularly reviewing the contents of the TSDB and promptly adjusting or deleting outdated information. During the course of our review, we were informed by TSC officials that in September 2006 they had identified 2,682 records that were not being exported to any downstream screening database. Working with NCTC, the TSC confirmed that 2,118 of these records did not belong in the TSDB and needed to be removed from the consolidated watchlist.[34] TSC officials conducted a manual review of the remaining 564 records and determined that 8 had not been appropriately watchlisted and needed to be renominated to the TSDB.[35]

---

[34] On April 27, 2007, the TSC implemented an information technology solution to delete these records.

[35] The TSC determined that the 564 records represented 443 unique identities. As of June 15, 2007, the TSC had resolved 413 of the 443 records.

Despite being responsible for removing outdated or obsolete data from the TSDB, however, the TSC did not have a process for regularly reviewing the contents of the TSDB to ensure that the database does not include records that do not belong on the watchlist. TSC officials told us that they intend to begin performing a periodic review of the database to identify any records that are being stored in the TSDB that are not being exported to any downstream systems. We believe it is essential that the TSC regularly review the TSDB to ensure that all outdated information is removed, as well as to affirm that all records are appropriately watchlisted.

FBI Procedure for Processing Watchlist Data

The FBI's Terrorist Review and Examination Unit (TREX) receives requests from FBI agents to include individuals with known or suspected ties to terrorism on the terrorist watchlist. These requests are provided on nomination forms, which are also used to modify previous submissions or remove records from the watchlist. Analysts at TREX review the nomination information for accuracy and completeness. Once verified, nomination forms for known or suspected *domestic* terrorists are electronically forwarded to the TSC where a TSC analyst manually enters the information into the TSDB. This information is electronically distributed to the downstream screening agency data systems, including the FBI VGTOF, part of the NCIC system.

By contrast, once the TREX analyst verifies an FBI-generated *international* terrorist nomination, the analyst enters the information into VGTOF directly and then submits the nomination form to NCTC. Following its review and vetting, the NCTC analyst manually enters the information into its database – TIDE – that in turn feeds the information to the TSDB. Because TREX has already entered the record into VGTOF, it is not necessary for the TSC to export the record it receives from TIDE to VGTOF. Therefore, these records are not exported from the TSDB to VGTOF.[36] Because these VGTOF records will not receive electronic modifications or deletions from the TSDB, the TSC and TREX have agreed that TREX will be responsible for ensuring FBI-originated international watchlist records in VGTOF are accurate, complete, and current.

The FBI's direct entry of international terrorist watchlist nomination data into a downstream screening database bypasses NCTC and the TSC and makes it difficult for these agencies to carry out their responsibilities related to watchlist nominations and records. In our opinion, this process

[36] To alert the TSC of this non-standard entry of records into the TSDB, the TSC implemented a special flag, referred to as "FBI sole source," for FBI-originated international records. This designation precludes all future electronic transactions, including related modifications and deletions, from being exported from the TSDB to VGTOF.

does not comport with the nomination and data flow procedures outlined in the MOU and agreed to by the partner agencies, which requires agencies to provide directly to NCTC, rather than directly into a downstream database, information related to known or suspected international terrorists. Additionally, we believe the FBI's practice is cumbersome for the TSC and creates unnecessary data errors, anomalies, and inconsistencies as described below.

To test for data accuracy and consistency, we reviewed a judgmental sample of 50 FBI-originated additions or modifications to the watchlist.[37] We found that while the records for the domestic terrorist nominations were generally accurate, the international terrorist nominations were not. We identified 16 records with 28 instances in which the identifying information related to international terrorists was inconsistent between the nomination form, VGTOF, TIDE, TSDB, or other screening systems. According to TSC personnel, TREX analysts frequently augment the data on the nomination forms with information they glean from FBI case files and enter this additional information into the VGTOF system. However, this supplemental case information is not forwarded to NCTC and as a result the information is not included in TIDE, not sent to the TSDB, and not made available, if appropriate, to downstream screening systems. Further, because TREX enters the record into VGTOF before the addition of any other existing information from other government databases to which NCTC has access, this additional information is often not included in VGTOF. As a result, vital information on watchlist subjects is not being shared with all appropriate screening agencies.

In addition, we found that the FBI's procedures for processing international terrorist watchlist nominations are cumbersome for the TSC and can inadvertently create an incomplete watchlist. The difference in procedures between the FBI's and other agencies' watchlist nominations requires TSC analysts to review every incoming international terrorist nomination and indicate within the record whether it is an FBI source record. If a terrorist watchlist record is improperly designated as an FBI source record, the subset of terrorist watchlist records in VGTOF will be incomplete because that record will not be exported to or modified within VGTOF. TSC staff told us that they were also concerned about this because, when reviewing nominations from NCTC, it is often difficult to distinguish between FBI source records and nominations received from other agencies. TSC staff stated that there was a period of time (possibly as long as a year) in which many records had been improperly designated as an FBI-originated

[37] The total sample of 50 records consisted of 25 each for domestic and internationally known or suspected terrorists.

record or not. In March 2007, the TSC and NCTC addressed this problem by developing a method to permit TSC analysts to more easily identify FBI source records.

In response to these concerns, FBI officials informed us that they had implemented nomination procedures to ensure that FBI international terrorist information was entered into VGTOF in the most efficient manner. Yet, our review of 70 FBI record transactions (50 nominations previously mentioned and 20 deletions) revealed that although the transactions were entered into VGTOF in a timely manner, the transactions were not incorporated in the TSDB in a timely fashion.[38] Specifically, 18 of the 70 transactions took more than 5 days for TREX to process, with 1 transaction taking 35 days. In addition, we identified 2 instances in which TREX erroneously delivered nomination forms for domestic terrorists to NCTC that resulted in delays of 6 and 16 days, respectively.

Delays in including terrorist information in the consolidated database present a significant vulnerability to the integrity of the consolidated watchlist. Further, the FBI's current practice of bypassing NCTC and the TSC and entering international terrorist-related data directly into VGTOF increases the likelihood that watchlist information within the TSDB, TIDE, VGTOF, and other downstream databases is inaccurate and incomplete. As a result, we recommend that the FBI, NCTC, and TSC work together to design a more consistent and reliable process by which FBI-originated international terrorist information is provided to NCTC for inclusion in TIDE and disseminated to the TSDB and downstream screening systems, including VGTOF.

Duplicate Records

As shown in Exhibit 2-2, the TIDE and TSDB systems store all information known about an individual in a single "identity" record using five core identifying fields, including [SENSITIVE INFORMATION REDACTED]. However, the downstream screening agency data systems do not store information at the identity level. Rather, the identity information is split into separate watchlist records to reflect unique combinations of the five core fields.

[38] Officials from NCTC, the TSC, and TREX stated that each agency attempts to process nominations to the watchlist within 1 day.

EXHIBIT 2-2
Record Overview

[SENSITIVE INFORMATION REDACTED]

Source: The Terrorist Screening Center

Multiple records containing the same unique combination of identifying information can increase the number of records that a call screener must review when researching a specific individual. In addition, when multiple records for a single identity exist, it is essential that identifying information and handling instructions be consistent. Otherwise, the screener may mistakenly rely on one record while a second, more complete or accurate record may be ignored. This can result in important information being missed. Further, inconsistent handling instructions may pose a safety risk for law enforcement officers.

In our June 2005 report, we identified 31 instances in which 5 core identifying fields were the same and recommended that the TSC implement corrective action to address the duplicate records and develop an ongoing process to review the TSDB for duplicate records.

In our current audit, we identified a significant increase in duplicated records – 2,533 repeated combinations in these 5 fields involving over 6,262 watchlist records. For example, one unique combination of the 5 core fields had 19 associated records.

In response to the apparent duplicates we identified, TSC officials explained that the duplicates were the result of multiple TIDE identity records for a single individual, system-generated duplicate records, and

improperly processed expedited nominations. TSC officials stated that, while they did not have an ongoing process by which they reviewed the TSDB for duplicate records, as a result of our finding the TSC will review the TSDB on a weekly basis for duplicate records. The results will be forwarded to the TSC's internal quality assurance unit for further review and action.

Multiple Identity Records for the Same Individual

Of the 2,533 instances in which the core identifying fields were the same, TSC stated that most were not necessarily duplicate records. Rather, because the records have different TIDE record numbers, the TSC was unable to independently determine whether these records were duplicates. TSC officials explained that NCTC has indicated to them that many of these occurrences are inherent to old data. For example, prior to the implementation of HSPD-6 in 2003, both the FBI and the State Department may have maintained information regarding a single terrorist identity. During the blending of all sources of international terrorist information, both records may have been included in the TIDE data system resulting in duplicated data. In addition, TSC officials explained that some terrorist information remained classified and, as a result, could not be linked to unclassified data.[39] To ensure that the most complete subset of unclassified information was disseminated, NCTC created multiple identity records for some individually known or suspected terrorists. As a result, rather than the optimal one identity record with multiple watchlist records, some individuals have multiple identity records that contain multiple identical watchlist records.

Through additional data analysis of the duplicate records we identified, the TSC identified at least one instance in which both the FBI and another government agency nominated the same individual. Because both records pertain to the same individual, the identifying information and instructions for handling the subject should be consistent. However, we identified significant differences in the handling instructions and warnings for the individual. Specifically, one record indicated that the individual was "armed and dangerous with violent tendencies" and also had a valid federal arrest warrant. The other record did not contain this information. Moreover, our analysis of the instances in which the five identifying fields were the same indicates that at least 20 percent have some discrepancy in handling instruction, identifying information, or watchlist export designation. These

[39] By August 2004, the Attorney General, the Director of Central Intelligence, and the Secretaries of Homeland Security, State, Treasury, and Defense signed Addendum A to the original governing MOU. Addendum A contained provisions for the declassification and sharing of terrorist information, including [SENSITIVE INFORMATION REDACTED]. However, the provisions only covered information obtained after August 2004.

descriptions and instructions are used by frontline law enforcement personnel to assess and determine the level of threat posed by the individual encountered and help to protect themselves and others. Therefore, it is essential that this information be accurate and consistently applied to all records related to one individual.

Because these multiple records occur in TIDE, the TSC believes the review of the 2,533 possible duplicates more appropriately falls to NCTC. In June 2006, NCTC implemented an Identity and Person Merge project. Through this project, NCTC intends to resolve the duplication of identity data across multiple TIDE identity record numbers. However, until the identity information is consolidated, NCTC analysts should apply new information for an existing individual to each TIDE identity record for the individual. Through this process, NCTC intends to ensure that users of TIDE do not miss information about an individual that is potentially relevant to their work because they viewed the "wrong" TIDE identity when conducting their analysis. NCTC and the TSC anticipate that NCTC initiatives will help to alleviate many of these multiple identity records. However, until corrected we believe that these multiple records can affect a screening agent's ability to protect against terrorism and can also pose significant risks to the safety of frontline law enforcement officers.

System-Generated Duplicates

According to TSC officials, the TSDB should not contain multiple watchlist records for a single identity from TIDE with identical information in the five core identifying fields. We determined that the TSDB contained one TIDE identity with two associated watchlist records with duplicated identifying information. The TSC determined that these two records resulted from a nomination from NCTC in February 2005 in which the two records were either improperly included in the daily import file or an error occurred during the import process on that day. Based on our review, the TSC submitted this record to its internal quality assurance unit, and the duplicate record was deleted.

Expedited Nominations

When the TSC is informed about an individual who poses an imminent threat, it creates an "expedited" watchlist record directly into the TSDB. The TSC then forwards all of the information gathered on the subject to NCTC or the FBI for subsequent creation of a record through the standard nomination process. Once the record is submitted through the standard processes, the original expedited record should be deleted. However, our review of the duplicate record issue identified three expedited records that had been

improperly processed and not deleted from the TSDB after the record was submitted through the standard nomination process.

According to TSC officials, these duplicated records (the expedited and subsequent routine nomination) should contain identical information. Our analysis revealed two instances in which either an additional date of birth or passport number was missing. According to the TSC CIO, these three expedited nominations have been submitted to the TSC's internal quality assurance unit for further review, and the duplicated records have been deleted.

Inclusion of Known Terrorists in the TSDB

We also performed limited testing on the TSDB to examine the completeness of the watchlist by determining if known terrorists were included in the consolidated database. We selected for our review a total of 49 names: 10 from NCTC, 4 from news media accounts, 17 from the FBI's Most Wanted list, 16 from the State Department's List of Terrorists under Executive Order 13224, and 2 from the Rewards for Justice website.[40] We searched the TSDB for these 49 names, and found that each was recorded in the TSDB. TSC officials also said they regularly checked their database against names reported in the news, broadcast on television, or included on lists such as the FBI's Most Wanted.

However, our review of the 49 known terrorist names also revealed that the handling instructions for individuals from the FBI's Most Wanted list had significant discrepancies. Specifically, two VGTOF records indicated that the watchlist subjects were armed and dangerous, but the TSDB records did not reflect this handling instruction. In addition, we identified four records containing discrepancies in identifying information between TIDE and TSDB. As previously discussed, it is essential that the TSC ensure that individuals are properly and consistently recorded in the TSDB and downstream screening systems, so that appropriate actions are taken if the individual is encountered by a frontline screening agent.

Conclusion

It is critical that the TSC ensure that the TSDB contains comprehensive information and that each watchlist record is appropriately disseminated to downstream screening systems in a timely manner. While we recognize that

---

[40] The State Department maintains a list of the most wanted terrorist organizations and individuals as specified by Executive Order 13224. The Rewards for Justice website is an organization operated by the FBI, CIA, DOJ, and the State Department.

no process will be perfect, the potential effect of omissions of a terrorist identity, or the existence of an inaccurate, incomplete, or obsolete watchlist record, requires the TSC and its partner agencies to take all available actions to minimize such errors.

Despite our identification in our June 2005 audit of deficiencies related to the TSC's information technology management and overall database reliability, our current audit determined that the TSC has not yet implemented routine processes to ensure that the TSDB contained all proper watchlist nominations and did not contain duplicate data resulting from improperly processed records, system malfunctions, and historical data deficiencies. Moreover, despite being responsible for removing outdated or obsolete data from the TSDB, the TSC did not have a process for regularly reviewing and verifying the contents of the TSDB. We believe that it is essential that the TSC regularly review the TSDB to ensure that all obsolete and out-of-date information is removed. Finally, because of internal FBI watchlisting processes, the TSC cannot ensure that accurate and complete terrorist information has been disseminated to downstream screening systems in a timely manner.

Recommendations

We recommend that the TSC:

1. Implement its plan to consolidate the TSDB NTP and legacy databases in a timely manner. In the interim while the two systems coexist, the TSC should establish a formal procedure to regularly review the TSDB NTP and legacy databases to ensure that the information in these systems remains synchronized.

2. Develop procedures to regularly review and test the information contained in the TSDB to ensure the data is complete, accurate, and non-duplicative.

3. Modify the TSDB NTP to accommodate designations for both CLASS/Visa and CLASS/Passport. In addition, the TSC should review and correct the records identified in the TSDB NTP to appropriately reflect that U.S. persons are not eligible for export to CLASS/Visa.

4. Review and correct the records identified in the TSDB NTP to ensure that the IBIS handling instructions are appropriately applied.

5. Develop procedures to regularly review the information in the TSDB to ensure that outdated or obsolete data is removed in a timely manner.

We recommend that the FBI:

6. Working with the TSC, revise the watchlist nomination process to provide international terrorist nominations directly to NCTC for inclusion in TIDE, submission to the TSC, and dissemination to all downstream databases, including VGTOF.

II. QUALITY ASSURANCE

Our review indicated that the TSC had the foundations of a sound quality assurance plan that will improve the accuracy of the TSDB. The TSC is also continuing its efforts to perform a record-by-record review of the TSDB. However, we are concerned the TSC has not instituted adequate internal controls to ensure that its quality control initiatives are properly implemented. In addition, the TSC's quality assurance efforts have been hampered by the growth in workload as the size of the watchlist increases.

To test the quality assurance plan, we reviewed 120 TSDB records that had been through the TSC's quality assurance process in FYs 2006 and 2007 and identified several instances in which the individual was not appropriately watchlisted, as well as inconsistencies between the TSDB record and other available information. These inconsistencies make it more difficult for screening agents to determine if encountered individuals are on the watchlist.

Overview of the TSC's Quality Assurance Process

In our June 2005 audit report, we identified weaknesses in the completeness and accuracy of the TSDB. During the TSC's earliest days, it had 12 staff assigned responsibility for nominations and data integrity tasks, including one staff member that was dedicated solely to quality assurance matters. During our initial audit, TSC management acknowledged that the organization needed to focus more attention on ensuring the quality of the watchlist. We recommended that the TSC regularly review and test the information contained in the TSDB to ensure data is complete, accurate, and non-duplicative. We also recommended that the TSC coordinate with participating agencies and establish procedures to identify and resolve missing and conflicting record information.

In response to our recommendations, the TSC increased its quality assurance efforts and implemented a data quality improvement plan that detailed the TSC's intent to conduct a record-by-record review of the TSDB. As of March 2007, the TSC had 34 staff on-board in its Nominations and Data Integrity Unit (NDIU), which is responsible for performing or overseeing

all of the TSC's activities related to ensuring the quality and accuracy of the watchlist, including:[41]

- Reviewing incoming watchlist data (referred to as the single review queue).
- Performing reviews of historical records following an encounter where the TSC identifies a potential discrepancy in watchlist records.
- Conducting special quality assurance projects, such as performing a targeted review of the No Fly list or individuals with particular handling codes.

Single Review Queue

Implemented in March 2006, the single review queue is a feature of the TSDB that segregates the incoming data feed from NCTC so that quality assurance analysts can test each record before releasing that record for inclusion in the TSDB. Prior to the implementation of the single review queue, each watchlist addition or modification the TSC received underwent numerous, separate reviews by individual subject matter experts (persons who were knowledgeable about the requirements of the specific databases used by various screening agencies). In implementing the single review queue, the TSC sought to make the nomination acceptance and review process more efficient. The single review queue was designed to have individual analysts in the NDIU be responsible for guiding individual records through the process of loading the information into the TSDB. The single review queue begins with the use of a computer program that analyzes incoming records against more than 45 business rules.[42] A business rule is an automated information technology function in which the record is analyzed for specific deficiencies and compliance with criteria.

Once the business rules have been applied to all of the records received, the records are routed to the NDIU for manual review. Although the TSC has drafted a standard operating procedure (SOP) describing the single review queue process, it does not detail how NDIU analysts should conduct this manual record review. We observed NDIU analysts reviewing records in the single review queue and found that, in general, the review

---

[41] The NDIU's 34 staff included 7 individuals whose primary duty was to function as a subject matter expert. The remaining 27 staff members were assigned to specific quality assurance tasks and assisted with other quality assurance efforts as necessary.

[42] The TSC also uses 55 business rules to ensure watchlist criteria are met in exporting records to downstream databases.

included: (1) determining whether the person met the criteria for inclusion in the TSDB (i.e., nexus to terrorism and quantity of identifying information); (2) confirming the supporting downstream screening systems to which the record should be exported; (3) resolving any issues identified during the execution of the business rules; and (4) comparing information contained in watchlist nominations, such as [SENSITIVE INFORMATION REDACTED], to source documents and source databases. The NDIU has seven individuals serving as subject matter experts who are consulted when NDIU analysts are unable to resolve all issues related to watchlist nominations prior to these nominations being sent to downstream screening databases. Generally, each record is reviewed by fewer persons than before the implementation of the single review queue. As of March 2007, 10 of the 34 staff members in the NDIU were dedicated to the single review queue.

Encounter-Driven Quality Assurance Reviews

In addition to data integrity work that is performed when new or modified data is processed through the single review queue, the NDIU receives referrals from the TSC Call Center for data checks on specific TSDB records. If a call center operator identifies a potential discrepancy in a watchlist record or obtains additional data relevant to a watchlist subject, the operator alerts the NDIU to perform a quality assurance review of the record. Generally, this occurs following a frontline screening agency's encounter with a watchlist subject.

