



# Report on Effects on Privacy & Civil Liberties

DHS Privacy Office Report Assessing the Impact of the Automatic Selectee and No Fly Lists on Privacy and Civil Liberties as Required Under Section 4012(b) of the Intelligence Reform and Terrorism Prevention Act of 2004

*April 27, 2006*



**Homeland  
Security**



Report Assessing the Impact of the  
Automatic Selectee and No Fly Lists on  
Privacy and Civil Liberties as Required  
Under Section 4012(b) of the Intelligence  
Reform and Terrorism Prevention Act of  
2004, Public Law 108-458

Respectfully submitted  
Maureen Cooney  
Acting Chief Privacy Officer  
U.S. Department of Homeland Security  
Washington, DC

April 27, 2006

## I. Executive Summary

This report responds to Section 4012(b)(2) of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, P.L. 108-458, which requires the “Security Privacy Officer” of the Department of Homeland Security (DHS) to submit to Congress a report assessing the impact of the Automatic Selectee and No-fly (“Selectee” and “No-fly”) lists on privacy and civil liberties. In particular, the Privacy Office was asked to make recommendations for practices, procedures, regulations, or legislation necessary "to minimize adverse effects of [these lists] on privacy, discrimination, due process, and other civil liberties"; to discuss the implications of "applying those lists to other modes of transportation"; and to discuss the effect that the implementation of recommendations would have on "the effectiveness of the use of such lists to protect the United States against terrorist attacks".<sup>1</sup>

The No-fly list is a list of individuals who are prohibited from boarding an aircraft. The Automatic Selectee list is a list of individuals who must undergo additional security screening before being permitted to board an aircraft. Originally created and maintained by the Transportation Security Administration (TSA), No-fly and Selectee lists are now derived from the consolidated terrorist watch list maintained by the Terrorist Screening Center (TSC).<sup>2</sup> Two agencies of the Department of Homeland Security, TSA and Bureau of Customs and Border Protection (CBP), use the No-fly and Selectee lists for screening airline passengers. TSA is responsible for screening domestic airline passengers; CBP screens international passengers. CBP also uses these lists to screen cruise line passengers.

The terrorist watch list and No-fly and Selectee lists are useful tools for preventing terrorist activity that could endanger the safety of airline passengers and others. Understandably, the collection of personal information to create these tools may raise concerns about privacy and civil liberties. For example, to perform matching with reasonable quality and to correct mistakes, the entities that now use watch lists must collect personal information from everyone who travels by air or passenger ship, raising concerns that this information might be used inappropriately, particularly if adequate safeguards are not in place. Further, individuals who are mistakenly put on watch lists or who are misidentified as being on these lists can potentially face consequences ranging from inconvenience and delay to loss of liberty.

---

<sup>1</sup> This report focuses on privacy and civil liberties issues in the use of No-Fly and Selectee lists consistent with the statutory authority and subject matter expertise of the DHS Chief Privacy Officer.

<sup>2</sup> In addition to the Selectee list maintained by the TSC, TSA maintains a short list of Non-terrorist Selectees.

One significant concern with the use of No-fly and Selectee watch lists pertains to the quality of information on the lists. This concern arises directly from questions about the standards for putting individuals on watch lists and taking them off these lists, and, indirectly, from questions about the quality of the underlying intelligence. This concern also touches on the framework for access to the information in the databases in order to make corrections and to perform redress. Another type of concern is with the operation of watch lists. Even if the lists themselves were perfect, matching systems would still involve a risk of misidentification because no matching technology works perfectly. Research on matching technologies continues and they are expected to improve over time, particularly with respect to matching of foreign names and as it becomes better determined which data elements best facilitate an accurate match. Moreover, both types of risks can be mitigated to a measurable extent through a robust redress process. Currently, individuals who feel that they have been unfairly singled out for screening or denied boarding can request redress from agencies performing such screening, such as TSA or CBP, as well as from the DHS Office for Civil Rights and Civil Liberties and the DHS Privacy Office, depending on the nature of the concern raised.

#### **A. Findings**

Considerable progress has been made towards streamlining the accuracy and efficiency of the various watch lists or data bases. In particular, the creation of the TSC, as a centralized coordinator of terrorism information, has allowed for a unified team of personnel to focus on data accuracy and data quality as one of a number of drivers of greater success in counter-terrorism efforts.

In particular, the Privacy Office believes that the current TSC standards for No-fly and Selectee lists are appropriately tailored to current uses. That is, these standards are sufficiently narrow, while still broad enough to be effective for screening purposes. In reaching this conclusion, the Privacy Office primarily examined the standards from a privacy and fair information principles perspective: evaluating whether the information collected and used is relevant to the screening inquiry at hand, rather than evaluating the validity of the law enforcement risk determination.