In April 2005, TSC management began requiring call center operators to perform limited data quality tests while handling encounters. Because the operators have access to all of the databases that interact with the TSDB, they were in a position to point out inconsistencies in the information contained in the records on specific individuals in the various databases. This process was modified slightly in November 2006 when the TSDB was upgraded to incorporate quality assurance activities. As a result of the upgrade, individual watchlist records in the TSDB now contain a record (referred to as a QA ticket) in which TSC staff can record all quality assurance work that has been performed on that record.[43] With the upgrade, call center screeners were instructed to create a QA ticket in the

[43] Prior to the November 2006 TSDB upgrade, NDIU analysts first used an electronic spreadsheet and then a database commonly referred to as the "quality assurance tracker" to monitor quality assurance matters. NDIU analysts continued to use the quality assurance tracker for matters requiring classified correspondence because classified information cannot be placed into the QA ticket, which is housed within the TSDB – an unclassified system. In April 2007, the quality assurance tracker program was discontinued due to a number of concerns; the concerns and the TSC's interim solution for recording classified quality assurance matters are discussed on page 39.

TSDB for each positive screening encounter for which they identified any erroneous or inconsistent information in the database records.[44] In addition, the call screeners were told to create a QA ticket if they obtained new information that should be added to the watchlist records.[45]

When a call center operator prepares a QA ticket, the TSDB electronically routes the QA ticket to the NDIU for further action. An encounter-driven QA ticket indicates that the encounter revealed that information needs to be added or modified, or it will indicate that a call screener identified a discrepancy with the completeness and accuracy of the records. Upon receipt of QA tickets, dedicated NDIU staff review the information from the call center screener and perform a full quality assurance review of all affected records. The QA ticket is closed when all necessary changes have been communicated to the source agencies and fed back into the TSDB, which then updates the downstream screening databases. As of March 2007, the NDIU had 9 individuals dedicated to responding to QA tickets.[46]

Special Quality Assurance Projects

The TSC also examines historical TSDB records for accuracy and completeness through targeted reviews of specific subsets of the watchlist records. Examples of special projects that the TSC has conducted include a review of TSDB records for individuals on the No Fly list and individuals with particular handling codes. As of March 2007, the TSC assigned 8 of the 34 NDIU staff to these kinds of special projects.

---

[44] Each encounter is positive, negative, or inconclusive. A negative encounter occurs when a screening agency contacts the TSC because during a screening event an individual is a potential match to a TSDB record, and the TSC (or other law enforcement responder) determines that the individual is not a match to the name on the watchlist. Conversely, a positive encounter is where the individual encountered is a match to the watchlist. An inconclusive encounter occurs when the TSC is unable to determine if the individual encountered is a match to an individual on the watchlist.

[45] Encounters offer law enforcement agents an opportunity to obtain additional information about watchlist subjects. For example, if a watchlist subject is positively identified during an attempted border crossing, the federal agent may obtain previously unknown information, such as a new passport number, eye color, or current address.

[46] These NDIU staff members also address QA tickets generated from TSC quality assurance efforts other than encounter-driven reviews, such as through the single review queue and during ad hoc record quality reviews.

OIG Analysis of TSC Quality Assurance Efforts

To examine the TSC's efforts to ensure the quality of the information in the TSDB, we examined the TSC's review of records in the single review queue and its review of encounters and special projects. In total, we examined 156 TSDB records. Of these 156 records, 36 involved a request for deletion. We determined that each of these records had been appropriately deleted from the consolidated watchlist. Using the remaining sample of 120 records, we performed tests to determine if the watchlist records were accurate. We found that, in general, the TSC's actions to review records as part of a targeted special project successfully ensured the quality of the data, and we identified virtually no errors in the 15 records we tested in connection with special project reviews. In contrast, our examination of 105 records subjected to the single review queue or post-encounter quality assurance reviews revealed that 38 percent of these tested records continued to contain errors or inconsistencies that were not identified through the TSC's quality assurance efforts. Our results are discussed in detail below.

Review of TSC No Fly List Special Project

The first major subset of TSDB records that the TSC began reviewing as a special project was the Transportation Security Administration (TSA) No Fly watchlist records. The No Fly list includes individuals who, in general, are considered a threat to civil aviation and should be prevented from boarding commercial aircraft.[47]

To assist the TSC in its review of the No Fly list, the DHS temporarily assigned 10 federal air marshals to the TSC. The process included a review of the available information for each individual listed on the No Fly list and a determination of whether the individual should remain on the No Fly list. In addition to reviewing each entry on the No Fly list, the TSC performed a concomitant quality assurance review of all information contained in the TSDB's records for individuals on the No Fly list. As a result, all of the TSDB's records associated with individuals who were on the No Fly list underwent a comprehensive quality assurance review.

When the TSC began its review in July 2006, the No Fly list contained 71,872 records. As a result of the review, the TSC identified 22,412 records for removal from the No Fly list and placement on the TSA's Selectee list.[48]

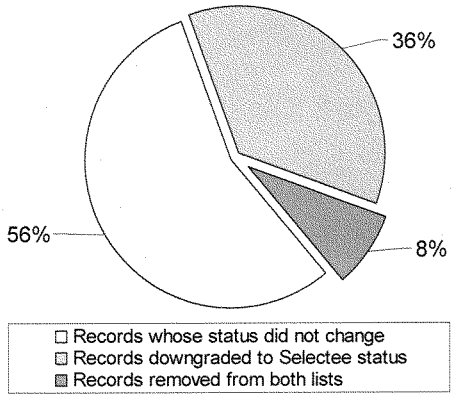
---

[47] [SENSITIVE INFORMATION REDACTED]

[48] [SENSITIVE INFORMATION REDACTED]

For another 5,086 records, the TSC determined that the individual did not require inclusion on either the No Fly or Selectee list. The resulting No Fly list changes the TSC identified are displayed in Exhibit 3-1. As of January 31, 2007, the TSC had determined that the No Fly list should contain 34,230 records.[49]

EXHIBIT 3-1
Results of TSC Review of No Fly List



Source: The Terrorist Screening Center Nominations and Data Integrity Unit

We reviewed a sample of 15 TSDB records that had undergone a quality assurance review as part of the TSC's review of the No Fly list. We did not find any data inaccuracies or inconsistencies in the records we reviewed. Each record's basic information [SENSITIVE INFORMATION REDACTED] were shown consistently in all of the affected databases, and each record remained the same or was downgraded from the No Fly list in accordance with the final recommendation from the NDIU.

We did, however, identify an issue with the implementation of the status changes that the TSC identified during its review of the No Fly list. TSC officials told us that although the No Fly records were reviewed at the TSC, the status changes for known or suspected international terrorists could not be reflected in the TSDB until the changes were processed in TIDE

[49] During its review of the No Fly list, the TSC continued to receive routine No Fly list additions, modifications, and deletions through the watchlist nomination process. As a result, it is not possible to subtract the special project-driven No Fly list changes from the starting point of 71,872 records and obtain the correct number of No Fly records as of January 31, 2007.

at NCTC. The correct watchlisting status could then be uploaded from TIDE to the TSDB during the normal daily data feed. In turn, the TSC would export the No Fly and Selectee lists to the TSA for dissemination to the airlines on a daily basis.

According to TSC officials, NCTC and the airlines told the TSC that they could not effectuate all of the 27,498 changes (22,412 downgrades from the No Fly to the Selectee list plus 5,086 removals from the No Fly list) at once due to resource limitations. TSC management had previously decided not to send any record changes to NCTC until this special project was nearing completion. TSC management explained that TSC analysts needed the time to complete their quality assurance checks for each individual, particularly those with multiple TSDB records. The first changes were sent to NCTC on January 19, 2007. We were told that NCTC and the airlines could only process between 500 and 1,000 record changes a day. As a result, the TSC agreed to limit the number of changes it provided to NCTC and the airlines each day.

This piecemeal approach to implementing the changes in all of the databases meant that the status of many individuals was incorrectly shown on the TSA's No Fly and Selectee lists for a period of time.[50] According to TSC officials, all of the changes had been passed back to NCTC as of March 21, 2007. However, as of May 31, 2007, the TSC and NCTC were in disagreement about the proper No Fly-list status of 108 records.

Review of Routine Quality Assurance Matters

Unlike our review of the No Fly list special project, our examination of records passed through other TSC quality assurance processes revealed that the reviewed records were still likely to contain errors or inconsistencies. We selected a judgmental sample of 105 new and historical TSDB records that had undergone the single review queue or encounter-driven quality assurance processes.[51] We examined the records to ensure that each record was exported to the appropriate screening databases. Additionally, we reviewed the records to determine if basic information [SENSITIVE

---

[50] The period of time for which a record would have been inappropriately watchlisted to the No Fly list could range from a minimum of 1 day to a maximum of about 9 months.

[51] We have consolidated our single review queue and encounter-driven quality assurance sample selection and testing results here for ease of presentation. Although we selected records from different subsets of the TSDB, each had been subjected to the same quality assurance steps in the NDIU, making this consolidation possible. Details of our sample selection and the populations from which we selected them are provided in Appendix I.

INFORMATION REDACTED] was shown consistently in all of the affected databases.

Watchlist Designation and Handling Code Errors

Our review revealed that 7 of the 105 TSDB records examined were not being exported to all appropriate downstream watchlists. Specifically, three records were not exported to CLASS Visa. Moreover, these three records and an additional three records were not exported to [SENSITIVE INFORMATION REDACTED].[52] Additionally, one record was not properly exported to the Interagency Border Inspection System (IBIS).

We discussed these records with NDIU officials who agreed with our findings. As a result of the TSC's failure to export the four records to IBIS or CLASS Visa, which are used by U.S. screening agencies, the watchlisted individuals could be issued a U.S. visa erroneously or inappropriately allowed to enter the United States. The TSC's failure to export the six records to [SENSITIVE INFORMATION REDACTED] can prevent U.S. allies from identifying known or suspected terrorists and sharing additional intelligence.

Our review also revealed that in two instances the TSDB records did not correctly indicate how the record would be seen within the IBIS system. When records are exported from the TSDB to the IBIS system, watchlist records can be identified with a special, less-intrusive handling code, as described earlier. We identified two TSDB records that were exported to IBIS with the special handling designation but should not be because the subjects were considered armed and dangerous or were not deemed a U.S. person. In addition to incorrect IBIS handling designations, an additional three records contained improper VGTOF handling codes. As discussed earlier, VGTOF handling codes instruct law enforcement officers how to properly handle an encounter with a watchlist subject. Incorrect watchlist designations and handling codes can place frontline screeners at increased risk.

Inconsistent or Incomplete Watchlist Records

Our review of the 105 TSDB records submitted to the TSC's single review queue or encounter-driven quality assurance examinations also revealed that 35 TSDB records and the source or downstream records contained inconsistent identifying information in one or more data fields. In total, we identified 54 instances of inconsistent information. Our results are displayed in Exhibit 3-2:

---

[52] [SENSITIVE INFORMATION REDACTED]

EXHIBIT 3-2
TSDB Record Inconsistencies

TSDB Record Field	Inconsistencies[53]
[SENSITIVE INFORMATION REDACTED]	
TOTAL	**54**

Source: OIG analysis of TSDB, TIDE, and VGTOF watchlist records

During our review, it became apparent that both the TSC's quality assurance efforts and our reviews of watchlist records identified errors and inconsistencies in incoming records from the source agencies – NCTC and the FBI. We discussed the watchlist nomination process with NCTC and FBI officials, and both agency representatives stated that records are reviewed for accuracy, completeness, and consistency before the records are forwarded to the TSC. However, these efforts are failing to identify a significant number of deficiencies in the nominated records. The TSC's quality assurance efforts, therefore, are hampered by the inaccurate and incomplete source material.

However, inconsistent records can confuse or delay TSC Call Center operators in their efforts to determine if encountered individuals are a positive match for watchlisted known or suspected terrorists. Further, inconsistent information among databases involved in terrorism screening indicates that at least one record may be incorrect. Incorrect records can also misinform frontline screening agents and contribute to the misidentification and delay of an innocent person or the inappropriate release or admittance of a dangerous individual.

Quality Assurance Management and Oversight

In general, we believe the actions the TSC has taken to improve quality assurance since our last audit are positive steps. We also recognize

[53] Each entry in this column represents a TSDB record for which we determined that the identified TSDB record field was not in agreement with TIDE and VGTOF. (We limited our review to those databases.) It is possible for one record to have more than one error, and the overall total is the number of field errors.

that it is impossible to completely eliminate the potential for errors. However, we identified inaccuracies in the TSDB that persisted even after undergoing the quality assurance process. This underscores the need for additional actions to ensure that the TSDB is a reliable source of information about known or suspected terrorists. Specifically, as described below, we believe that the TSC should: (1) work with the participating agencies to improve coordination related to quality assurance work, including establishing areas of responsibility and timeframes for following up on quality assurance matters; (2) develop a comprehensive standard operating procedure for quality assurance matters; (3) regularly review the NDIU's quality assurance work; (4) develop a reliable and secure method for tracking quality assurance matters that involve classified correspondence; and (5) develop quality assurance benchmarks to monitor the TSC's progress in conducting a record-by-record review of the TSDB.

Coordinating with Participating Agencies

According to TSC personnel, NDIU analysts should follow up on all quality assurance matters every 30 days. However, the TSC does not have a mechanism such as a standardized report or digital dashboard that catalogs all outstanding quality assurance matters.[54] As a result, NDIU analysts are not prompted to follow up on long-outstanding quality assurance matters for which the TSC is waiting for a response from another agency, such as NCTC. Rather, it is up to each individual analyst to take follow-up action.

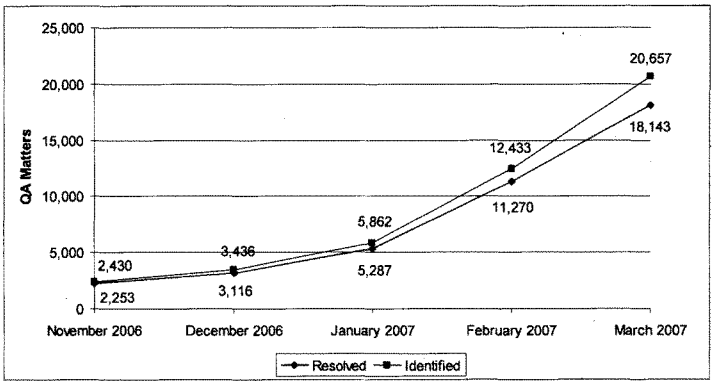
We examined a sample of 51 quality assurance matters opened between February 2006 and February 2007 and found that the matters were open from 0 days (the matter was closed the same day as it was opened) to 329 days. On average, quality assurance matters in our sample were open for 80 days. We also obtained TSC data related to the number of quality assurance matters identified and resolved between November 2006 and March 2007.[55] This data shows that the TSC is identifying incomplete or inaccurate information in TSDB records faster than the matters are being resolved.

---

[54] A digital dashboard is a business management tool to visually display the status of a business project. The dashboard can provide warnings, next steps, action notices, and summaries of a project.

[55] The TSC could provide historical data on quality assurance matters only since November 2006 when the latest version of the TSDB was deployed.

EXHIBIT 3-3
Cumulative Growth in Quality Assurance Matters



Source: The Terrorist Screening Center

Exhibit 3-3 shows that the cumulative difference between quality assurance matters identified and addressed has increased from 177 in November 2006 to 2,514 in March 2007. A significant portion of the increase in quality assurance matters processed by the TSC resulted from its implementation of its No Fly special project in January 2007. However, the TSC is regularly identifying errors or concerns with known or suspected terrorist records. To resolve inaccuracies and inconsistencies in watchlist records, the TSC usually must involve the source agencies – NCTC and the FBI. TSC officials acknowledged that the TSC and the participating agencies have not established timeframes for the resolution of quality assurance matters.

We believe that the TSC needs to work more closely with watchlisting agencies to better coordinate quality assurance efforts. This includes setting a standard for the timeliness of response to quality assurance matters, as well as delineating the roles and responsibilities of the various agencies involved. To improve the overall quality of the watchlist, the TSC needs the source agencies to provide records that are accurate, complete, and consistent, and to respond to quality assurance matters within a reasonable time. Without such an agreement, the TSC must expend additional effort to resolve errors that should have been identified earlier in the nomination process and continue to remind watchlist agencies about individual quality assurance matters.

Further, the delayed closure of quality assurance matters directly affects the accuracy of the consolidated watchlist database because records

can contain inaccurate and incomplete information for extended periods of time while the matter is being resolved. Therefore, in concert with the development of established timeframes for resolving quality assurance matters, we recommend that the TSC develop a tickler system or aging schedule for its quality assurance work.

Standard Quality Assurance Procedures

During our audit, we personally observed NDIU analysts conducting quality assurance reviews of watchlist records. We noted that the analysts' method of performing their reviews was not always consistent. For example, some analysts inspected all of the documents supporting a TSDB record, while other analysts relied solely upon summary information. We also found that the analysts were not documenting their quality assurance work consistently. The TSC has an SOP for its quality assurance efforts which was last revised on August 16, 2005. The document did not provide complete guidance to the analysts on the processing of quality assurance matters. Further, this SOP informs the analysts to review the record, but does not detail what fields, supporting information, and other aspects of the record the analysts should be verifying and comparing. In addition, these procedures do not instruct the analysts on the necessary actions to take when inaccurate or incomplete information is identified. Moreover, this protocol does not mention the existence of special projects within the TSC's quality assurance efforts. We believe that the TSC should develop a detailed, comprehensive quality assurance SOP to better guide the NDIU analysts through all aspects of their work.

NDIU Analyst Oversight

The TSC provides only a few days of training to its quality assurance analysts in the NDIU. Following the completion of that training, the analysts begin working independently and no additional routine training or refresher courses are required. However, staff meetings are held on an ad-hoc basis to discuss specific issues that have been encountered. The TSC does not have a mechanism for regularly spot-checking the work of its quality assurance analysts to help ensure that the analysts are performing appropriate reviews and keeping abreast of any process changes. We believe that the TSC should develop a system for performing regular spot-checks of NDIU analysts' work to identify any weaknesses and needs for additional training. This process should be included within the comprehensive quality assurance SOP.

Handling Classified Quality Assurance Matters

Prior to April 2007, the TSC was using an in-house system called quality assurance tracker to catalog all classified correspondence related to quality assurance matters.[56] However, TSC officials determined that the database: (1) had reached its storage capacity, (2) temporarily lost an estimated 2,000 records in January 2007, (3) did not have a reliable process for backing up the data, (4) did not create any standard management reports, (5) had no method for audit tracking, (6) had not been examined and tested thoroughly by the FBI, and (7) was used by very few staff. Therefore, the TSC shut down the database in April 2007 to prevent any more problems with its use.

The TSC researched several possible long-term methods for tracking classified quality assurance correspondence. As of April 2007, the TSC's temporary method was to use electronic folders on a classified server. We believe that this method will not be an effective method for tracking classified correspondence. In addition, a quality assurance analyst in the NDIU told us that the electronic folder method will be more time-consuming and less useful than tracking their individual correspondence within e-mail accounts and, as a result, some analysts do not plan to use the temporary system. We believe the TSC needs to develop a more effective and user-friendly means for temporary tracking of classified quality assurance correspondence.

---

[56] The TSC cannot place classified information into its QA tickets because this information is stored within the TSDB, which is an unclassified system.

Progress on the TSC's Record-by-Record Review of the TSDB

In responding to our earlier audit, TSC officials reported that they planned to conduct a record-by-record review of all records within the TSDB. In February 2006, TSC officials estimated that this review would not be complete until 2012. At the time of our current audit, the record-by-record review was ongoing through the three-pronged strategy of the NDIU – the single review queue, encounter-driven quality assurance reviews, and special projects. TSC officials told us that they plan to examine the TSDB following the completion of the on-going special projects and determine how many TSDB records have not yet been reviewed. The TSC then plans to review any previously unexamined records in an effort to examine the entire TSDB.

In February 2007, TSC officials told us that since the inception of the single review queue in March 2006 over 670,000 TSDB records had been reviewed and the agency had revised its estimated completion date. TSC officials now project that the record-by-record review will be complete by the end of 2007.

Yet, we believe that the TSC may have overstated the number of records reviewed and is underestimating the amount of time and effort that it will take to complete its review of the entire TSDB. We base these conclusions on the following factors:

- As previously discussed, the TSC's single review queue and encounter-driven quality assurance processes do not sufficiently ensure the quality of the watchlist records. Therefore, the TSC should reconsider records examined in these processes in its count of records reviewed.

- The number of records reviewed is not limited to the review of unique records. Rather, the TSC's quality assurance process allows for one record to be reviewed multiple times: through the single review queue, following each request to modify or delete the record, in accordance with one or more special projects, and subsequent to each encounter. Therefore, we believe that the TSC's cumulative tally of records reviewed can include records counted multiple times.

- Between September 2006 and April 2007, the TSDB grew at an average rate of over 20,000 records per month, or approximately 174,000 additional records during this 8-month period. This growth adds to the analysts' workload. Since

April 2004, the TSDB has more than quadrupled in size, growing from 150,000 to 724,442 records in April 2007.

- In February 2007, there were about 3,000 open quality assurance matters that required follow-up.

We believe that, if the number of records in the TSDB continues to grow at the current rate and the number of quality assurance matters similarly increases, the NDIU will not complete the record-by-record review of the TSDB by the end of 2007 as anticipated. We recommend that the TSC accurately determine the magnitude of the unexamined portion of the TSDB so that agency officials can implement a sound plan for examining those records and develop a realistic completion date for the endeavor. Further, the TSC should establish benchmarks against which it can measure its progress.

TSC Efforts to Enhance Terrorist Watchlisting

Although we identified several actions that the TSC should take to help improve the accuracy and completeness of watchlist records, our audit also revealed a recent TSC initiative that we believe is a noteworthy practice for enhancing watchlist records. Specifically, we noted that the TSC runs a report each week of NCIC hits in VGTOF and compares these hits to positive encounters in its Encounter Management Application (EMA) database to determine if each hit was called into the TSC Call Center. Performing this review offers the TSC an opportunity to educate local law enforcement officers about the importance of the TSC mission and determine if there have been additional known or suspected terrorist encounters of which the TSC was previously unaware. If the encountered individual was a positive identity match to a terrorist watchlist record, then any new information obtained during the encounter should be added into the TSDB record to enrich the record and provide added value to the intelligence community. TSC officials stated that currently they are identifying an average of 40 to 70 encounters each week that are not being called into the TSC. When the TSC identifies a hit that was not called into the call center, this information is relayed to the FBI. In turn, the local FBI field office is asked to follow up with the local law enforcement agency that ran the NCIC check. The FBI field office sends an agent to the local, state, or tribal law enforcement agency to obtain any information about the encounter and to remind the law enforcement agency that they should call all NCIC hits for known or suspected terrorists into the TSC Call Center.

We believe this practice can provide useful information for enriching the watchlist records. However, we noted that although the NCIC hit report

is run on a weekly basis, it is taking an additional 2 weeks to notify the FBI of these encounters. Our concern with the 2-week time lag is that some local, state, and tribal law enforcement personnel will not remember clearly the encounter by the time they are contacted by the FBI, which can result in a missed opportunity to obtain new information. TSC officials told us that they are working with the FBI to expedite this process.

We were also told that other law enforcement agencies do not always follow up with the TSC to inform them about any newly obtained encounter information. Considering that approximately 60 percent of the encounters are identified by the CBP, the TSC should explore methods for performing similar enrichment exercises related to other screening agency encounters.

Conclusion

The TSC has made significant strides in its quality assurance efforts since our last review, including the creation of the NDIU and the development of new quality assurance processes. In addition, the TSC's goal to perform quality assurance testing of all new and historical records in the TSDB is a positive step. However, we believe that more needs to be done to ensure the accuracy of the watchlist records.

The number of quality assurance matters identified by the TSC increased from about 2,500 in November 2006 to over 20,000 in March 2007, with the number of unresolved matters increasing from 177 to 2,514 during this period. Additionally, the overall size of the consolidated terrorist watchlist has quadrupled in size since the TSC's inception, increasing from about 150,000 records in April 2004 to over 700,000 as of April 2007. This growth further adds to the amount of work for the TSC quality assurance staff to ensure the quality of the records in the consolidated watchlist database.

Our review found that the TSC has not developed a detailed plan of action and benchmarks or milestones to accomplish its goal of reviewing every record in the watchlist database. Additionally, we found errors in records that had undergone routine TSC quality assurance reviews, but a higher quality for watchlist records examined in TSC special project reviews.

We also found that the TSC's SOP for quality assurance matters did not provide sufficient guidance for analysts to use in performing their examinations of watchlist records. Further, the TSC's oversight and internal controls over the quality assurance process did not detect the continued existence of significant record errors and omissions. Finally, we believe the

TSC is hampered by the lack of agreements with the nominating and screening agencies. Such agreements could improve the timeliness for resolving quality assurance matters and help ensure that additional information is obtained during encounters with known or suspected terrorists.

Without a standardized process, adequate internal controls, and agreements with source and watchlist agencies, watchlist records may remain inaccurate and incomplete for an unnecessary amount of time. Before the records are corrected or updated, law enforcement agencies may encounter watchlisted individuals. Additionally, inaccurate records can cause screeners to unnecessarily delay or detain individuals misidentified as a known or suspected terrorist.

Recommendations

We recommend that the TSC:

7. Correct the records identified by the OIG containing incorrect watchlist designations, handling code errors, and inaccurate and inconsistent information.

8. Coordinate with NCTC and the FBI to implement an agreement that establishes the areas of responsibility and the timeframes for data quality assurance matters.

9. Develop a comprehensive standard operating procedure that describes the TSC's three-pronged quality assurance strategy and details the methodology to be used in performing quality assurance reviews.

10. Develop a process to perform regular spot-checks of NDIU analysts' work to identify any weaknesses and need for additional training.

11. Develop an improved and user-friendly process for tracking classified correspondence related to quality assurance matters.

12. Develop a tickler system or digital dashboard for all pending quality assurance matters.

13. Develop a comprehensive plan, including benchmarks or milestones, to complete the record-by-record review of the TSDB.

14. Coordinate with other partner agencies to establish a formal process for relevant encounter information to be captured by frontline screening agents and returned to the TSC to update watchlist records.

III. TERRORIST WATCHLIST REDRESS

The TSC has developed comprehensive procedures, has dedicated staff, and coordinates with partner agencies to help ensure that it effectively and efficiently processes complaints from individuals experiencing delays or difficulties due to terrorist watchlist screening. Our review found that the TSC was following its procedures and reaching appropriate resolutions in such redress reviews. TSC redress disposition data indicated that nearly half of the total closed redress reviews resulted in a modification to or removal of a terrorist watchlist record. We believe that the TSC's redress review results provide a further indicator that watchlist data needs continuous monitoring and attention.

We also found that there are excessive delays in closing redress matters. Additionally, we believe that the TSC should use information related to terrorist watchlist identities that are frequently the subject of watchlist encounters to proactively initiate redress reviews before complaints are filed.

Overview of the TSC's Redress Efforts

Persons stopped as a result of watchlist matches may be actual watchlist subjects, individuals misidentified to a terrorist identity, or someone mistakenly included on the watchlist. As a result of the terrorist watchlist screening process, individuals may complain that they were adversely affected and seek relief. Individual government agencies involved in terrorist watchlist screening should have a redress process to effectively resolve the complaint and respond to the complainant. Similarly, the TSC should have reasonable procedures to provide redress for individuals from faulty watchlist identifications.

When we initiated our first TSC audit in 2004, the TSC did not have an established process for handling inquiries related to private individuals who sought watchlist information following their involvement in a screening encounter. In January 2005 the TSC assigned staff to address terrorist watchlist screening complaints and began to develop a strategy for redress matters. In our previous audit report, we recommended that the TSC develop formal procedures for handling redress inquiries. In response, the

TSC formalized its process by implementing an official Redress SOP in July 2005 and a revised version in May 2007.[57]

In brief, individuals who believe they were unnecessarily and adversely affected by watchlist-related screening procedures may file a redress complaint with the agency involved in the event. For example, if an individual is prohibited from boarding a commercial airline flight, the person would contact the TSA to file a redress complaint. If the TSA determines that the event was related to terrorist watchlist screening, the complaint is forwarded to the TSC for review. Once the TSC has completed its examination, it makes any necessary changes to associated watchlist records and forwards its results back to the TSA, which provides feedback to the complainant.

In November 2005, the TSC created a separate Redress Office to process redress matters. As of April 2007, the TSC Redress Office was managed by the Redress Officer and supported by four analysts and one management assistant. TSC officials said they plan to expand the Redress Office to seven analysts.[58] The analysts in this office are responsible for reviewing redress inquiries, corresponding with partner agencies for clarification or additional information, and recommending to the Redress Officer how to dispose of an inquiry. The Redress Officer is responsible for supervising the analysts, reviewing each redress evaluation, facilitating coordination with other agencies, and finalizing the disposition of the redress inquiry.

We believe the TSC has taken a number of other positive steps to address redress matters since our prior audit. For example, the TSC helped to spearhead the creation of a multi-agency agreement addressing watchlist redress. In addition, the TSC has enhanced its own procedures for handling redress matters.

However, in this audit we identified areas in need of continued improvement and further development, such as the timeliness of redress

---

[57] The TSC's revised May 2007 Redress SOP includes more detailed guidance and reflects changes within the TSC, such as technology improvements, organization structure, and staffing. The revised Redress SOP also expanded TSC redress disposition categories and provided more detailed instructions on its redress processing as well as the incorporation of new technology and terminology.

[58] As of April 2007, the TSC allocated six analyst positions to its Redress Office, of which four positions were filled. The TSC reported that it expected to add an additional analyst position for a total of seven.

matter resolution and utilizing encounter information to provide redress without a complaint being submitted. These issues are discussed below.

Multi-agency Redress Agreement

In December 2006, a multi-agency agreement entitled Memorandum of Understanding on Terrorist Watchlist Redress Procedures (Redress MOU) was developed by a working group of representatives from the various agencies involved in terrorist watchlisting and screening. Representatives from the Privacy and Civil Liberties Oversight Board of the Executive Office of the President were also included in the development of the MOU.[59] As of April 2007, the Redress MOU was being circulated for signature by the heads of the TSC, DOJ, DHS, State Department, the Office of the Director of National Intelligence (ODNI), the FBI, the Central Intelligence Agency (CIA), NCTC, the Department of Defense (DOD), and the Department of the Treasury.[60]

The Redress MOU formalizes the responsibilities of each agency in adjudicating redress inquiries. The agreement requires each agency to assign redress responsibilities to a senior official and commit necessary resources to ensure the efficiency of the redress process and compliance with the Redress MOU. The Redress MOU notes that the TSC has ultimate authority on redress decisions related to the terrorist watchlist.[61]

Overview of the Terrorist Watchlist Redress Process

On February 20, 2007, DHS and the State Department implemented the Traveler Redress Inquiry Program (TRIP). This program established a centralized portal for persons to file complaints regarding difficulties experienced at screening points during travel, such as airports, train stations, and border crossings. DHS headquarters officials informed us that TRIP will also help coordinate the resolution of complaints, monitor trends in complaints, and measure redress process efficiencies.

Exhibit 4-1 shows a basic illustration of the U.S. government's process for addressing redress inquiries related to the terrorist watchlist.

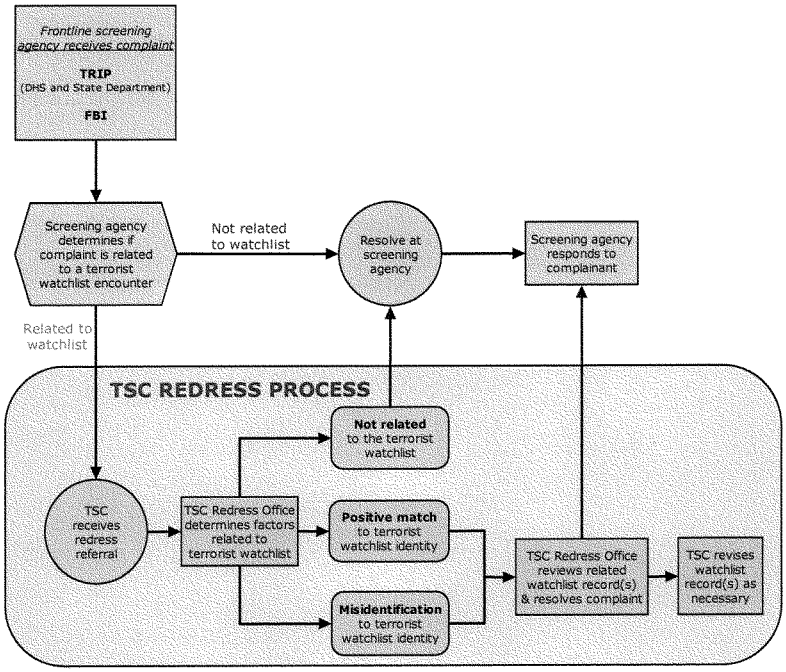
---

[59] The Privacy and Civil Liberties Oversight Board advises the President and other senior executive branch officials on matters with respect to privacy and civil liberties.

[60] The TSC reported that as of April 18, 2007, all agencies had signed the agreement except the DOD, the CIA, and the State Department.

[61] The TSA makes final decisions on No Fly list redress appeal matters.

EXHIBIT 4-1
Flowchart of Terrorist Watchlist Redress Process



Source: The Terrorist Screening Center

Receipt of Redress Complaints

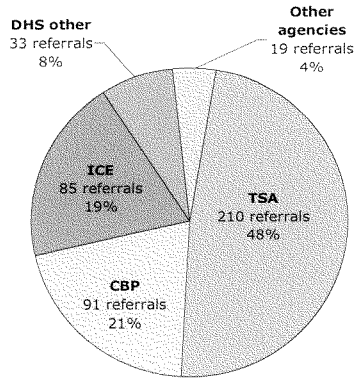
Complainants file redress inquiries with the frontline screening agencies involved in the encounters, such as to the FBI or through TRIP for DHS and the State Department.[62] As shown in Exhibit 4-1, the screening agency reviews the complaint and determines if the inquiry relates to a possible terrorist watchlist match.

[62] The FBI is typically not the agency encountering the individual, but its NCIC system is used in the screening process. Therefore, the FBI is considered the screening agency in such instances.

Individuals can also be affected by screening protocols unrelated to the terrorist watchlist, such as through random search procedures or other security screening practices. Despite someone's actual presence or non-presence on the terrorist watchlist, individuals may assume they have been mistakenly included on the watchlist or misidentified to a terrorist watchlist identity and submit a complaint requesting relief. If the screening agency determines that the complaint is not related to the terrorist watchlist, it should resolve the matter internally and respond to the complainant. For example, an airline may deny a person from boarding an airplane because of drunkenness or disorderly behavior. Complaints related to these types of matters and others unrelated to the terrorist watchlist should not be referred to the TSC.

However, the screening agency should refer to the TSC all redress inquiries determined to pertain to a possible watchlist match. From January 2005 through February 2007, the TSC received 438 such redress referrals. As illustrated in Exhibit 4-2, 96 percent of the redress inquiries referred to the TSC were forwarded by DHS components (CBP, TSA, Immigration and Customs Enforcement (ICE), and other DHS entities). The TSA referred nearly one-half of all redress inquiries received by the TSC. Non-DHS agencies referred a total of 19 redress matters, including the FBI (9 referrals), the State Department (3 referrals), state and local law enforcement agencies (6 referrals), and the Executive Office of the President (1 referral).

EXHIBIT 4-2
TSC Redress Referrals by Referring Agency
(January 2005 through February 2007)



Source: The Terrorist Screening Center Redress Office

TSC Redress Process

When the TSC receives a redress complaint, the TSC Redress Office analyst assigned responsibility for resolving the complaint determines the relationship of the complainant to the terrorist watchlist and places the individual in one of the following three categories: (1) non-related, (2) positive match, and (3) misidentified.

Non-related – The analyst may determine that the complainant does not match a terrorist watchlist identity and was not the subject of an encounter involving a potential match. Essentially, the inquiry should not have been referred to the TSC in the first place. In these cases, the TSC returns this matter to the appropriate screening agency for resolution.

Positive Match – A complainant who matches an identity on the terrorist watchlist and was the subject of at least one watchlist-related encounter is considered a positive terrorist watchlist match. For positive match redress referrals, a Redress Office analyst conducts a complete review of the watchlist records to ensure information on the individual meets the criteria for watchlisting and is accurate, complete, and current. This review will also include contacting the nominating agency to obtain any new information on the individual not yet available to the TSC.

After reviewing this information, the analyst recommends that a record: (1) remain unchanged, (2) be modified, or (3) be removed from the watchlist. If it is determined that the watchlist record is accurate, complete, and current, the analyst then recommends that no changes be made to the record or the watchlist status of the individual.

For some redress inquiries, the analyst recommends a modification to the record. This could entail updating the record with new information or correcting errors in the record. Another recommended revision may include changing the watchlist status of an individual, such as removing a person from the Selectee list or escalating a person's watchlist status from the Selectee list to the No Fly list.

The last disposition scenario for a positive match record involves removing the identity record from the terrorist watchlist altogether. Based on a review of relevant and current information, the analyst may determine that an identity does not meet the criteria for inclusion on the terrorist watchlist.

Misidentification – An individual who is the subject of a terrorist-related screening but whose identity is not on the terrorist watchlist is

considered to have been misidentified. Redress referrals for misidentified complainants are processed by the TSC similarly to positive match referrals. The Redress Office analyst assigned the inquiry reviews the terrorist watchlist record involved in the misidentification and ensures that the record is accurate, complete, and current. The analyst then recommends any necessary changes to the record or watchlist status.

If, as a result of a redress review, the TSC recommends a change to the watchlist record or status (for either a positive match or misidentification referral), the Redress MOU and the TSC Redress SOP both require that the TSC discuss its findings with the nominating agencies. While the nominating agencies may provide input, the TSC has the ultimate authority to resolve all terrorist watchlist redress matters. Finally, the TSC Redress Office ensures that the necessary changes are made to watchlist records before closing its review and alerting the frontline screening agency of its resolution. The TSC does not respond to the complainant. Rather, the TSC coordinates with the frontline screening agency, which should submit a formal reply to the complainant.

The TSC's revised May 2007 Redress SOP includes an expansion of the redress disposition categories. The non-related category was expanded to capture two additional situations: (1) instances in which the TSC administratively closes its review because screening agencies do not comply with TSC redress requirements, and (2) occasions that a redress complaint was considered moot because the terrorist identity to which the redress inquiry refers was already removed from the watchlist through normal watchlist modification or quality assurance procedures. In addition, the TSC renamed its misidentification category to "near match." Lastly, the TSC added one disposition category to use when the TSC Call Center incorrectly identified an individual as a positive watchlist match. The TSC believes its expansion of disposition categories will allow it the ability to better track its redress resolutions and to identify areas in the watchlist process that could be improved. For instance, the Redress Office could find that the TSC Call Center's percentage of incorrect identifications has increased significantly and recommend that a thorough review be conducted.

Disposition of Redress Complaints

The TSC tracks its processing and disposition of redress inquiries in a TSC database. At the time of our review, the database included only those disposition categories used by the TSC prior to the revision of the TSC's Redress SOP. The disposition for the 388 redress inquiries closed by the TSC between January 2005 and February 2007 is shown in Exhibit 4-3.

EXHIBIT 4-3
TSC Redress Complaint Disposition
(January 2005 through February 2007)

Disposition	Number of Complaints	Percentage of Complaints
Misidentification	52	13%
Positive Match (no change)	136	35%
Positive Match (remove record)	76	20%
Positive Match (modify record)	97	25%
Non-related	27	7%
Total	**388**	**100%**

Source: The Terrorist Screening Center Redress Office

Misidentified Complainants

TSC redress complaint disposition data show that 13 percent of the 388 closed redress inquiries were for complainants who were misidentified to a terrorist identity and were not an actual watchlist subject.