At this time, the analysis of data relevance and accuracy is a positive one. We must caution, however, that as the lists expand both in number of individuals and in number of uses, the use of these lists and the analysis of the privacy/civil liberties impact must be re-evaluated.

#### **B. Recommendations**

Based on our current findings, we offer the following issues and recommendations for consideration in the operation of No-fly and Selectee lists and possible expansion of these lists to other modes of transport. These recommendations reflect our belief that an

effective screening program would enhance the nation's ability to fight terrorism, and that greater data quality and accuracy are supporting components of these efforts.

- **Standards for No-Fly, Selectee, and other "No Transport" Lists.** As these lists are used in more contexts, there is a potential that criteria for putting individuals on these lists will become less focused. Criteria for inclusion on such lists must be strong and consistently applied. Further, routine auditing and appropriate oversight of standards for inclusion of individuals on the consolidated terrorist watch list or the export of that individual identity for inclusion on one of its subsets, such as the No-fly and Selectee lists, is necessary, particularly at the nominating agency level. Consistent oversight of the application of the subsets of the consolidated watch list to screening processes and other operations is necessary to ensure adherence to privacy and fair information principles, as well as for consideration of other civil liberties impacts. Procedures should be in place to periodically review the lists in order to determine whether those who are on the lists continue to be appropriately included, and to ensure continued relevance of the criteria to the use of the lists.
- **Screening in Modes Other Than Aviation** The 9-11 Commission recommended that aviation-related watch list screening be performed by the government in order to improve security of watch lists and to permit the government to use all available terrorism-related information. Consideration should be given to which are the appropriate entities to collect travel-related information and to use it for screening in other modes of transportation. The questions of relevance of the selection criteria, the amount of actual data contained on the lists, and the impact on privacy and civil liberties must be routinely considered going forward if the use of the No-fly and Selectee lists is expanded to other modes of transportation beyond aviation. Expanding the use of No-fly and Selectee lists for screening many or all transportation systems, because of its potential to deprive individuals of all means of travel, may have greater legal and personal implications than the use of these lists to screen only airline passengers.
- **Other Appropriate Uses for Information Collected for Terrorist Screening Purposes** In order to effectively perform screening, the government must collect personal information. It must also compare this information to information available in various databases, including general law enforcement databases. This raises the concern that terrorist screening programs will possibly evolve into broader and more routine law enforcement tools for other purposes. Such evolution from terrorism screening to routine, general law enforcement tools for unspecified purposes would certainly raise concerns about further privacy incursions. The question of appropriate uses of screening information and

appropriate oversight for such programs must be considered on an ongoing basis, not only at the inception of a program, but throughout its operation.

- **Appropriate Mechanisms and Venues for Redress in the Case of Misidentified Individuals or Individuals Who Are Placed on Watch Lists Improperly** Access and redress are fundamental components of a program's adherence to fair information principles, the exercise of civil liberties, and the resulting public trust that ensues from such policies. Currently different agencies have different redress processes, and these processes vary in effectiveness. A robust redress program is essential for any federal program that uses personal information in order to grant or deny to individuals a right, privilege or benefit. If watch-list screening is applied to modes of transport other than aviation, quick and effective redress will become increasingly important. Inclusion of a robust, effective redress process should be an essential element of any current or future federal screening program.

## Table of Contents

<b>I.</b>	<b>EXECUTIVE SUMMARY</b>	<b>I</b>
A.	FINDINGS	II
B.	RECOMMENDATIONS	II
<b>I.</b>	<b>INTRODUCTION</b>	<b>1</b>
<b>II.</b>	<b>WATCH LISTS AND THE TERRORIST SCREENING CENTER</b>	<b>2</b>
<b>III.</b>	<b>TRAVEL SCREENING PROGRAMS</b>	<b>4</b>
<b>IV.</b>	<b>EXPERIENCE OF INDIVIDUALS WHOSE NAMES MATCH NO-FLY AND SELECTEE LISTS</b>	<b>5</b>
<b>V.</b>	<b>PRIVACY AND CIVIL LIBERTIES CONCERNS IN THE USE OF NO-FLY AND SELECTEE LISTS</b>	<b>7</b>
A.	OVERVIEW	7
B.	STANDARDS FOR PUTTING INDIVIDUALS ON NO-FLY AND SELECTEE LISTS AND FOR TAKING THEM OFF LISTS	9
C.	MATCHING ERRORS	11
D.	MATCHING IN AN ENVIRONMENT WHERE IDENTITY THEFT AND SYNTHETIC IDENTITIES MAY BE PRESENT	14
<b>VI.</b>	<b>REDRESS PROCESSES AND MECHANISMS</b>	<b>16</b>
A.	OVERVIEW	16
B.	REDRESS AT TSA	16
C.	REDRESS AT CBP	17
D.	REDRESS AT CRCL	18
E.	REDRESS THROUGH THE DHS PRIVACY OFFICE	19
F.	REDRESS AT THE TSC	20
<b>VII.</b>	<b>ISSUES FOR CONSIDERATION</b>	<b>20</b>
<b>VIII.</b>	<b>CONCLUSION</b>	<b>22</b>