According to the TSC, the most common cause of a misidentification is name similarity. As previously discussed, the watchlist is identity-based and relies on name searches in order to vet persons against the watchlist. This can result in a person with an identical or similar name being identified as a terrorist watchlist identity. In many instances the screening agency can use additional identifying information, such as a date of birth or a passport number, to eliminate the individual as a terrorist watchlist match.[63]

Positive Watchlist-Match Complainants

Of the 388 redress complaints reviewed by the TSC between January 2005 and February 2007, 80 percent involved complainants who were on the terrorist watchlist. Through its redress review process, the TSC determined that watchlist records for 35 percent of the closed positive

[63] Screening agencies have also developed programs to assist persons repeatedly misidentified to terrorist watchlist identities. For instance, an individual can voluntarily submit personal-identifying information to the TSA and request to be placed on the TSA Cleared List. If approved for placement on the Cleared List, the individual's name and personal-identifying information can be used to more quickly determine that the individual is not on the No Fly or Selectee lists. Similarly, the CBP and the State Department have implemented procedures to annotate records of misidentified persons in their databases to help avoid future port-of-entry screening and visa application delays. These actions are particularly helpful for a non-watchlist individual with an exact or a very similar name match to a known or suspected terrorist.

watchlist-match redress complaints required no change, 25 percent required some modification to the watchlist records, and 20 percent necessitated removing the complainant's identity from the watchlist.

Therefore, the TSC determined through its review that 45 percent of the watchlist records related to redress complaints were inaccurate, incomplete, not current, or incorrectly included.[64] TSC officials stated that, in some instances, at the same time that a nominating agency was going through the process of having an individual removed from the watchlist, that individual filed a redress complaint. In other instances, the TSC Redress Office found inaccuracies in the watchlist record or discovered additional, relevant information that had not been passed to the TSC.

Specifically, in 76 redress reviews, the TSC determined that the individual should not be watchlisted. In an additional 97 instances, the TSC found that the watchlist record was inaccurate or incomplete. The TSC's redress review results indicate that the watchlist includes individuals that should not be watchlisted and that other records contain deficiencies. These results are further evidence that watchlist data needs continuous monitoring and attention.

At the time of our review, the TSC did not track whether a change to the watchlist record was the result of a TSC redress review or whether the change was coincidental to a concurrent nominating agency submission of information to update the watchlist record. The TSC believes its expanded disposition categories will better account for these scenarios and provide a more accurate picture of redress resolution. The TSC Privacy Officer acknowledged that the high percentage of records requiring modification or removal may point to deficiencies in the terrorist watchlist nomination process and with nominating agencies not providing the TSC additional information important to appropriately update terrorist records.

Timeliness of Processing Redress Complaints

For each redress complaint it receives, the TSC develops a file folder and inputs information into a redress tracking database. The redress file contains information obtained, verified, and developed by the Redress Office. The file contains the Redress Office's review of relevant databases, correspondence with partner agencies, rationale for the resolution of the complaint, and management review.

---

[64] This 45 percent does not include the terrorist records that were modified or removed as part of a redress inquiry by a misidentified individual because the TSC did not specifically track those types of dispositions.

We judgmentally selected 20 redress inquiries the TSC received between January 2006 and February 2007 and reviewed the corresponding redress files to determine if the TSC followed its Redress SOP for resolving a redress complaint. We found the TSC complied with its Redress SOP in all 20 cases, including reviewing the applicable screening and intelligence databases, coordinating with partner agencies, and reaching appropriate resolutions.

We also reviewed TSC redress files and statistics to determine the efficiency of redress reviews. Our analysis of TSC data reveals that it took the TSC, on average, 67 days to close its review of a redress inquiry.[65] For redress matters referred to the TSC during the last semiannual period in our review (July through December 2006), it took the TSC an average of 57 days to finalize its review.

In addition to closed matters, we also analyzed the number of days that pending TSC redress matters had been open. The TSC had a total of 50 open redress inquiries as of February 27, 2007 and the average number of days these matters were open was 61. Of these inquiries, 38 percent were open over 60 days, including 2 inquiries that were pending over 180 days. Exhibit 4-4 details the number of days the 50 redress matters were open as of February 27, 2007.

EXHIBIT 4-4
Open TSC Redress Matters
(as of February 27, 2007)

Number of Days Open	Number of Open Redress Matters	Percentage of Total Open Redress Matters
180 days or more	2	4%
90-179 days	12	24%
60-89 days	5	10%
30-59 days	11	22%
less than 30 days	20	40%
Total	**50**	**100%**

Source: The Terrorist Screening Center Redress Office

Our analysis of closed and open redress matters indicates that it takes, on average, about 2 months for the TSC to finalize its review of a redress inquiry. TSC redress files included copies of e-mails and records of discussion between the TSC Redress Office and nominating agency personnel, as well as an accounting of other significant actions taken by TSC

[65] Redress matters pending as of February 27, 2007, were not included in our analysis of closed redress matters.

analysts to resolve the inquiry. TSC officials stated that each redress review is unique and that more complex cases require a longer review period.

Our review of TSC redress files revealed that long review periods were caused by a variety of factors. In some instances, the TSC took a significant amount of time to finalize its determination before coordinating with other agencies for additional information or comment. A TSC official involved in redress also stated that the Redress Office staffing level sometimes affected the TSC's ability to reach timely determinations. At times, the Redress Office used staff from other TSC units on a collateral, part-time basis. These persons would process redress matters when not performing their primary responsibilities and as time permitted. However, the TSC determined that this collateral assignment method did not provide the most efficient or effective means of resolving redress matters and, as a result, stopped this practice as of April 2007.

Other lengthy redress reviews were affected by nominating agencies not providing timely feedback to the TSC or not efficiently processing watchlist paperwork. The coordination TSC conducts with nominating agencies on redress matters includes corresponding with subject matter experts and case agents for clarification or updated information, requesting necessary watchlist processing documents (such as the FBI's terrorist watchlist nomination and modification form), and resolving differences of opinion between the TSC and nominating agency. For two redress matters, we found that the TSC repeatedly requested the FBI to file necessary paperwork in order to modify the watchlist records, and that it was finally able to close the matters over 140 days after its original requests. Further, we reviewed another redress file showing the FBI closed a preliminary investigation on an individual in November 2005. However, it did not notify the TSC that it determined the individual had no nexus to terrorism and should be removed from the watchlist. The TSC's redress review finally effected the overdue removal of this individual from the watchlist in January 2006.

Additionally, our file review found that certain screening agencies were slow to update their databases with accurate and current information. For instance, the State Department and the CBP did not revise encounter records in the IBIS database in a timely fashion to reflect modified or removed terrorist identities. For example, in one case the CBP did not make a TSC-requested change for more than 130 days.

TSC officials noted that no response timeframes have been established with partner agencies for redress matters. The Redress MOU states that one of the goals of the redress process is to provide for a *timely* review, but

explicit timeframes are not defined. We believe that timeliness measures should be established for resolving terrorist watchlist redress complaints and responding to complainants. The TSC Privacy Officer stated a next step in improving terrorist watchlist-related redress coordination among government agencies is to negotiate timeframes for redress processing. Given the TSC's responsibility for the content of the consolidated terrorist watchlist and its role in developing the Redress MOU, we recommend that the TSC attempt to coordinate timeliness measures for the entire watchlist redress process.

Response to Redress Complainants

The TSC does not respond to complainants filing redress inquiries. Instead, the TSC notifies the frontline screening agency of its disposition decision as it relates to the terrorist watchlist. The frontline screening agency involved in the watchlist-related encounter prompting the complaint is responsible for responding to the complainant. TSC policy dictates that responses to complainants neither confirm nor deny the existence of watchlist records relating to the complainant. This nondisclosure policy exists to protect U.S. counterterrorism operations and intelligence objectives and to safeguard the personnel involved in these sensitive activities. The TSC works with screening agencies such as the TSA in developing appropriate language for responding to complainants.

While the FBI is not the user of the NCIC database during a terrorist watchlist-related encounter involving a state or local law enforcement officer, it is the de facto screening agency in instances involving its NCIC database, and therefore responsible for responding to redress complaints concerning its database.[66] In May 2007, the FBI implemented a watchlist redress policy, identifying its Terrorist Review and Examination Unit (TREX) as responsible for processing the FBI's review of redress matters and for responding to complainants for NCIC-related complaints.[67] However, before it developed this policy, the FBI had not decided how it would respond to complainants, and we found that as of June 2007 it had not responded to a

[66] A typical NCIC-related encounter involves a state or local law enforcement officer conducting a routine traffic stop. The officer searches the subject's identification information (full name and date of birth) through the NCIC system to check for any outstanding warrants on the person. In the event the person is a possible terrorist watchlist identity match, the NCIC system will instruct the officer to contact the TSC to confirm the identity of the individual as an actual watchlist subject and to be instructed on the proper handling procedures for this individual.

[67] As stated earlier, only 4 percent of the redress referrals provided to the TSC from January 2005 through February 2007 were from non-DHS components such as the FBI.

redress complainant on a matter the TSC had closed on February 13, 2007, and had forwarded to the FBI for action.

Appeal of Redress Disposition

If a complainant is not satisfied with the disposition of an initial redress inquiry, the complainant may file an administrative appeal where available by the screening agency. The Redress MOU outlines the responsibilities for each agency in processing an administrative appeal of an original redress inquiry determination. Additionally, the TSC adopted a separate Redress Appeals SOP in November 2006 to expressly describe its administration of an appealed redress decision. The TSA is the only frontline screening agency that has developed its own process for redress appeals.

The TSC Redress Appeals SOP stipulates that a complete analysis of the appeal be performed by the TSC Legal Department, a unit separate from the Redress Office. The TSC prohibits the TSC Redress Office and any personnel involved in the original redress review from direct involvement in the redress appeal process. According to the SOP, the TSC will alert NCTC and the nominating agency that an appeal has been submitted, and it will facilitate necessary communication between the nominating and screening agencies. The final recommendation or decision is determined by the TSC Redress Appeals Board, comprised of TSC Deputy Directors. For an appeal involving a No Fly watchlist status, the TSC recommends a disposition and the TSA has the final decision authority.

As of May 1, 2007, the TSC had received four redress appeals. It resolved two appeals, and these resulted in downgrading the watchlist status of the individuals. The remaining two appeals had been pending resolution for 83 and 167 days, according to the TSC. The TSC stated that staffing constraints hindered its ability to more quickly resolve these redress appeals. The TSC informed us that in April 2007 it was able to assign redress appeal duties to a permanent staff position and the TSC believes that this action will improve the TSC's timeliness in resolving redress appeals.

Proactive Redress

It is possible for the TSC and other watchlist agencies to use available information to provide unsolicited relief to non-watchlist persons identified by the terrorist watchlist process. Besides its standard redress reviews, the TSC Redress Office also conducted ancillary evaluations of persons reported to have been identified by terrorist watchlist screening who had not filed a formal complaint. Additionally, the U.S. government, including the TSC and screening agencies, has information on persons misidentified as a terrorist

watchlist subject in the various screening databases. However, the U.S. government, including the TSC, is not currently coordinating the use of this data in attempts to proactively reduce the incidence and impact of misidentifying persons as watchlist subjects.

TSC Informal Redress Reviews

Typically, the TSC undertakes a redress review only when an individual submits a formal redress request. Occasionally, however, the TSC Redress Office reviews records outside this formal process. The TSC may be asked by a government official to look into a matter or it may acquire from a news media publication the name of a person possibly stopped due to the terrorist watchlist. For instance, a newspaper may publish an article explaining that a foreigner was not allowed to board a flight destined for the United States and the TSC Redress Office believes that the TSC should research the events. In such a case, the TSC Redress Office performs an evaluation similar to its formal redress review for such matters. First, it determines if the person was the subject of a terrorist watchlist-related encounter. If so, it reviews the related watchlist record for accuracy and completeness, making changes and updates as necessary.

The TSC Redress Office maintains a log that records the intake and resolution of these proactive reviews. Our review of this log shows that since this initiative began in December 2005, the TSC had resolved 76 cases through March 1, 2007, tracking them according to its redress disposition categories. Exhibit 4-5 shows that over 80 percent of these reviews involved an individual who experienced a watchlist-related encounter (misidentification and positive-match categories). Of the 32 positive matches, terrorist records were modified or removed from the watchlist for 16 of the reviews.

EXHIBIT 4-5
TSC Informal Redress Reviews
(December 2005 through March 1, 2007)

Disposition Category	Number	Percent
Misidentification	32	42%
Positive Match	32	42%
Non-related	10	13%
Further Investigation[68]	2	3%
Total	**76**	**100%**

Source: The Terrorist Screening Center Redress Office

[68] Two of the TSC Redress Office's informal reviews required further investigation in order to determine the relationship of the individual to a watchlist identity.

Use of Watchlist Encounter Information for Misidentified Individuals

The TSC has a record of all potential terrorist watchlist encounters referred to its call center, including information on positive, negative, and inconclusive encounters.[69] Therefore, the TSC has knowledge of the watchlist records involved in the negative encounters referred to its call center, as well as information on the individual that was misidentified as a potential terrorist for a period of time.

The TSC does not have any policy or procedures to proactively use information from negative encounters to reduce the incidence and impact of terrorist watchlist misidentifications. Moreover, the TSC's strategic plan does not include goals or actions associated with reducing the incidence of misidentifications or the impact on misidentified persons, other than that covered by the formal redress process. Considering that 43 percent of all encounters referred to the TSC Call Center are negative for a watchlist match, we believe the TSC should develop strategic goals and policy specific to mitigating the adverse impact of the terrorist screening process on non-watchlist subjects, particularly for individuals who are repeatedly misidentified as potential watchlist subjects.

Additionally, we believe the TSC should consider developing the ability within its encounter tracking system or consolidated watchlist database to alert the TSC to take proactive action on watchlist records that have been the subject of a certain number of encounters. For example, the system could be programmed to automatically generate a quality assurance lead for the TSC to perform a comprehensive review of the terrorist record. Such a function would help certify that a watchlist record frequently the subject of encounters, whether the encounters are positive, negative, or inconclusive, is accurate, complete, and current. This is important for both appropriately handling suspected or known terrorists and for reducing the adverse effects on persons misidentified as watchlist subjects.

Conclusion

Screening agencies across the federal government are in the process of instituting an interagency agreement that will formalize the U.S. government's review of redress inquiries from individuals who complain they were adversely affected during watchlist screening. Additionally, the

---

[69] Not all potential watchlist matches are referred to the TSC. If possible, screening agencies resolve negative encounters without contacting the TSC by comparing information on the encountered individual to the potential terrorist watchlist identity match. Screening agencies contact the TSC Call Center on all encounters where it cannot definitively make this determination.

TSC has developed its own SOP for processing redress complaints. We found that the TSC generally followed these procedures, the procedures are comprehensive, and TSC staff resolved redress matters logically and accurately.

However, our examination of TSC redress files also revealed that the TSC's comprehensive redress reviews often resulted in watchlist record changes and removals. We believe that the high percentage of redress reviews resulting in changes to or removals of watchlist records provides further evidence that watchlist data needs continuous monitoring and attention.

Our review also revealed that watchlist agencies, including the TSC and nominating and screening agencies, sometimes caused unnecessary delays in closing redress inquiry reviews. We recommend that the TSC coordinate efforts for the watchlist agencies to develop timeliness measures for each stage in the redress process.

Recommendations

We recommend that the TSC:

15. Organize a working group comprised of representatives from agencies involved in the terrorist watchlist redress process to develop timeliness measures for each phase in the redress process.

16. Develop goals and measures for its strategic plan to reduce the incidence and impact of misidentifications.

17. Develop procedures to proactively review terrorist watchlist identities that are frequently the subject of watchlist encounters, no matter if the encounter was positive, negative, or inconclusive.

We recommend that the FBI:

18. Develop and implement timeliness measures to ensure that the FBI responds in a timely manner to redress inquiries from complainants subject to terrorist watchlist-related encounters involving the NCIC database, including the complainant identified by the OIG whose complaint has been pending since February 2007.

STATEMENT ON INTERNAL CONTROLS

In planning and performing our audit of the TSC, we considered its control structure for the purpose of determining our audit procedures. This evaluation was not made for the purpose of providing assurance on the TSC management control structure as a whole. However, we noted certain matters involving management controls that we considered to be reportable conditions under the *Government Auditing Standards*.

Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operations of the management control structure that, in our judgment, could adversely affect the TSC's ability to maintain and disseminate accurate and complete information on known or suspected terrorists used during watchlist screening. We identified weaknesses in the TSC's internal control structure that resulted in inaccurate and incomplete watchlist records and terrorist identities not being correctly exported to downstream watchlist databases. These issues are discussed in Findings I, II, and III of the report.

Because we are not expressing an opinion on the TSC's management control structure as a whole, this statement is intended solely for the information and use of the TSC management. This restriction is not intended to limit the distribution of the report.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

In connection with this audit of the TSC, as required by generally accepted government auditing standards, we reviewed management processes and records to obtain reasonable assurance about the organization's compliance with laws and regulations that, if not complied with, in our judgment, could have a material effect on TSC operations. Compliance with laws and regulations applicable to the management of the TSC is the responsibility of the TSC's management.

Our audit included examining, on a test basis, evidence about laws and regulations related to the maintenance and sharing of information on suspected or known terrorists. The specific laws and regulations we reviewed included the relevant portions of:

- Intelligence Authorization Act, Public Law 108-177;
- Homeland Security Presidential Directive 6; and
- Homeland Security Presidential Directive 11.

Our tests of the consolidated terrorist watchlist identified weaknesses related to the accuracy and completeness of the data which is discussed fully in Findings I, II, and III. The requirements for an accurate and complete watchlist are contained in HSPD 6.

With respect to areas that were not tested, nothing came to our attention that caused us to believe that the TSC management was not in compliance with the laws and regulations cited above.

APPENDIX I: OBJECTIVES, SCOPE, AND METHODOLOGY

Audit Objectives

The objectives of the audit were to: (1) determine whether accurate and complete records are disseminated to and from the Terrorist Screening Center's (TSC) watchlist database in a timely fashion; (2) review the TSC's efforts to ensure the quality of the information in the watchlist database; and (3) assess the TSC's efforts to address complaints raised by individuals who believe they have been incorrectly identified as watchlist subjects.

Scope and Methodology

We performed our audit in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States, and accordingly, included such tests of the records and procedures that we considered necessary. Our audit covered but was not limited to the period of June 2005 through April 2007.

To accomplish our objectives, we conducted work primarily at the TSC, located in the Washington, D.C., metropolitan area. Additionally, we interviewed personnel at other federal agencies and offices whose work relates to TSC operations, such as NCTC, the FBI, DHS, and the White House Privacy and Civil Liberties Oversight Board.

To obtain an overall understanding of the TSC's role and responsibilities, we reviewed legislative materials related to the TSC's creation and watchlisting requirements, prior audit reports, and various other documents as needed, including financial documents, strategic plans, and staffing reports.

Accuracy and Completeness of Database Records

To obtain an understanding of the TSC's processes and procedures for ensuring the quality of data ingested into and exported from the Terrorist Screening Database (TSDB), we reviewed the TSC's procedures for processing database nominations and encounters. In addition, we interviewed:

- Contractors and representatives from the various participating Departments working within the TSC's Administration Branch, Operations Branch, Information Technology Branch, Call Center, Nominations and Data Integrity Unit, and other support areas.

- Program managers at NCTC.
- Supervisors from the FBI's Terrorist Threat Center, Terrorist Review and Examination Unit, and Terrorist Screening Operations Unit.
- The Executive Assistant Director of the FBI's National Security Branch and the Assistant Director and Deputy Assistant Director of its Counterterrorism Division.

Testing of Watchlist Database Records

As of March 16, 2007, there were 689,613 records in the web-based version of the TSDB. We performed various tests of a limited number of these records, and reviewed related records from the pertinent automated data systems used to store terrorist-related information maintained by the NCTC and FBI, to determine whether the records were accurate and complete, and any record changes were made in a timely fashion. The automated data systems were the TSDB, TSC's Encounter Management Application (EMA), NCTC's Terrorist Identities Datamart Environment (TIDE), and the FBI's Violent Gang and Terrorist Organization File (VGTOF).

In addition to querying the TSDB to identify duplicate records and determining whether records related to 20 FBI requests for removal had been deleted from the TSDB in a timely manner, our tests of judgmentally selected records included:

- Review of 50 TSDB records related to 25 FBI international terrorist and 25 FBI domestic terrorist nominations to determine whether basic identifying information [SENSITIVE INFORMATION REDACTED] listed on the FD-930 (the form used by the FBI for watchlisting nominations) were accurately entered into the databases. In addition, we analyzed key dates shown on the FD-930s to determine whether the names and other information were entered into the TSDB in a timely fashion.
- Review of a sample of 49 known terrorist names to determine whether the basic identifying information as well as citizenship and physical characteristics were accurately entered into the databases. Of these names, 10 were non-FBI originated international terrorist identities in the TIDE database, 17 were selected from the FBI's Most Wanted Terrorists list, 2 were selected from the Rewards For Justice website, 16 came from the State Department's Office of

Counter Terrorism, and 4 were obtained from various newspaper articles.

- Review of 51 TSDB records for which TSC staff had identified as having quality assurance issues, such as missing, outdated, or inaccurate information.[70] This review included identifying the quality assurance issue that was raised, determining whether the appropriate changes had been made to the TSDB, TIDE, and VGTOF records. In addition, we evaluated the timeliness of the revision and any additional follow-up performed by TSC staff to ensure that the necessary changes were made. Finally, we reviewed these records to determine whether the basic identifying information was accurately entered into the databases.

- Review of 20 TSDB records related to positive encounters with watchlist subjects, as recorded in EMA, to determine whether the basic identifying information was accurately entered into the databases and information obtained by law enforcement agencies as a result of the encounters was added to appropriate database records.

- Review of 15 TSDB records that TSC staff identified as having undergone a thorough quality assurance review as part of a special project to evaluate the adequacy of the TSC's review and to determine whether the basic identifying information was accurately entered into the databases.

Finally, we compared information in the TSDB records to watchlisting criteria to determine whether the individuals were nominated for the appropriate watchlists and were assigned an appropriate handling instruction.[71]

Watchlist Redress

To obtain an understanding of the TSC's role in the terrorist watchlist redress process and its efforts to reduce watchlist misidentifications, we reviewed the TSC's redress procedures and the U.S. government's

---

[70] 25 of the 51 records were selected from the TSC's Quality Assurance Tracker, the TSC's original system for monitoring TSDB records with quality assurance issues. The remaining 26 records were selected from quality assurance tickets, the TSC's current monitoring system.

[71] The criteria used by the agencies hosting TSDB records are identified in Appendix II.

interagency agreement on terrorist watchlist redress. We judgmentally selected and examined 20 redress complaints reviewed by the TSC Redress Office to evaluate whether the TSC followed its Redress SOP for resolving a redress complaint.

We also conducted interviews with the TSC's Privacy and Redress Officers, and we reviewed the TSC's strategic plan to identify any goals related to redress or reducing the incidence and effect of watchlist misidentification. Additionally, to obtain an understanding of the partner agencies' roles in the redress process and how they coordinate with the TSC, we interviewed representatives from the White House Privacy and Civil Liberties Oversight Board, the DHS's Screening Coordination Office, TSA, and CBP.

From January 2005 through February 2007, 438 redress complaints were referred to the TSC. During this same period, the TSC closed 388 complaints. We performed various analyses of TSC's redress referral data, including calculating:

- the percent of cases referred to the TSC according to referring agency;
- the average amount of time cases were open, and evaluating the reasons affecting delays in closing the matters; and
- the TSC's disposition for its closed redress matters.

APPENDIX II: SYSTEMS USED IN THE TERRORIST WATCHLIST PROCESS

The Terrorist Screening Database (TSDB) is the U.S. Government's consolidated terrorist watchlist. The TSDB contains basic biographical information on known or appropriately suspected domestic and international terrorists. In this regard, the underlying derogatory information on individuals nominated for inclusion in the TSDB must demonstrate a reasonable suspicion of ties to terrorism.

Currently, TSDB records are exported to various U.S. and international government entities tasked with conducting terrorism screening. Each agency receiving TSDB records has established criteria that dictate what records it receives from the TSC. The TSC provided us with the following descriptions of the databases receiving watchlist records and the minimum criteria for exporting records to them:

CLASS

The Consular Lookout and Support System (CLASS) is maintained by the Department of State (State Department). CLASS, divided into CLASS/Visa and CLASS/Passport, is used by State Department representatives when processing visa and passport applications, respectively.

[SENSITIVE INFORMATION REDACTED]

IBIS

The Interagency Border Inspection System (IBIS) is maintained by DHS's U.S. Customs and Border Protection agency. IBIS is generally queried by federal law enforcement agents at ports of entry.

[SENSITIVE INFORMATION REDACTED]

No Fly and Selectee Lists

The No Fly and Selectee Lists are maintained by the Transportation Security Administration. These lists are used by public carriers, both airline and other modal, to screen their passengers. The No Fly list includes individuals who are prohibited from boarding an aircraft. The Selectee list includes individuals who must undergo additional security screening checks before being permitted to board an aircraft.

[SENSITIVE INFORMATION REDACTED]

- In addition, a minimum threshold of derogatory information for inclusion on the No Fly or Selectee lists was established on October 21, 2004, by the Homeland Security Council.

[SENSITIVE INFORMATION REDACTED]

VGTOF

Terrorist records contained in the Violent Gang and Terrorist Organization File (VGTOF) is one segment of the FBI's National Crime Information Center (NCIC) system. The NCIC is a database queried by federal, tribal, state, and local law enforcement agencies in performance of their duties.

Minimum Criteria:

In order for a known or suspected terrorist to be included in VGTOF, the following minimum biographical information is required:

- first name
- last name
- approximate year of birth

APPENDIX III: DIAGRAM OF TERRORIST WATCHLIST DATAFLOW

[SENSITIVE INFORMATION REDACTED]

APPENDIX IV: ACRONYMS

CBP	Customs and Border Protection
CIA	Central Intelligence Agency
CIO	Chief Information Officer
CLASS	Consular Lookout and Support System
DHS	Department of Homeland Security
DOJ	Department of Justice
EMA	Encounter Management Application
FBI	Federal Bureau of Investigation
FY	Fiscal Year
HSPD-6	Homeland Security Presidential Directive-6
IBIS	Interagency Border Inspection System
ICE	Immigration and Customs Enforcement
IT	Information Technology
MOU	Memorandum of Understanding
NCIC	National Crime Information Center
NCTC	National Counterterrorism Center
NDIU	Nominations and Data Integrity Unit
NTP	Nomination Tracking Processor
ODNI	Office of the Director of National Intelligence
OIG	Office of the Inspector General
TIDE	Terrorist Identities Datamart Environment
TREX	Terrorist Review and Examination Unit
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Database
TSOU	Terrorist Screening Operations Unit
SOP	Standard Operating Procedure
VGTOF	Violent Gang and Terrorist Organization File

APPENDIX V: TERRORIST SCREENING CENTER RESPONSE

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

August 28, 2007

The Honorable Glenn A. Fine
Office of the Inspector General
United States Department of Justice
Room 4322
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

Dear Mr. Fine:

This letter is submitted by the Federal Bureau of Investigation (FBI) in response to the audit report by the Office of Inspector General (OIG) entitled: Follow-up Audit of the Terrorist Screening Center (hereinafter the Report).

The FBI appreciates the opportunity to comment and agrees fully with the OIG that the mission and function of the Terrorism Screening Center (TSC) is a critical part of the layered national strategy to safeguard the Homeland from a future terrorist attack.

The FBI remains committed to ensuring the timely and accurate collection of watchlisting data for distribution to those government agencies responsible for screening, law enforcement and intelligence work. One of the TSC's highest priorities is to ensure the Terrorist Screening Database (TSDB) is accurate, current and thorough. When the consolidated watchlist was originally created, agencies and Departments provided all possible data from their holdings to serve as the foundation for terrorist watchlist information. Much of the original data provided to the TSC lacked a validation or review process by the originating agency, which presented initial challenges in quality of the TSDB. Since that time the quality of the TSDB data has vastly improved. For example, as of July 2007, TSC has completed a full vetting of the Department of Homeland Security's No-Fly list, resulting in an approximate 50% reduction of records.

The field work of the OIG has confirmed that the TSC has enhanced its efforts to ensure the quality of watchlist data, we have increased the level of staff assigned to data quality management and we have developed a process, complete with a separate office to respond to redress complaints filed by persons seeking relief from adverse effects related to terrorist watchlist screening.

I believe the TSC has improved the security of the Homeland by leading the effort to consolidate the terrorist watchlisting process and serving as the accountable entity pursuing watchlisting as its single core competency. The TSC's efforts combined with the U.S. Government's (USG) community effort to significantly increased information sharing at all levels of state, local and federal government, has lead to enhanced security. The TSC is fully committed to constantly examining its operations for enhancements in efficiency and effectiveness. The TSC has made significant progress in its mandate to consolidate the USG's approach to terrorism screening and its leadership makes every effort to ensure the most thorough, current and accurate information is provided to law enforcement and intelligence community partners for a safer and more secure nation. In that spirit, the FBI and the TSC offers the following responses to the specific recommendations made in the Draft Audit Report, *Follow-Up Audit of the Terrorist Screening Center*.

Recommendation # 1:

Implement its plan to consolidate the TSDB NTP and legacy systems in a timely manner. In the interim while the two systems coexist, the TSC should establish a formal procedure to regularly review the TSDB NTP and legacy systems to ensure that the information in these systems remains synchronized.

Response: The TSC has developed a project plan that guides the prioritization of tasks to achieve the objective of consolidating NTP component with the official record keeping component of the TSDB. The TSC has implemented a daily reconciliation process between the two components in the interim period for routine monitoring of the data.

Recommendation # 2:

Develop procedures to regularly review and test the information contained in the TSDB to ensure the data is complete, accurate, and non-duplicative.

Response: The TSC accepts this recommendation and notes that it has used informal procedures to review and test TSDB information in the past, but has now implemented procedures to formalize this process.

Recommendation # 3:

Modify the TSDB NTP to accommodate designations for both CLASS/Visa and CLASS/Passport. In addition, the TSC should review and correct the records identified in the TSDB NTP to appropriately reflect that U.S. persons are not eligible for export to CLASS/Visa.

TSC Response: The TSC agrees with this recommendation and will implement these changes as part of the transfer of exports to TSDB NTP.

Recommendation # 4:

Review and correct the records identified in the TSDB NTP to ensure that the IBIS handling instructions are appropriately applied.

Response: The TSC agrees with this recommendation and has corrected the records.

Recommendation # 5:

Develop procedures to regularly review the information in the TSDB to ensure that outdated or obsolete data is removed in a timely manner.

Response: The TSC accepts this recommendation and notes it has used previously undocumented procedures to remove outdated or obsolete data, and will now formalize this process to ensure it is removed in a timely manner.

Recommendation # 6:

Working with the TSC, revise the watchlist nomination process to provide international terrorist nominations directly to NCTC for inclusion in TIDE, submission to the TSC, and dissemination to all downstream databases, including VGTOF.

Response: The FBI and TSC watchlist nomination process was initially created to address a concern that watchlist nominations were not being processed in an expedient manner. Both the FBI and TSC conduct 24/7 operations that include near real-time submissions to the watchlisting process on weekend days and after normal business hours. The NCTC personnel assigned to the watchlisting process now work a 16 hour shift Monday through Friday. With the objective in-mind to ensure that all watchlisting nominations are processed timely. The FBI will continue to work to revise the current process recognizing watchlisting must take place when NCTC is not available.

Recommendation # 7:

Correct the records identified by the OIG containing incorrect watchlist designations, handling code errors, and inaccurate and inconsistent information.

Response: The TSC agrees this recommendation and has taken steps to correct the records under its purview.

Recommendation # 8:

Coordinate with NCTC and the FBI to implement an agreement that establishes the areas of responsibility and the timeframes for data quality assurance matters.

Response: The TSC accepts the recommendation to implement an agreement with both NCTC and the FBI's National Threat Center Section to establish areas of responsibility and timeframes for data quality assurance matters.

Recommendation # 9:

Develop a comprehensive standard operating procedure that describes the TSC's three-pronged quality assurance strategy and details the methodology to be used in performing quality assurance reviews.

Response: The TSC accepts this recommendation to document a comprehensive SOP which describes it quality assurance strategy and methodology.

Recommendation # 10:

Develop a process to perform regular spot-checks of NDIU analysts' work to identify any weaknesses and need for additional training.

Response: The TSC accepts this recommendation to document and perform a standardized methodology for NDIU spot-checks that will identify areas for targeted training, replacing its previously used undocumented process.

Recommendation # 11:

Develop an improved and user-friendly process for tracking classified correspondence related to quality assurance matters.

Response: The TSC agrees with this recommendation and has already implemented a solution. TSC will utilize the FBI's Automated Case Support (ACS) system to track all quality assurance classified correspondence. All classified correspondence, to include e-mails and electronic communications (EC), will be uploaded to a control file within ACS which will house such communications.

Recommendation # 12:

Develop a tickler system or electronic dashboard for all pending quality assurance matters.

Response: The TSC accepts this recommendation and has begun efforts to develop same.

Recommendation # 13:

Develop a comprehensive plan, including benchmarks or milestones, to complete the record-by-record review of the TSDB.

Response: TSC will develop a comprehensive plan that will ensure each record in the TSDB has undergone a quality assurance review in addition to those high priority projects currently underway.

Recommendation # 14:

Coordinate with other partner agencies to establish a formal process for relevant encounter information to be captured by frontline screening agents and returned to the TSC to update watchlist records.

Response: The TSC accepts this recommendation to establish a formal process to update watchlist records with encounter information and notes it has used an undocumented process to accomplish this recommendation since its inception.

Recommendation # 15:

Organize a working group comprised of representatives from agencies involved in the terrorist watchlist redress process to develop timeliness measures for each phase in the redress process.

Response: TSC accepts this recommendation; the implementation of which is underway and pending signatures by all parties.

Recommendation # 16:

Develop goals and measures for its strategic plan to reduce the incidence and impact of misidentifications.

Response: TSC accepts this recommendation and is developing appropriate goals and performance measures as part of the strategic plan.

APPENDIX V

Recommendation # 17:

Develop procedures to proactively review terrorist watchlist identities that are frequently the subject of watchlist encounters, no matter if the encounter was positive, negative, or inconclusive.

Response: TSC accepts this recommendation. TSC is currently developing the framework for a new program that will proactively review watchlist records related to frequently encountered individuals.

Recommendation # 18:

Develop and implement timeliness measures to ensure that the FBI responds in a timely manner to redress inquiries from complainants subject to terrorist watchlist-related encounters involving the NCIC database, including the complainant identified by the OIG whose complaint has been pending since February 2007.

Response: The FBI accepts this recommendation and has instituted new policy and process. The February 2007 complainant involves a unique and very sensitive matter which has been resolved.

The FBI, the TSC and our strategic partners will continue to pursue efforts to improve the terrorist watchlisting process.

Sincerely,

Willie T. Hulon
Executive Assistant Director
National Security Branch

APPENDIX VI: OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT

In its response to our draft audit report, the TSC concurred with each of our 18 recommendations and discussed the actions it has already taken and others it will implement in response to our findings. This appendix contains our analysis of the TSC's responses to our recommendations and the actions necessary to close each recommendation.

Status of Recommendations

1. **Resolved.** The TSC concurred with our recommendation that it implement its plan to consolidate the TSDB NTP and legacy databases in a timely manner, and the TSC stated that it developed a project plan to guide the future consolidation of the system. In the interim period while it is still necessary to operate both databases, the TSC stated that it implemented a daily reconciliation process between the TSDB NTP and legacy databases for routine monitoring of the data.

   This recommendation can be closed when we receive evidence that the TSC has fully implemented its plan to consolidate the TSDB NTP and legacy databases. In the meantime, please provide evidence that the TSC has implemented a daily reconciliation process that identifies and addresses differences in database content.

2. **Resolved.** In its response to our draft report, the TSC concurred with our recommendation to develop procedures to regularly review and test the information contained in the TSDB to ensure the data is complete, accurate, and non-duplicative. The TSC noted that it has used informal procedures to review and test the information in the TSDB, and it now has implemented procedures to formalize this process.

   This recommendation can be closed when we receive documentation or other evidence to support that the TSC has developed and fully implemented procedures to regularly review and test information in the TSDB to ensure the data is complete, accurate, and non-duplicative.

3. **Resolved.** The TSC concurred with our recommendation and stated that it will implement our recommended changes as part of its planned, phased improvements for the TSDB NTP, including the incorporation of the export capability of the legacy system.

This recommendation can be closed when we receive evidence that the TSC has mofidied the TSDB NTP to accommodate designations for both CLASS/Visa and CLASS/Passport, and that it has reviewed and corrected the records identified in the TSDB NTP to appropriately reflect that U.S. persons are not eligible for export to CLASS/Visa.

4. **Resolved.** The TSC concurred with this recommendation and stated that it had completed its review of watchlist records and made corrections to records in the TSDB NTP with incorrect IBIS handling instructions.

   This recommendation can be closed when we receive evidence that the TSC identified and corrected the watchlist records with inappropriate IBIS handling instructions.

5. **Resolved.** In its response to our draft report the TSC concurred with this recommendation and stated that while it had used previously undocumented procedures, it will now formalize this process to ensure that outdated or obsolete data is removed in a timely manner.

   This recommendation can be closed when we receive evidence that the TSC has developed and implemented formal procedures to regularly review the information in the TSDB to ensure that outdated or obsolete data is removed in a timely manner.

6. **Resolved.** The FBI concurred with our recommendation and stated that it will continue to work to revise the current nomination process. However, the FBI stated that it had implemented its current nomination process initially to address its concern that watchlist nominations were not being processed in a timely manner due to the operations schedule of the NCTC.

   While we recognize that the FBI conducts its watchlisting operations on a continuous basis, we believe that the NCTC is operational during the time period in which the majority of watchlist nominations are submitted. Further, an additional emergency nomination process is available to the FBI for those instances in which the FBI determines a nomination is exigent and the NCTC may not be available. Given our identification of significant data errors and inconsistencies resulting from the FBI's non-standard nomination process for international terrorists, we believe that the FBI, NCTC, and TSC should work together to design a more consistent and reliable process by which FBI-originated international terrorist information is provided to the

NCTC for inclusion in TIDE and disseminated to the TSDB and downstream screening systems, including VGTOF. To close this recommendation, please provide us with information on specific steps taken to revise the FBI's watchlist nomination process for known or suspected international terrorists.

7. **Resolved.** The TSC concurred with this recommendation and stated that it has taken steps to correct the watchlist records under its purview. This recommendation can be closed when we receive evidence that the records we identified during our review that contained incorrect watchlist designations, handling code errors, and inaccurate and inconsistent information have been corrected.

8. **Resolved.** The TSC concurred with our recommendation to coordinate with NCTC and FBI to implement an agreement that establishes the areas of responsibility and the timeframes for data quality assurance matters.

   This recommendation can be closed when we receive evidence supporting the implementation of a signed agreement between the NCTC and FBI that outlines areas of responsibility and the timeframes for data quality assurance matters.

9. **Resolved.** The TSC concurred with our recommendation to develop a comprehensive standard operating procedure that describes the TSC's quality assurance strategy and details the methodology to be used in performing quality assurance reviews.

   This recommendation can be closed when we receive evidence that the TSC has finalized its quality assurance strategy and methodology and has trained its staff on using the standard operating procedure in performing quality assurance reviews.

10. **Resolved.** The TSC concurred with our recommendation to develop a process to perform regular spot-checks of NDIU analysts' work. This recommendation can be closed when we receive evidence that the TSC has developed, documented, and implemented a process to perform regular spot-checks of NDIU analysts' work to identify weaknesses and needs for additional training.

11. **Resolved.** In its response, the TSC concurred with this recommendation and stated that it had implemented a solution to remedy our finding. Specifically, the TSC stated that it will utilize the FBI's Automated Case Support (ACS) system to track all quality

assurance classified correspondence, including e-mails and electronic communications.

This recommendation can be closed when we receive evidence that the TSC has formally documented this process and communicated the policy to its staff.

12. **Resolved.** The TSC concurred with this recommendation and stated that it has begun developing a tickler system or electronic dashboard for pending quality assurance matters. This recommendation can be closed when we receive evidence that the TSC has implemented such a system.

13. **Resolved.** The TSC concurred with this recommendation and stated that it will develop a comprehensive plan to ensure that each record in the TSDB has undergone a quality assurance review.