## I. Introduction

This report responds to Section 4012(b)(2) of the Intelligence Reform and Terrorism Prevention Act, P.L. 108-458, which requires the “Security Privacy Officer” of the Department of Homeland Security (DHS) to submit to Congress a report assessing the impact of the Automatic Selectee and No-fly (“Selectee” and “No-fly”) lists on privacy and civil liberties.<sup>1</sup> In particular, the statute requires the report to address the following issues:

- (A) any recommendations for practices, procedures, regulations, or legislation that the Security Privacy Officer considers necessary to minimize adverse effects of automatic selectee and no-fly lists on privacy, discrimination, due process, and other civil liberties;
- (B) a discussion of the implications of applying those lists to other modes of transportation; and
- (C) the effect that implementation of the recommendations would have on the effectiveness of the use of such lists to protect the United States against terrorist attacks.

The DHS Privacy Office is the first statutorily required comprehensive privacy operation in any U.S. federal department or agency. It operates under the direction of the Chief Privacy Officer, who is appointed by and who reports directly to the Secretary. The DHS Privacy Office serves as a steward of Section 222 of the Homeland Security Act of 2002, and has programmatic responsibilities involving the Privacy Act of 1974, the Freedom of Information Act, the privacy provisions of the E-Government Act, and DHS policies that protect the collection, use, and disclosure of personal and Departmental information.

The Privacy Office oversees privacy policy matters and certain information disclosure issues. It is also statutorily required to evaluate all new technologies used by the Department for their impact on personal privacy. In addition to its other responsibilities, the Privacy Office is responsible for privacy-related education and training initiatives for DHS’s more than 180,000 employees.

---

<sup>1</sup> Section 608 of Vision 100 – Century of Aviation Reauthorization Act of 2003, P.L. 108-176, requires the submission of a report on Passenger Prescreening Program. Some of the issues that the report was required to address, such as the use of risk scores, are no longer pertinent with the cancellation of the CAPPS II program. Other issues, related to privacy and civil rights concerns arising from the use of No-fly and Selectee lists and redress procedures for minimizing the impact of such lists on privacy and civil rights, are addressed in this report.

The DHS Chief Privacy Officer wishes to acknowledge assistance from the Transportation Security Administration, Bureau of Customs and Border Protection, and Office of the General Counsel, and, in particular, the staff and leadership of the Terrorist Screening Center at the Department of Justice.

In writing this report at the direction of Congress, the DHS Chief Privacy Officer also wishes to acknowledge assistance from the Department's Office for Civil Rights and Civil Liberties. In accordance with 6 U.S.C. 345, the Office for Civil Rights and Civil Liberties oversees Departmental compliance with requirements relating to the civil rights and civil liberties of individuals.<sup>2</sup>

The report is structured as follows: Section II provides a high-level overview of the Selectee and No-fly lists. Section III discusses current screening programs that use such lists. Section IV describes the experiences of individuals whose names may match names on the No-fly and Selectee lists. Section V identifies legal, policy and technical issues in the creation, maintenance and use of the Selectee and No-fly lists that give rise to concerns about privacy and civil liberties. Section VI discusses complaints received by agencies using Selectee and No-fly lists and describes current approaches to redress provided to individuals who submit such complaints. The final section of the report identifies issues for consideration by Congress regarding practices, procedures, regulations, or legislation to minimize the adverse effect of using automatic Selectee and No-fly lists, particularly as their use may be expanded to other modes of transportation.

## **II. Watch Lists and the Terrorist Screening Center**

Historically, nine government agencies maintained 12 different watch lists intended to accomplish a variety of purposes.<sup>3</sup> Two of these lists, the "No-fly" and "Selectee" lists, were maintained by the Transportation Security Administration (TSA) within the Department of Transportation and later as part of DHS.<sup>4</sup> The authority for maintaining watch lists was granted to TSA in the Aviation and Transportation Security Act, PL 107-71, codified as 49 U.S.C. 114(h). The No-fly list is a list of individuals who are prohibited from boarding an aircraft. The Selectee list is a list of individuals who must undergo additional security screening before being permitted to board an aircraft.