    This recommendation can be closed when we receive evidence that the TSC has developed a plan that: (1) includes specific milestones for the successful completion of this comprehensive review, (2) tracks its progress against these milestones, and (3) identifies actions to take if the milestones are not met.

14. **Resolved.** The TSC concurred with this recommendation and stated that since its inception the TSC has used an undocumented process to coordinate with other partner agencies to obtain relevant information captured by frontline screening agents during encounters with known or suspected terrorists. We recognize that the TSC has endeavored to update watchlist records by incorporating encounter information captured by frontline screening agents. However, without a formal process with which frontline screening agencies agree, the TSC is unable to ensure that it is receiving complete, accurate, and timely encounter information. This recommendation can be closed when the TSC provides documentation to support that a formal process has been developed and implemented between partner agencies to ensure that encounter data is appropriately returned to the TSC for updating watchlist records.

15. **Resolved.** The TSC concurred with this recommendation and stated that implementation to address this recommendation was underway and pending signatures by all parties. This recommendation can be closed when we receive the finalized agreement containing timeliness measures for processing watchlist redress matters agreed to and signed by the appropriate agencies.

16. **Resolved.** The TSC concurred with this recommendation and stated it is developing goals and performance measures relative to misidentifications for its strategic plan. This recommendation can be closed when the TSC provides its updated strategic plan that includes goals and performance measures to address reducing the incidence and impact of misidentifications.

17. **Resolved.** The TSC concurred with this recommendation, stating in its response that it is developing the framework for a program that will proactively review watchlist records related to frequently encountered individuals. This recommendation can be closed when the TSC provides documentation formalizing this new proactive redress program, as well as evidence that this program has been implemented.

18. **Resolved.** The FBI concurred with our recommendation and stated that it has instituted a new policy and process for resolving redress matters involving the NCIC database. Additionally, the FBI noted that the February 2007 redress matter that was pending at the time of our review has been resolved.

    To close this recommendation, please provide us the FBI policy containing timeliness measures for processing NCIC-related redress matters. Additionally, please provide documentation to confirm that the February 2007 redress matter that was pending at the time of our review has been appropriately resolved.

Post-Hearing Responses to Questions for the Record
Submitted to Eileen R. Larence
From Senator Joseph I. Lieberman

"Watching the Watch List: Building an Effective Terrorist Screening System"
October 24, 2007

1. What role do fusion centers play today as part of the overall watch listing system? What role should they play in the future? Have any federal agencies, to your knowledge, developed guidance with respect to the use of the terrorist watch list (or its subsets) by fusion centers?

   Response: Terrorism information and intelligence that can be generated by fusion centers is directed to the Federal Bureau of Investigation (FBI) because of its counterterrorism mission.[1] The agency can use this information to support the nomination of an individual to the Terrorist Screening Center for inclusion on the watch list and any ongoing investigations the FBI may have on such individuals. Fusion centers also can have access to watch list records through the FBI's National Crime Information Center (NCIC) database. This database not only contains information on individuals such as criminal histories but also integrates records from the watch list. Currently, state and local law enforcement officers and other criminal justice agencies access NCIC to screen individuals in conjunction with arrests, detentions, and other criminal justice purposes, thus, they are also screening the individuals against watch list records at the same time. As fusion centers enhance their operations, they can play an increasingly important role in collecting and analyzing information to support watch list nominations and investigations and to help federal agencies identify known or suspected terrorists who are on the watch list.

   In August 2006, the Department of Justice—in collaboration with the Department of Homeland Security—issued fusion center guidelines.[2] The guidelines note that fusion centers should consider obtaining access to a variety of databases and systems, including the NCIC database and the Terrorist Screening Center database.

---

[1]See GAO, *Homeland Security: Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers*, GAO-08-35 (Washington, D.C.: Oct. 30, 2007).

[2]See U.S. Department of Justice, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era* (Aug. 2006).

Post-Hearing Responses to Questions for the Record
Submitted to Eileen R. Larence
From Senator Daniel K. Akaka

"Watching the Watch List: Building an Effective Terrorist Screening System"
October 24, 2007

1. A critical component of using the watch list to protect our country against terrorists is ensuring that the law enforcement and intelligence community is really working together and sharing threat information.

   Government Accountability Office's report states that the Central Intelligence Agency (CIA) and the Homeland Security Council (HSC) denied your requests for interviews.

   a. Did the CIA and HSC provide an explanation for their refusal to cooperate with your review?

   Response: Both the CIA and HSC verbally declined our requests for interviews, and they provided a general rationale. With regard to the CIA, we had asked to interview CIA officials about the CIA's role as a nominating entity in the terrorist screening process. In declining to discuss this issue, a CIA official explained that the agency's role in the terrorist screening process involves intelligence activities, and that the CIA considers these activities as not subject to GAO oversight. We disagree with this position. GAO has authority to perform oversight of such activities. GAO has broad statutory authority to audit and evaluate agency financial transactions, programs, and activities, and these authorities apply to reviews of the intelligence community. See 31 U.S.C. §§ 712, 717. Subject to a few limited exceptions established in law,[1] each agency must provide the Comptroller General with information the Comptroller General requires about the duties, powers, activities, organization, and financial transactions of the agency. See 31 U.S.C. § 716(a). These requirements also apply to the intelligence community.

   With regard to HSC, council officials told us that it is HSC's policy and practice not to participate in GAO reviews since HSC is part of the Executive Office of the President. As such, they did not provide us with specific responses regarding HSC's role in the terrorist screening process.

[1]These exceptions include narrow legal limitations on our access to certain "unvouchered" accounts of the CIA and on our authority to compel our access to foreign intelligence and counterintelligence information. For more detail, see our testimony, U.S. General Accounting Office, *Central Intelligence Agency: Observations on GAO Access to Information on CIA Programs and Activities*, GAO-01-975T (Washington, D.C.: July 2001). See also 31 U.S.C. § 716(d).

b. Did these refusals to cooperate with your review limit your review in any way? If so, please provide details.

Response: While the positions of these two organizations did limit our detailed understanding of parts of the terrorist watch list screening process, we were able to obtain a general understanding of the CIA's and HSC's role from other sources to complete our review and provide a useful report to the Congress. The CIA's position limited our more detailed understanding of the specific criteria and processes that agencies within the intelligence community use to nominate individuals for inclusion on the watch list and manage encounters with individuals on the list. HSC's position limited our more specific and detailed understanding of the council's role in setting policy for the management and use of the watch list in agency screening processes.

Watchlisting Testimony
Hearing of the Senate Homeland Security
and Governmental Affairs Committee
October 24, 2007

Inspector General Fine's Responses to Questions for the Record

At the hearing on October 24, 2007, Senator Warner asked each of the witnesses to respond in writing to the question reprinted below.

SEN. JOHN WARNER (R-VA): *We're privileged in the Commonwealth of Virginia to have the National Ground Intelligence Center, and I visit quite frequently. And they're on the cutting edge of the biometrics, and somehow it's come to my attention -- I'm not sure of the accuracy -- that the Terrorist Screening Center presently does not have a number of these capabilities.*

Question: *Are you leveraging it from other areas to incorporate it, are you planning to get it, or do you think it should be made a part of the program? Please answer the question for the record because I've got to yield to my colleague.... I'll ask each of the witnesses to make a contribution. Thank you.*

ANSWER: In the Office of the Inspector General's (OIG) 2005 audit of the Terrorist Screening Center (TSC), we reported that the TSC had developed its consolidated database to accommodate biometric information. However, at that time TSC officials decided it would not incorporate biometric data into the TSC's consolidated database because the TSC believed it was more appropriate to maintain the consolidated database as more of an "index," which would maintain its role as an unclassified subset of information on watchlisted persons. As a result, the TSC database serves as the consolidated source of basic identifying information, and a pointer to other databases, which have a greater capacity to include biometric data. In order to obtain available biometric data to assist in confirming the identity of encountered individuals, the TSC would use the databases that provide source material for the watchlist, such as the National Counterterrorism Center's TIDE database or the FBI's Automated Case Support system. During our 2007 audit of the TSC, we were told that the TSC would be working to increase the number of photographs of known or suspected terrorists in the consolidated terrorist screening database (TSDB).

Based upon our findings, particularly those related to record inconsistencies and duplication, we do not believe that the TSC's position that it should not further expand the biometric content of the records in the consolidated database is unreasonable. At present, the TSC has exhibited weaknesses in its ability to ensure that the watchlist records are consistent, accurate, and current and the addition of biometric data could further exacerbate these problems. Further, TSC call screeners and analysts have ready access to the

supporting systems and the available biometric information contained therein. Lastly, the inclusion of biometric data also would add complexity to classification of the information in the TSDB, which by Presidential order is to remain sensitive but unclassified. This is not to say that at a future point it would not be technologically feasible and operationally prudent to add biometric data to the database.

Clarification of Response to Question from Senator Levin

I also want to clarify and amplify a response that I gave to questions from Senator Levin. The clarification relates to the following questions and answers:

SEN. CARL LEVIN (D-MI): *Mr. Chairman, thank you for holding this hearing. I will try to avoid the questions if they have been asked before.*

The IG has found duplicate records in the terrorist screening database which can slow down the screening process or even put a law enforcement officer at risk if the handling instructions are inconsistent. In their report, the IG's report says that TSC officials stated that they will review the TSDB on a weekly basis for duplicate records. Is that now going on?

MR. BOYLE: *Yes, sir. And I think it's important to identify that duplicate records in some instances are unavoidable because we have to maintain more than one record on a particular person because our downstream customers may want different fields of information. So while it appears to be duplicative because the name, date of birth, et cetera, is the same, we have to include some additional information.*

What is of real concern, and was importantly pointed out by the Office of Inspector General, is when there are inconsistencies that might result in a different sort of category code. We are reviewing that to make sure that that doesn't occur.

SEN. LEVIN: *About how many inconsistencies have appeared? Is this a rare, rare thing? Is this one out of 1,000?*

MR. BOYLE: *I believe that the figure that was identified by the Office of Inspector General was -- (to Mr. Fine) -- 38 percent?*

MR. FINE: *I'm not -- I think that was the problem with quality assurance review. I think our report said that it was approximately -- we saw approximately 2,000*

in the first instance of duplicate records. I'm not sure all of them had different handling instructions, but that was the concern that we had, duplicate records with significantly different handling instructions --

SEN. LEVIN: *What percentage is that?*

MR. FINE: *If there are approximately 800,000 records, it's a very small percentage.*

SEN. LEVIN: *So it's less than a --*

MR. FINE: *Less than 1 percent, yeah.*

SEN. LEVIN: *Okay.*

I wanted to clarify the response to this question. In the OIG's 2007 audit, we reviewed the TSC's consolidated database for duplicate records, which we defined as those records that contain the same information for 5 primary identifying fields. We identified at least 2,533 repeated combinations in these 5 core identifying fields involving about 6,262 watchlist records. My answer focused on the 2,533 duplicated records, which, as noted in my answer to Senator Levin, is less than 1 percent of the approximately 800,000 records in the TSC's consolidated database.

After the hearing, our auditors checked the data and of the more than 2,000 duplicate records, we identified approximately 136 duplicate records in which the handling code was not consistent among all duplicates attributed to one record. For example, we identified one individual with duplicate identity records in the consolidated watchlist. Because both records pertained to the same individual, the instructions for handling the subject should be consistent. Yet, we identified significant differences between the records regarding handling instructions and additional warnings related to the individual. Specifically, one record noted that the individual was "armed and dangerous with violent tendencies" and also had a valid arrest warrant. The other record did not contain this important information. These types of inconsistencies place screeners and law enforcement officers at undue risk and could potentially result in the admittance of a dangerous individual into the United States.

Therefore, we believe that of the duplicate records we reviewed, approximately 136 had differing handling instructions. This number is, as I answered at the hearing, much less than 1 percent of the total number of records in the database.

It is important to point out that these results pertain only to duplicate records. We also identified inconsistent handling instructions in non-duplicate records contained within the various databases involved in the screening process. For example, 2 of 49 known or suspected terrorist records we reviewed exhibited inconsistent handling information between the database and the downstream screening database in the National Crime Information Center system. Therefore, the number of watchlist and screening records with inconsistent handling instructions is greater than 136. However, based on our limited sampling, we cannot determine with certainty how many inconsistencies there are in the TSC's consolidated database or between the TSC's consolidated database and the individual watchlist systems.

I hope this amplification addresses your question. If you have further questions, please let me know.

Watchlisting Testimony
Hearing of the Senate Homeland Security and Governmental Affairs Committee
October 24, 2007

Inspector General Fine's Responses to Post-Hearing Questions for the Record Submitted By Senator George V. Voinovich

1. International cooperation and information sharing, particularly with nations in the Visa Waiver Program, could be vital to populating the terrorist watch list. To the extent possible, please discuss current agreements or negotiations with other countries which seek to increase the sharing and quality of information on the consolidated watch list.

   Answer: In the Department of Justice (DOJ) Office of the Inspector General's (OIG) 2005 audit of the Terrorist Screening Center (TSC), we reported that the TSC had cooperative agreements to share appropriate information about terrorists with two foreign governments. Since that time, the TSC has entered into information-sharing agreements with six additional foreign governments. Although we have not reviewed in detail these new information sharing agreements, we believe these arrangements represent a positive step toward enhancing the utility of the terrorist watchlist. We also believe that the TSC should continue to pursue such arrangements with additional nations, including those that participate in the Visa Waiver Program.

2. In Mr. Rosenzweig's testimony, he states that the Department's Traveler Redress Inquiry Program received over 21,000 requests for redress between February and October of 2007, but many of these are on hold, waiting for the travelers to submit the required documentation. In your testimony, however, you note that a redress review on the part of the Terrorist Screening Center averages 67 days. Your testimony suggests that the delay is not linked to the individual, but rather to problems with the nominating agencies or in finalizing a determination. How is the Department's process of redress different from the Terrorist Screening redress process? Should this process become more formalized and uniform for all participating agencies?

   Answer: In the DOJ OIG's 2007 audit of the TSC, we noted that complainants file redress inquiries with the frontline screening agencies involved in the encounters, such as the FBI, the State Department, or through the Traveler Redress Inquiry Program (TRIP) to the Department of Homeland Security (DHS). Once

received, the screening agency reviews the complaint and determines if the inquiry relates to a possible terrorist watchlist match. If the screening agency determines that the complaint is not related to the terrorist watchlist, it should resolve the matter internally and respond to the complainant without referring the matter to the TSC. However, the screening agency should refer to the TSC all redress inquiries if the individual was a positive or inconclusive match to a watchlist record. For all inquiries forwarded to the TSC, a TSC Redress Office analyst reviews the corresponding watchlist record to ensure it is accurate, complete, and current. The analyst then recommends any necessary changes to the record or watchlist status. Then the TSC Redress Office ensures that the necessary changes are made to watchlist records before closing its review and alerting the frontline screening agency of its resolution. The TSC does not respond to the complainant. Rather, the TSC coordinates with the frontline screening agency, which should submit a formal reply to the complainant.

The DHS is a frontline screening agency that deals directly with travelers' complaints, while the TSC coordinates with the DHS to resolve watchlist matters related to these complaints. Because we are not the OIG for the DHS, we did not, and could not, examine the DHS's redress process. It is important to note that the delays we noted and time frames we calculated (67-day average for redress matters) related only to the time it took for the TSC to complete its redress activities. Because the DHS and TSC have different roles in the resolution of redress complaints, we believe it is likely that the reasons for delays in each agency may be different.

Finally, while there is some benefit to uniformity in redress procedures among different agencies, we also believe that effective processes will likely have some differences across agencies. However, we believe there should be performance goals in each agency that require the agency to resolve redress complaints within a specified time period. The time period could vary with each agency, depending on the number of complaints normally received, or the difficulties involved in resolving the complaints. Each agency should set goals, test to see whether those goals are being met, and take action to reform the process if the timeliness goals are not being met.

Committee on Homeland Security and Governmental Affairs
United States Senate

"Watching the Watch List:
Building an Effective Terrorist Screening Center"

October 24, 2007

Responses of the Federal Bureau of Investigation to Questions for the Hearing Record from Terrorist Screening Center Director Leonard Boyle

Questions Posed by Senator Lieberman

1. a. What role do fusion centers play today as part of the overall watch listing system?

Response::

Currently, Fusion Centers (FCs) interact with the Terrorist Screening Center's (TSC) 24/7 Terrorist Screening Tactical Operations Center and Tactical Analysis Unit, have access to much of the Terrorist Screening Database (TSDB) through the National Crime Information Center (NCIC) and the Treasury Enforcement Communications System, where available, and are able to access several other Department of Justice (DOJ) and Department of Homeland Security (DHS) systems that contain terrorist watchlists or subsets thereof. At present, though, the FCs are not always notified of encounters with known or appropriately suspected terrorists.

Generally, when a suspect is encountered by a screening agency (local law enforcement, U.S. Customs and Border Protection (CBP), etc.), this information is passed to the TSC, which determines whether the individual is a known or suspected terrorist. If the individual is a positive match in the TSDB, the TSC notifies the FBI's Terrorist Screening Operations Unit, which coordinates with the relevant Joint Terrorism Task Force (JTTF) to develop an appropriate response. FCs may be contacted by the TSC, often after the encounter, when it appears beneficial to tap the FC's ability to blend, analyze, and disseminate criminal intelligence and other information in an effort to anticipate, identify, prevent, and/or monitor terrorism and other criminal activity. FCs serve as a mechanism through which local law enforcement can share critical information with the FBI for further analysis, dissemination, and potential inclusion on the watchlist.

As part of the effort to better use the FCs, the TSC is creating an Information Technology (IT) solution through which local FCs will be automatically notified in real-time of an encounter in their area of responsibility. Some states have already

modified their NCIC query protocols so the FC is alerted when a law enforcement official's NCIC inquiry returns a watchlist hit. The TSC intends to incorporate FCs into the process more fully to ensure the FCs are made aware of encounters and have the opportunity to add value in appropriate circumstances. In another effort to integrate the FCs' critical skill set into the terrorist screening process, the TSC has initiated a pilot project in which portions of the TSDB will be provided to the New York Police Department (NYPD).

b. What role should they play in the future?

Response:

The FCs need to become formally involved in the encounter process. While individual FCs have made efforts to ensure they are notified, a more standardized approach needs to be taken by the TSC. The TSC Concept of Operations, which is scheduled to be completed in the late spring of 2008, is being refined to more clearly provide for FC integration into the terrorist screening process, including the adoption of a real-time notification process in which FCs are alerted to encounters in their areas of responsibility when they occur. As discussed above, FCs will receive real-time notification of encounters with known or appropriately suspected terrorists and will have access to much of the TSDB and to relevant DOJ and DHS systems. This will eliminate or substantially reduce the number of unreported encounters with known or appropriately suspected terrorists, facilitating more effective, efficient, and timely analysis, information flow, and intelligence development, including the development of more comprehensive analytical products to be used throughout the law enforcement and intelligence communities. The TSC will continue to provide direct phone support to local law enforcement and to the FCs. As the information sharing environment matures, TSC information will be shared with FCs according to protocols currently being developed.

c. Has the Terrorist Screening Center developed guidance with respect to the use of the terrorist watch list (or its subsets) by fusion centers?

Response:

To date, the TSC has not directly provided to FCs copies of terrorist watchlists or subsets thereof, though the FCs do have access to much of the information contained in the TSDB through the NCIC and the Treasury Enforcement Communications System, where available. In addition, several other DOJ and DHS systems will have this information in their data sharing systems, and these systems will be shared with users in the FCs. As noted above, however, the TSC is developing a pilot project to provide a watchlist subset to the NYPD. This may serve as a prototype by which a similar data set will be provided to FCs.

2. Please provide detailed statistics on the sources for the nominations in the Terrorist Screening Database (TSDB), including the number of records created as the result of actions by each nominating agency (e.g. CIA, NSA, DIA, DHS, FBI, Department of State), for all current TSDB records and for records created in FY 2007. (If necessary, these statistics may be transmitted to the Committee in a sensitive or classified format.)

Response:

Based on the information contained in the TSDB, the TSC can only determine whether a nomination is derived from the FBI or from another government agency, since the TSC does not categorize Other Government Agency (OGA) information by specific agency. Of the approximately 906,200 records contained in the TSDB, approximately 110,200 are FBI derived and approximately 796,000 are OGA derived. As the collector of international terrorism nominations, it is possible that the National Counterterrorism Center (NCTC) may be able to provide the additional detail requested.

Questions Posed by Senator Akaka

3. As of May 2007, the terrorist watch list had more than 750,000 records, and that number now is approximately 860,000. Just over three years ago, there were approximately 150,000 records in the watch list, and the list is growing by approximately 20,000 records per month.

With such rapid growth, I am concerned that many people with no connection to terrorism are being added to the list. This can lead to innocent people being detained at airports or by police, denied visas, or turned back at border crossings without reason. Also, extra names lead to more misidentifications, which increase costs and distract anti-terrorism and law enforcement officials from focusing on real threats.

a. Under Homeland Security Presidential Directive 6, the Terrorist Screening Center (TSC) is directed to "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." What specific criteria are used to assess whether someone is "appropriately suspected" of ties to terrorism within that definition?

Response:

The TSC has published guidance on watchlist nominations that instructs agencies to evaluate the "totality of information" in determining if an individual meets the "known or appropriately suspected" standard from Homeland Security Presidential Directive (HSPD) 6. In conducting this review, the reviewer relies on his or her own experience, the available facts, and rational inferences from those facts

(including the individual's past conduct, current actions, and credible intelligence concerning future conduct). In considering the totality of information, the reviewer is to evaluate the quality of the underlying derogatory information by considering both the specificity of the information and the reliability of the source(s).

While the TSC's guidance includes a non-exclusive list of specific types of conduct that would typically warrant watchlisting, generally a "known terrorist" is one known to be involved in activities constituting terrorism or activities in preparation for or related to terrorism, and an "appropriately suspected terrorist" is one who is suspected of having engaged in such activities under appropriate guidelines. For example, the Attorney General's Guidelines for National Security Investigations and Foreign Intelligence Collection provide the parameters under which the FBI can open a preliminary or full international terrorism investigation. If these criteria are met and an international terrorism investigation is opened, the subject of the investigation is presumptively deemed a "suspected terrorist" and may therefore be watchlisted in the TSDB.

Additionally, in order for the TSC to "maintain thorough, accurate, and current information" on known and suspected terrorists, the TSC has developed quality control measures that provide for the appropriate review of records maintained in TSC systems. These measures seek to ensure that outdated or incorrect information is culled from these records so the information received by the agencies depending on them is both accurate and current.

b. When a person on the watch list is encountered, questioned, and either released or permitted to enter the country rather than detained or arrested, is the information obtained used to review whether it is appropriate for that person to remain on the watch list?

Response:

When an individual listed in the TSDB is positively identified during an encounter with law enforcement, the TSC's Encounter Management Application assembles relevant information, including the facts and circumstances of the encounter, in an "encounter packet," which is then reviewed by the TSC's Tactical Analysis Unit. This review includes an assessment of whether the individual is appropriately watchlisted, and if watchlisting appears unwarranted for any reason a quality assurance ticket is issued and the record is referred for additional review. If this further review determines that continued watchlisting is unwarranted, a process exists to have the record removed from the TSDB

c. On average, how many records does the TSC remove from the watch list each month?

Response:

Since the inception of the TSC, a total of 163,937 records have been removed from the TSDB. The TSC removed 76,802 records between April and October 2007 during an internal records review, an average of 10,971 records per month.

4. The TSC and Department of Homeland Security (DHS) are working to finalize guidelines for private sector entities to use the watch list to screen critical infrastructure employees. As Mr. Rosenzweig's testimony highlighted, critical infrastructure employers come from a wide variety of sectors, including agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry and hazardous materials, postal and shipping, and national monuments and icons. Greater dissemination of the watch list information poses serious privacy concerns.

a. Please describe in detail what safeguards exist to protect private information in the watch lists that is being shared outside of the federal government.

Response:

The TSC and DHS are currently working to develop the means by which private sector entities can conduct TSDB terrorist screening checks securely, protecting this sensitive information. It is currently envisioned that private sector entities will not be given a copy of the TSDB, but will instead be invited to provide names to DHS, which will forward these names to the TSC for vetting.

Because DHS is the lead agency for developing further policy and procedures with respect to private sector screening, that agency may be able to provide additional information in response to this inquiry.

b. What entities currently have access to the watch lists?

Response:

The TSC currently provides to the Transportation Security Administration the No-Fly list and Selectee list for distribution only to those airlines that travel into, out of, or within the United States. It is not envisioned that any other private sector entities will be given access to the TSDB.

As noted above, because DHS is the lead agency for developing further policy and procedures with respect to private sector screening, that agency may be able to provide additional information in response to this inquiry.

c. What entities will have access when the guidelines are finalized?

Response:

As noted above, because DHS is the lead agency for developing further policy and procedures with respect to private sector screening, that agency may be able to provide information in response to this inquiry.

5. The Government Accountability Office (GAO) report released in conjunction with this hearing states that the State Department has approached all visa waiver countries and two non-visa waiver countries with a proposal to exchange terrorist screening information. Your testimony states that six nations have signed such information sharing agreements with the United States. What are the principal barriers to negotiating additional agreements?

Response:

While various U.S. Government agencies already share terrorist screening information with visa waiver countries through long-established liaisons, this information sharing is being enhanced and formalized through bilateral agreements. The abilities of various countries to reach these agreements consistent with their own laws may vary, but the execution of six agreements is indicative of the importance that both the United States and other countries place on institutionalizing terrorist screening information sharing.

HSPD 6 tasks the Department of State with leading the effort to negotiate terrorist screening information sharing agreements with foreign partners. The TSC has a full-time Department of State representative on staff to facilitate the development of these agreements with our foreign partners. Within the Department of State, this responsibility rests with the Bureau of Consular Affairs, Office of Policy Coordination and Public Affairs, which may be able to provide additional information in response to this inquiry.

6. Your written testimony states that the TSC participates in a working group to identify how to better use biometric data to enhance security screening.

a. Is biometric data currently incorporated into the records where it is available? For example, is biometric data included in watch list records when someone on the watch list submits fingerprints and photographs with a visa application?

Response:

Currently, the TSDB contains limited biometrics and biometric indicators. In the example given, the photograph would be stored in the record but the fingerprints would not be; the fingerprints would be placed on the watchlist of DHS's

Automated Biometric Identification System (the IDENT fingerprint system) and the fingerprints of visa applicants, applicants for admission to the U.S., individuals seeking immigration or credentialing benefits, and those encountered while attempting illegal U.S. border crossings would be checked against this DHS system. The TSC recognizes the importance of using biometrics in the terrorist screening process and has been working with its interagency partners to develop the capability to store and disseminate the biometric identifiers used by government screening organizations and to otherwise integrate biometrics into the terrorist watchlisting process, recognizing the need to employ appropriate safeguards to protect the privacy and civil liberties of those involved.

b. If not, is TSC moving forward with plans to incorporate biometric data into watch list records?

Response:

The TSC has been working through the NCTC's Interagency Coordination Group on identity management and biometrics to develop a plan to integrate biometrics into the terrorist watchlisting process. The interagency subgroup on interoperability has proposed a data exchange model under which the TSC will store biometric data (or pointers to the actual biometric data) in the TSDB and will provide this information to its screening customers.

7. An October 2007 article in the Los Angeles Times reported that the Identity Project, a privacy-rights organization, obtained Customs and Border Protection (CBP) records containing information about such things as the book that someone carried or a passenger's profession.

a. Was this information incorporated in the watch list records or in some other database that CBP uses? If the latter, which database?

b. Is this type of information incorporated in watch list records and, if so, why?

Response to subparts a and b:

Non-identifying information, including information regarding a traveler's reading materials, is NOT incorporated into the TSDB. The TSDB contains only the watchlisted person's identifying information, such as name, date of birth, passport number, and driver's license number. A person's profession may be included in the TSDB as information that may help to identify the proper individual during screening or to rule out a person who may merely have the same or a similar name.

When additional identifying data on a watchlisted person is obtained during screening by CBP or other agencies, it is passed to the NCTC for possible inclusion in the Terrorist Identities Datamart Environment and, if appropriate, passed to the TSC for inclusion in the TSDB. By enhancing the identifying information in the watchlist, it becomes easier for government screeners to distinguish watchlisted persons from those who may merely have the same or a similar name, minimizing the inconvenience to the traveling public. The FBI and TSC are not able to address what information CBP retains in its data systems.

Question Posed by Senator Warner

8. We are privileged in the Commonwealth of Virginia to have the National Ground Intelligence Center, and I visit quite frequently, and they are on the cutting edge of the biometrics. And somehow it has come to my attention - I am not sure of the accuracy - that the Terrorist Screening Center presently does not have a number of these capabilities. Are you leveraging it from other areas to incorporate it? Are you planning to get it? Or do you think it should be made a part of the program?

Response:

The National Ground Intelligence Center (NGIC) is a cutting-edge operational unit that supplies soldiers in the field with actionable information related to biometric match reports taken from biometric signatures captured in their theater of operations. The TSC has a mission similar to that of the NGIC, as the TSC supplies real-time operational information to screening organizations upon their encounters with screened individuals. Encounter information is also shared with appropriate law enforcement personnel who can benefit from the details of the encounter.

As indicated in response to Question 6, above, the TSDB currently contains limited biometrics and biometric indicators. The TSC recognizes the importance of using biometrics in the terrorist screening process and has been working with its interagency partners to develop the capability to store and disseminate the biometric identifiers used by government screening organizations and to otherwise integrate biometrics into the terrorist watchlisting process. For example, the TSC has been collaborating closely with the Department of Defense, including the NGIC, on interagency efforts. As more robust biometric capabilities are designed for government use, the TSC will continue to look at successful biometric implementations, such as the accomplishments of the NGIC, to identify "best practices."

Question Posed by Senator Carper

(The following question originally was posed to DHS witness
Paul Rosenzweig but was referred by DHS to the TSC for response)

9. You (Ms. Larence) note in your testimony that the decision on whether or not to place someone on the watch list is often somewhat subjective. There are individuals apparently on the watch list who are terrorists, suspected terrorists, but there are also some there who are simply being investigated for some other reason. My question is: Are there clear enough rules out there for determining who should and who should not be on the list and who ultimately makes the decision and what does he or she base their decision on? That is not a question for you (Ms. Larence). You are the one who made the point. I believe that would be a question, I think, for the Secretary, and if you would respond to that for the record, I would be grateful.

Response:

Please see the response to Question 3a, above.

Question#:	1
Topic:	guidelines
Hearing:	Watching the Watch List: Building an Effective Terrorist Screening System
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Post-Hearing Questions for the Record
Submitted to Paul Rosenzweig
From Senator Joseph I. Lieberman

Question: It is our understanding that the Department of Homeland Security is in the process of developing guidelines for the use of the terrorist watch list for private sector purposes, such as the screening of workers employed in critical infrastructure sectors.

Is this correct? If so, by what date do you anticipate that these guidelines will be completed? In what form will they be promulgated (e.g. as a proposed or interim rule, or as an internal directive, or in some other form)?

What are some of the core factors and criteria that the Department is considering in its development of these guidelines? What do you believe are appropriate criteria for the use of the terrorist watch list in screening workers in critical infrastructure sectors? Is the relatively criticality of a particular sector or a certain job position one factor that will be considered?

When, if ever, do you believe that the terrorist watch list should be used as a tool in the adjudication of employment decisions in the private sector?

In cases where DHS determines that there is a private sector role for the terrorist watch list, by what means should it be shared with the private sector? What steps will be necessary (or are used today) to protect the terrorist watch list?

Is the terrorist watch list being used (or is it anticipated that it will be used) as part of the screening and credentialing activities under the Transportation Worker Identification Credentialing (TWIC) program?

ANSWER:

As outlined in Homeland Security Presidential Directive (HSPD)-6, DHS is drafting guidelines to establish basic mechanisms and parameters for private sector entities to request terrorist watch list screening for individuals with recurring unescorted access to sensitive areas of their facilities or premises. This screening will be strictly voluntary.

Relative criticality of a particular sector and the job responsibilities and access of the individuals to be screened will be factors considered when approving or denying a screening request from a private sector entity. The Department is considering factors such as:

Question#:	1
Topic:	guidelines
Hearing:	Watching the Watch List: Building an Effective Terrorist Screening System
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

- the extent to which each requesting private sector entity comprises critical infrastructure, and
- the access of persons associated with the entity and their ability to cause harm.

For these purposes, critical infrastructure is defined consistent with HSPD 7, the Homeland Security Act (6 U.S.C. 101(9)), and the USA PATRIOT Act (42 U.S.C. 5195c(e)), as systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Privacy and civil liberties considerations figure prominently in our approach. Private sector companies must demonstrate in their screening requests that employees have been notified of the screening and have consented to it. Each company must also ensure that adequate controls are in place to protect privacy, security of information, and the civil rights and liberties of all individuals to be screened.

DHS does not advocate the sharing of the terrorist watch list with the private sector, but supports access to screening through federal, state or local government screening initiatives. Under the Private Sector Screening Guidelines, no private sector entity will have access to the terrorist watch list and DHS will not directly provide the screening results to private sector entities. As such, DHS does not view the terrorist watch list as a tool to be used in the adjudication of employment decisions. Accordingly, to participate in the screening program, private sector entities must certify that they will not take adverse action against any employee solely as a result of the screening process. DHS will coordinate with the Terrorist Screening Center to provide any confirmed watch list matches to the appropriate law enforcement agency. The law enforcement agency will determine the appropriate response. DHS will provide support to the law enforcement agency if requested.

The TWIC program screens enrollees against the terrorist watch list.

Question#:	2
Topic:	fusion centers
Hearing:	Watching the Watch List: Building an Effective Terrorist Screening System
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: What role do fusion centers play today as part of the overall watch listing system? What role should they play in the future? Has the Department of Homeland Security developed guidance with respect to the use of the terrorist watch list (or its subsets) by fusion centers?

Answer: The Department of Homeland Security is working closely with the Terrorist Screening Center (TSC) to develop a stronger link to the State fusion centers. The TSC, in coordination with DHS and the FBI, is in the process of developing a Concept of Operations document to define specifically the role of the fusion centers in the federal watch listing and encounter processes. Currently, terrorist related leads identified from the fusion centers are passed to the FBI through the Joint Terrorism Task Forces (JTTF) for review and nomination to the watch list. Fusion center access to the Terrorist Screening Database (TSDB) is primarily through the National Crime Information Center (NCIC) system, a database that houses all wants and warrants, and all possible matches include instructions to contact the TSC for identification support and coordination with the FBI.

Question#:	3
Topic:	HSPD-11
Hearing:	Watching the Watch List: Building an Effective Terrorist Screening System
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: HSPD-11 required the submission of a strategy and implementation plan to enhance the effectiveness of terrorist-related screening activities. It is our understanding that a strategy and implementation plan were produced by DHS but never approved by the Homeland Security Council. Is this accurate? At a House Homeland Security Committee hearing on November 8, 2007, DHS Screening Coordination Office Director Kathy Kraninger indicated that efforts are now underway to comply with this provision of HSPD-11, and produce a revised HSPD-11 strategy and implementation plan. Is this also accurate? If so, please provide a detailed timeline for this work (including expected completion date) and describe the key ways in which you expect that the strategy and implementation plan will differ from the 2004 documents. If you are not prepared to answer this last part of the question at this time, please indicate when you will be able to answer it.

Answer:

In partnership with the Homeland Security Council DHS has coordinated an updated HSPD-11 strategy for comprehensive terrorist-related screening procedures. This report reflects revisions to the overarching strategy outlined in the 2004 reports and an update on programs aimed at enhancing terrorist-related screening capabilities. This updated strategy report is currently under interagency review. It is anticipated that the report will be finalized for delivery to the President in January 2008.

Question#:	4
Topic:	Secure Flight
Hearing:	Watching the Watch List: Building an Effective Terrorist Screening System
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: With respect to the Secure Flight program, how will DHS deal with the inevitable misidentifications and appeals for redress? What safeguards is the Department including in the development of Secure Flight to minimize misidentification, while still maintaining the security of the aviation system?

The Administration requested $53 million for Secure Flight in FY08, a dramatic increase for the program. And on November 6, 2007, the White House requested an additional $21 million for FY 2007 (above the $53 million request) as part of its amendments to the FY 2007 budget request. What purposes will these additional funds serve?

The Department's current timeline for Secure Flight envisions the program becoming fully operation in 2010, leaving passenger prescreening in the hands of the airlines for 2-3 more years. Has DHS considered expediting implementation of Secure Flight?

Answer:

The President's Amended FY 2008 Budget Request included $74 million for Secure Flight, an increase of $21 million above the previous FY 2008 request of $53 million. Congress provided $50 million in FY 2008 funds and granted DHS the authority to transfer up to $24 million into the program with Congressional approval.

With the $50 million, DHS will minimize misidentifications by conducting extensive testing of the watch list matching algorithms used to identify potential threats to aviation. This testing will be performed prior to assuming the responsibility for prescreening passengers from air carriers. DHS will continue to refine the algorithms on an ongoing basis once the system is fully operational. Additionally, DHS will staff a 24/7 service center to resolve ambiguous matches and work with airlines to immediately clear any misidentifications that do occur. Finally, the public will be able to appeal for redress through the DHS TRIP program operated by the DHS Office of Appeals and Redress. Because DHS is assuming responsibility for passenger vetting from the airlines, the Department will be able to more effectively and consistently make use of the list of individuals who have been cleared by DHS TRIP.

The additional $24 million would accelerate the implementation schedule for Secure Flight. These funds would allow DHS to more quickly establish the Secure Flight Service Center and expedite the acquisition of the infrastructure and services needed to implement the program. DHS would be able to accelerate the Secure Flight schedule by one year, end parallel testing with the air carriers, and assume sole responsibility of passenger prescreening in by 2010.

Question#:	5
Topic:	TRIP
Hearing:	Watching the Watch List: Building an Effective Terrorist Screening System
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: On November 7, 2007, USA Today reported that DHS has received more than 15,000 requests for watch list redress since February 2007 through the Traveler Redress Inquiry Program (TRIP), and that the Department has been "unable to meet its goal of resolving cases in 30 days," instead taking 44 days to process a complaint.

What are the reasons why TRIP has been unable to meet its goal of resolving cases in 30 days? Please provide a detailed explanation as to whether and how budgetary, legal, technological, procedural, and other factors play a role in the Department's inability to meet its objectives.

Also, please provide a detailed explanation of the steps that are taken for each case that is submitted to TRIP for redress, including a detailed flowchart of the process.

Answer: The Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP), operated by the DHS Office of Appeals and Redress, is aggressively pursuing its goal of resolving redress cases within 30 days. To achieve this goal, the DHS TRIP Program Office is staffed with Federal employees on site, Federal employees off-site, and contract staff. The breakout is as follows: 8 Federal full-time equivalent (FTE) personnel from the Transportation Security Administration (TSA) on site; 1 FTE from U.S. Customs and Border Protection (CBP) detailed to be on site; 5.25 FTE personnel from various components who work as liaisons within their agencies and attend weekly meetings on site; and 4 contractor employees on site. The expenditures for fiscal (FY) 2007 were $930,000; however, this figure does not include personnel or real estate costs. Due to our communications outreach efforts, DHS TRIP has received a higher number of requests than originally anticipated. With this in mind, the DHS TRIP Program Office has requested an additional two contractors based on current volumes. DHS TRIP is also reviewing technological improvements that can be made to reduce the amount of manual intervention (such as document verification) and streamline redress request processing (i.e., sharing of redress requestor data with component Information Technology systems).

Another factor for the length of time required to resolve requests for redress is the amount of research involved in reviewing and resolving redress requests by the component agencies within DHS TRIP. The TRIP components are TSA, CBP, U.S. Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), U.S. Visitor and Immigrant Status Indicator Technology, DHS Civil

Question#:	5
Topic:	TRIP
Hearing:	Watching the Watch List: Building an Effective Terrorist Screening System
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Rights and Civil Liberties, DHS Privacy, and the U.S. Department of State. Depending on the traveler's concerns and the records that may be involved in the investigation, multiple component agencies may need to review the case and possibly involve Federal, State or local law enforcement agencies, or refer the case to the U.S. Terrorist Screening Center (TSC) for resolution.

A traveler may apply to TRIP online at www.dhs.gov/trip or by mail. When applying online, the traveler is instructed to print the DHS Traveler Inquiry Form acknowledgement page, sign it, and send it by mail or e-mail along with copies of identity documents to TRIP. When applying by mail, the traveler is requested to complete the DHS Traveler Inquiry Form and mail or e-mail the form along with copies of identity documents to TRIP.

When the DHS TRIP Program Office receives a traveler inquiry, the intake team reviews the inquiry for completeness, enters or updates the data in the redress management system, and assigns the inquiry to the appropriate component or components for investigation. TRIP cases are categorized and assigned to components based on the traveler's concerns. The DHS Traveler Inquiry Form includes a checklist of travel-related issues. TRIP assigns a case to a component or components according to the issues that the traveler selects along with any narrative the traveler may include in the form.

The component agencies review the traveler's documents and research any related records. If the component agencies determine that the traveler is misidentified, the component agencies correct or update records as necessary. If the traveler's information is an exact match to the terrorist watch lists or other records used by TRIP components, DHS TRIP refers the redress request to the TSC for resolution. Once the review process is complete, the assigned component agency, or the lead component agency in a multiple-concern inquiry, will close the case and prepare a DHS TRIP response letter to the traveler.

A flow chart entitled *Traveler Redress Inquiry Program (TRIP) Process Map* is available for your review. However, it has been marked as Sensitive Security Information (SSI) and as such special handling procedures apply to its storage and transmission. DHS will provide this SSI document to the Committee under separate cover.

Question#:	6
Topic:	TSC
Hearing:	Watching the Watch List: Building an Effective Terrorist Screening System
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Post-Hearing Questions for the Record
Submitted to Paul Rosenzweig
From Senator Daniel K. Akaka

Question: The Terrorism Screening Center (TSC) and Department of Homeland Security (DHS) are working to finalize guidelines for private sector entities to use the watch list to screen critical infrastructure employees.

As your testimony highlighted, critical infrastructure employers come from a wide variety of sectors, including agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry and hazardous materials, postal and shipping, and national monuments and icons.

Greater dissemination of the watch list information poses serious privacy concerns.

Please describe in detail what safeguards exist to protect private information in the watch lists that is being shared outside of the federal government.

What entities currently have access to the watch lists?

What entities will have access when the guidelines are finalized?

Answer:

Under the Draft Private Sector Screening Guidelines, no private sector entities will have access to the terrorist watch list. Instead, private sector entities approved for screening will submit to DHS a minimal amount of personal data for individuals to be screened against the watch list. In drafting the guidelines, the benefit to national security has been carefully weighed against the impact to the privacy of those to be screened. Several safeguards have been incorporated into the draft guidelines:

Limiting the Population to be Screened:
Only private sector entities that have been approved for screening based on having a substantial bearing on homeland security will be able to submit personally identifiable information (PII) to the Federal Government. In requesting screening, these entities must demonstrate that the population to be screened has access to critical infrastructure and the ability to cause harm. This population may include new hires, employees, contractors, and vendors with recurring, unescorted access to buildings or premises within the private sector

Question#:	6
Topic:	TSC
Hearing:	Watching the Watch List: Building an Effective Terrorist Screening System
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

entity. Blanket requests for screening all individuals associated with an entity regardless of their access or ability to cause harm will not be approved.

Minimizing and Protecting Personally Identifiable Information (PII):
In addition to the criteria described above, companies requesting screening must also demonstrate that individuals to be vetted have consented to the screening and that safeguards are in place to protect PII. Once a screening request has been approved, the private sector entity will be assigned a control number, which it must use to submit PII. Data must be submitted in a secure format using a secure method. Only data elements required to ensure effective watch list screening will be required. DHS may randomly select a small percentage of names to request additional information for quality assurance purposes. To participate in the screening program, private sector entities must certify that they will not take adverse action against any employee solely as a result of these requests or the screening process in general. DHS will destroy/delete the information collected on individuals that were not near matches to the watch list within 7 days after the screening is completed. Information for near or possible matches will be temporarily retained.

Law Enforcement Response:
DHS will not provide screening results to private sector entities. DHS will coordinate with the Terrorist Screening Center to provide confirmed watch list matches to the appropriate law enforcement agency, which in most cases will be the FBI. The law enforcement agency responsible for the terrorist watch list record will determine the appropriate response.

Outside of the commercial aviation industry, no other private sector company has access to any part of the terrorist watch list. Airline operators have access to the No Fly and Selectee lists to enable them to interdict potential threats to commercial aviation. Private sector entities do not and will not have access to the watch list under the private sector screening guidelines.

Question#:	7
Topic:	agreements
Hearing:	Watching the Watch List: Building an Effective Terrorist Screening System
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: The Government Accountability Office (GAO) report released in conjunction with this hearing states that the State Department has approached all visa waiver countries and two non-visa waiver countries with a proposal to exchange terrorist screening information. Mr. Boyle's testimony states that six nations have signed such information sharing agreements with the United States.

What are the principal barriers to negotiating additional agreements?

Answer:

Various agencies of the U.S. Government share terrorist screening information with all Visa Waiver countries through long-established liaisons. This sharing is being enhanced and formalized by bilateral sharing agreements. Homeland Security Presidential Directive-6 tasks the Department of State with leading efforts to negotiate agreements to exchange terrorist screening information with foreign partners. Within the Department of State, this responsibility has been delegated to the Bureau of Consular Affairs, Office of Policy Coordination and Public Affairs (CA/P). Specific country abilities to formalize agreements within their own laws vary, but the signing of six agreements in 1 year is a significant sign of the importance that both the U.S. and other countries place on institutionalizing terrorist screening information-sharing. The Department of State is better equipped to respond further to this question.

Question#:	8
Topic:	biographic records
Hearing:	Watching the Watch List: Building an Effective Terrorist Screening System
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: Your written testimony states that the Screening Community is "focused on aligning biometric watch list information in a more automated fashion with biographic records to provide even more efficient screening capabilities."

Please describe in detail what this would entail.

Is biometric data currently incorporated into the records where it is available? For example, is biometric data included in watch list records when someone on the watch list submits fingerprints and photographs with a visa application?

Would existing technology permit automated incorporation of biometric information into the watch list records?

If so, do TSC and DHS plan to move forward on implementing a system that uses automated incorporation of biometric information into the watch list records?

Answer:

Currently, the Terrorist Screening Database (TSDB) has limited biometrics and biometric indicators stored in the database. In the example given, the photograph would be stored inside of the record but the fingerprints would not. The Terrorist Screening Center recognizes the criticality of using biometrics in the terrorist screening process, and has been working through the National Counterterrorism Center's (NCTC) Interagency Coordination Group (ICG) on identity management and biometrics to integrate biometrics into the terrorist screening process. The TSC and DHS recognize the vast and necessary potential in biometrics, and are actively working with our interagency partners to develop this capability to store and disseminate the biometric modalities used by USG screening organizations.

Question#:	9
Topic:	Identity Project
Hearing:	Watching the Watch List: Building an Effective Terrorist Screening System
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: An October 2007 article in the Los Angeles Times reported that the Identity Project, a privacy-rights organization, obtained Customs and Border Protection (CBP) records containing information about such things as the book that someone carried or a passenger's profession.

Was this information incorporated in the watch list records or in some other database that CBP uses? If the latter, which database?

Is this type of information incorporated in watch list records and, if so, why?

Answer: Information relevant to the enforcement of U.S. laws discovered during a CBP Officer's secondary examination is included in the officer's Secondary Inspection Log maintained within the Treasury Enforcement Communications System (TECS). During subsequent travel, CBP officers would be alerted that a previous secondary exam had occurred. It is up to the CBP Officer performing the screening to determine whether there is a need to access the specific details uncovered during the past exam and whether those details are relevant to the present encounter. If information collected during a CBP Secondary exam is deemed to have a possible nexus to terrorism, CBP coordinates with FBI and ICE accordingly. It is important to note that a subject would not be watch listed based solely on the books carried or his/her profession.

Question#:	10
Topic:	Secure Flight - 2
Hearing:	Watching the Watch List: Building an Effective Terrorist Screening System
Primary:	The Honorable Thomas R. Carper
Committee:	HOMELAND SECURITY (SENATE)

Post-Hearing Questions for the Record
Submitted to Paul Rosenzweig
From Senator Thomas R. Carper

Question: First of all, to the Secretary, this is a question on Secure Flight, a system called Secure Flight. I understand that the Department of Homeland Security has a system in the works called Secure Flight that at least some believe will more accurately screen individuals at the airports against terrorist watch lists, and I am going to ask you to answer for the record. Explain to us how Secure Flight will reduce false positives and other screening issues that have been discovered over the years. And, further, I would ask when do you believe the system will be up and running and what is your department doing to help airlines improve their screening processes in the meantime?

Answer: As designed, Secure Flight will use automated and manual methods to consistently match passenger information to government watch lists. Additionally, in order to provide redress to individuals, Secure Flight will receive the approved redress request information from the Department of Homeland Security Traveler Redress Inquiry Program and use it in the watch list matching process to clear passengers who have been previously misidentified, thus reducing the number of false positives.

Secure Flight has incorporated a comprehensive end-to-end approach to testing into the work plans for program implementation. There will be appropriate system testing, communications testing, interface testing, and other technical testing performed as the final system is built. Where appropriate, the Transportation Security Administration (TSA) testing will be done in conjunction with the aircraft operators. TSA is planning to begin initial benchmark testing, with a limited number of aircraft operators, in December 2007. Benchmark testing is an important step in the development and implementation of Secure Flight and will help with the analysis of false positive and false negative rates. Conducting benchmark testing using a sampling of passenger data from airlines will allow validation of the program's watch list matching results with current aircraft operator matching results, thus enabling a refinement of the automated algorithms to appropriate rates of performance.

The final phase of testing will be parallel testing with aircraft operators. After the final rule for the Secure Flight program is published, Secure Flight will operate in parallel with each aircraft operator and conduct extensive analyses and comparisons of system performance under full volumes prior to assuming responsibility for watch list matching from the aircraft operators. The Secure Flight implementation strategy is to implement all aircraft operators over time in a parallel mode. TSA will assume watch list matching functions for domestic flights from aircraft operators on a rolling basis and is scheduled to begin in the second quarter fiscal year 2009.

Testing phases such as these are intended to help facilitate a successful implementation of the program, and are also required to comply with Congressional requirements that the program meet appropriate performance levels.

Question#:	11
Topic:	private sector
Hearing:	Watching the Watch List: Building an Effective Terrorist Screening System
Primary:	The Honorable Mark Pryor
Committee:	HOMELAND SECURITY (SENATE)

Post-Hearing Questions for the Record
Submitted to Paul Rosenzweig
From Senator Mark L. Pryor

Question: Whose responsibility is it to incorporate the private sector into the watch list screening system? Is DHS shepherding this effort? If so, is it coordinated through the Office of Critical Infrastructure Protection or the Office of the Private Sector? If the onus is on the private sector companies themselves, are actions coordinated with watch lists through the critical infrastructure sector coordinating councils or through the initiative of individual companies? Is anyone accountable for making sure this happens?

Answer:

The Screening Coordination Office (SCO) within DHS is drafting the Private Sector Screening Guidelines and coordinating the development of this screening program to support the National Protection and Program Directorate's Office of Infrastructure Protection (IP). IP will be the DHS lead office once the guidelines become operational. The guidelines will establish basic mechanisms and parameters for private sector entities to request terrorist watch list screening for individuals with recurring unescorted access to sensitive areas of their facilities or premises. This screening program will apply to private sector entities that have a substantial bearing on homeland security and are not required by other regulatory programs to conduct screening.

Many private sector entities are subject to regulated security and screening regimes such as segments of the transportation sector. The Private Sector Screening Guidelines are designed to provide a terrorist watch list screening mechanism for non-regulated entities on a voluntary basis. DHS has discussed the guidelines with the Sector Coordinating Councils, which will continue to be engaged as the program evolves. DHS IP is responsible for ensuring the program meets security needs.

Question#:	12
Topic:	timeframe
Hearing:	Watching the Watch List: Building an Effective Terrorist Screening System
Primary:	The Honorable Mark Pryor
Committee:	HOMELAND SECURITY (SENATE)

Question: Is there a timeframe in which DHS hopes to issue guidelines to the private sector on the use of watch list records in the hiring of employees who deal with critical infrastructure? Are there any barriers to issuing such guidelines that would require Congressional action?

ANSWER: DHS plans to publish the draft Private Sector Guidelines and associated supporting documentation in the *Federal Register* in the spring of 2008. There are no known or anticipated barriers to issuing Private Sector Guidelines that require Congressional action.

Question#:	13
Topic:	redress
Hearing:	Watching the Watch List: Building an Effective Terrorist Screening System
Primary:	The Honorable George V. Voinovich
Committee:	HOMELAND SECURITY (SENATE)

Post-Hearing Questions for the Record
Submitted to Paul Rosenzweig
From Senator George V. Voinovich

Question: In your testimony, you state that the Department's Traveler Redress Inquiry Program received over 21,000 requests for redress between February and October of 2007, but many of these are on hold, waiting for the travelers to submit the required documentation. In Mr. Fine's testimony, however, he notes that a redress review on the part of the Terrorist Screening Center averages 67 days. Mr. Fine suggests that the delay is not linked to the individual, but rather to problems with the nominating agencies or in finalizing a determination. How is the Department's process of redress different from the Terrorist Screening redress process? Should this process become more formalized and uniform for all participating agencies?

Answer:

Redress requests start with the screening agency. Whenever a person requesting redress is a close match to the terrorist watch list, there are always two levels of review. At the first level of review, through the DHS Traveler Redress Inquiry Program (DHS TRIP), DHS assesses the nature of the complaint and the potential watch list relevance. If the individual requesting redress has been misidentified or the request is unrelated to the watch list, DHS takes appropriate action to resolve the issue and no referral to the Terrorist Screening Center (TSC) is made. On the other hand, if the traveler is a match or a close match to the watch list, DHS refers the request to TSC Redress for final determination and, where applicable, adjudication. The vast majority of DHS TRIP inquiries are not actual or close matches to the terrorist watch list and are not referred to the TSC. The DHS TRIP Program is operated by the DHS Office of Appeals and Redress.

Once DHS refers a case to TSC, the second level of review begins pursuant to a multi–agency memorandum of agreement (MOA) signed earlier this year. The MOA outlines the responsibilities among agencies and their roles in resolving a redress request. DHS and TSC continue to work together to refine the redress process and the steps that are taken to facilitate communication among agencies.

Question#:	14
Topic:	international information sharing
Hearing:	Watching the Watch List: Building an Effective Terrorist Screening System
Primary:	The Honorable George V. Voinovich
Committee:	HOMELAND SECURITY (SENATE)

Question: International cooperation and information sharing, particularly with nations in the Visa Waiver Program, could be vital to populating the terrorist watch list. To the extent possible, please discuss current agreements or negotiations with other countries which seek to increase the sharing and quality of information on the consolidated watch list.

ANSWER: Pursuant to Homeland Security Presidential Directive 6 (HSPD-6) the Department of State and the Terrorist Screening Center (TSC) have been tasked with obtaining foreign watch lists, including those of Visa Waiver Program (VWP) countries, for integration into the Terrorist Screening Database. The Department of Homeland Security (DHS) is an active participant in the interagency working group organized by the Department of State to manage the United States Government's (USG) equities in such negotiations. To date, this process has resulted in a number of agreements for the direct exchange of watch list information between the United States and VWP nations.

In addition, DHS has entered into negotiations to exchange related information, such as the biometrics of criminals and terrorists, and to advance cooperation in the areas of border management and identity fraud. These efforts further improve DHS's ability to screen those individuals seeking to travel to the United States for terrorist and criminal ties. Information obtained as a result of these improved capabilities may also support the further development of USG case-files about known or suspected terrorists. DHS will continue to seek such cooperative arrangements, including as part of the security enhancements, to the VWP required by the 9/11 legislation.

Finally, the DHS component attachés frequently exchange information with foreign counterparts to support ongoing investigations. This may occur both through formal and informal mechanisms. Known and Suspected Terrorist information obtained as a result of this work may be shared within the USG through procedures established by TSC and the National Counterterrorism Center.

Question#:	15
Topic:	cost-benefit
Hearing:	Watching the Watch List: Building an Effective Terrorist Screening System
Primary:	The Honorable George V. Voinovich
Committee:	HOMELAND SECURITY (SENATE)

Question: Secretary Chertoff expects the Department to assume responsibility for airline passenger screening in late 2008, with TSA matching passengers to the consolidated watch list. Please describe what, if any, cost-benefit analysis was done in making this adjustment.

Answer: As part of the re-baseline of the Secure Flight program, an analysis of potential business models for the Secure Flight program was completed and included as part of the program's OMB300. As a result of this analysis, the current Secure Flight plan was deemed to provide the best value.

Question#:	16
Topic:	rules
Hearing:	Watching the Watch List: Building an Effective Terrorist Screening System
Primary:	The Honorable Thomas R. Carper
Committee:	HOMELAND SECURITY (SENATE)

Post-Hearing Questions for the Record
Submitted to Paul Rosenzweig
From Senator Thomas R. Carper

Question: You (Ms. Larence) note in your testimony that the decision on whether or not to place someone on the watch list is often somewhat subjective. There are individuals apparently on the watch list who are terrorists, suspected terrorists, but there are also some there who are simply being investigated for some other reason. My question is: Are there clear enough rules out there for determining who should and who should not be on the list and who ultimately makes the decision and what does he or she base their decision on? That is not a question for you (Ms. Larence). You are the one who made the point. I believe that would be a question, I think, for the Secretary, and if you would respond to that for the record, I would be grateful.

Answer:

The NCTC and the TSC have led multiple interagency efforts since 9/11 to ensure that the criteria for watch listing are clear, uniformly applied, and that questions as to whether watch listing is appropriate in a given scenario are resolved as they arise. Individuals who do not have a nexus to terrorism are specifically excluded from the watch list. It is important to note, however, that the criteria establish a minimum threshold. This was intentional.

To address one of the primary issues identified by the 9/11 Commission, the USG established a policy of more comprehensive information-sharing, rather than running the risk that information known to the USG was not provided to screening agencies. NCTC and TSC also conduct reviews of data to promote consistency and that the watch list is up to date. The TSC Nominations Unit (NDIU) receives all nominations from one of two sources: the FBI, which nominates domestic terrorism cases only (.05 percent of all nominations), and NCTC, which processes international terrorism subjects/nominations (99.95 percent of all nominations). NCTC receives and processes nominations from multiple agencies that encompass the International Terrorism (IT)/IC. Each one of those individual agencies, to include the FBI, applies its own criteria to intelligence to determine whether a subject is a known or appropriately suspected terrorist and determines whether that person should be sent to NCTC for watch listing processing. Upon receipt of the IT/IC nominations, NCTC will apply its specific criteria to each nomination to determine whether the subject should be labeled a KST and be entered into the Terrorist Identities Datamart Environment (TIDE). Upon entry into TIDE, the TSC will receive the daily nominations. At anytime during the nominations process, to include Quality Assurance, NDIU examines the derogatory information applied to each record and will determine

Question#:	16
Topic:	rules
Hearing:	Watching the Watch List: Building an Effective Terrorist Screening System
Primary:	The Honorable Thomas R. Carper
Committee:	HOMELAND SECURITY (SENATE)

whether the person is a known or suspected terrorist. On occasions when the derogatory information is determined to be insufficient, the TSC coordinates with NCTC to verify whether that record is appropriate for inclusion in the TSDB, and if necessary and possible, to obtain additional derogatory information.

During the nominations process, more stringent criteria are applied to comprise the No Fly and Selectee Lists. These criteria were established by the Homeland Security Council Deputies Committee on October 21, 2004, and derived from Title 18, USC, Sections 2331 and 2332b(g)(5)(b). At each step, analysts apply the provided derogatory information to the No Fly criteria to assess whether the record indicates possible "International Terrorism," "Domestic Terrorism," or a "Federal Crime of Terrorism." If parts of the derogatory information fit within these criteria, a subject could be included on the No Fly Lists. The criteria for the No Fly List are more stringent than the criteria for the Selectee List and are intended to isolate the most immediate threats to aviation.

○