---

<sup>2</sup> CRCL also assists the Secretary and senior officials in developing, implementing, and reviewing Departmental policies and procedures for the protection of civil rights and civil liberties. CRCL receives and reviews complaints from members of the public who claim that because of their race, ethnicity, or religion, or the exercise of their free speech rights, they have been placed on the watch list.

<sup>3</sup> Government Accountability Office, *Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*, GAO-03-322, April 2003, p. 12.

<sup>4</sup> GAO (2003), p. 13.

To consolidate the numerous watch lists and ensure that they are used in a coordinated fashion, Homeland Security Presidential Directive 6 (HSPD-6) was issued. HSPD-6 led to the establishment of the Terrorist Screening Center (TSC) under the administration of the Federal Bureau of Investigation (FBI), U.S. Department of Justice, in cooperation with the Central Intelligence Agency and the Departments of Defense, State, Homeland Security, and Treasury. TSC consolidates the federal government's terrorist watch lists and provides for appropriate and lawful use of terrorist information in screening processes.<sup>5</sup>

In FY 2004, TSA's No-fly and Selectee became a subset of the larger Terrorist Screening Database (TSDB) maintained by TSC.<sup>6</sup> The TSDB contains the names and identifiers of known and suspected terrorists and is referred to as the consolidated terrorist watch list. As of January 2005, the TSDB contained 237,615 records.<sup>7</sup> The number of individuals included in the TSDB is smaller, in part, than the number of records because the database contains some duplicate records and partial names.<sup>8</sup>

In addition to consolidating watch-list information, TSC serves as the source of up-to-date watch lists for agencies that use such lists to screen for terrorists ("screening agencies"). These screening-agency databases are subsets of the TSDB which are exported to the relevant agencies for use in screening. The No-fly and Selectee lists are distributed to TSA, which, pursuant to its statutory responsibility to screen airline passengers, shares the information with carriers for purposes of screening domestic airline passengers, and to the Bureau of Customs and Border Protection (CBP), which is responsible for screening international passengers. Other agencies get other watch lists, as required by their missions.<sup>9</sup>

TSC has established a process for adding names to watch lists. Nominations to the TSDB are submitted by various federal agencies, state and local law enforcement (via the Joint Terrorism Task Force), and the intelligence community. Purely domestic terrorism nominations are reviewed by the FBI and consolidated for submission to TSC;

---

<sup>5</sup> HSPD-6, para. 1.

<sup>6</sup> U.S. Department of Justice Report, referenced in B. Elias, W. Krouse, and E. Rappaport, *Homeland Security: Air Passenger Prescreening and Counterterrorism*, CRS Report for Congress, RL32802, Congressional Research Service (2005).

<sup>7</sup> U.S. Department of Justice, Office of the Inspector General, Audit Division, *Review of the Terrorist Screening Center*, Audit Report 05-27, June 2005, at p. 49.

<sup>8</sup> U.S. Department of Justice (2005), pp. 50-51.

<sup>9</sup> U.S. Department of Justice (2005), p. 11.

international terrorism nominations are consolidated, reviewed, and submitted to TSC by the National Counterterrorism Center (NCTC).<sup>10</sup> When TSC accepts a nomination, it assigns the record for export to one or more screening-agency databases, including the No-fly and Selectee lists. The lists are then provided to various screening agencies. An individual may only be removed from the various screening-agency databases by the nominating agency.<sup>11</sup>

When government screening agencies encounter a possible match to lists provided to them by TSC, they are instructed to contact TSC. TSC consults additional information in various government databases that may not be available to the screening agency in order to determine if there is an exact identity match. If there appears to be a match with the name on the watchlist, TSC coordinates an appropriate response through the Terrorist Screening Operations Unit at the FBI, specifically the appropriate Joint Terrorist Task Force (JTTF), including the agency which was the source of the nomination. This ensures that the encounter assists and does not jeopardize ongoing investigations.

### **III. Travel Screening Programs**

Two DHS agencies, TSA and CBP, have the statutory responsibility for screening airline passengers for security reasons, and thus use the No-fly and Selectee lists for this purpose. TSA is responsible for screening all airline passengers on domestic flights; CBP is responsible for screening passengers on international flights. At present, the matching of airline passenger names against No-fly and Selectee lists for domestic flights is performed by the airlines. Airlines are required to notify TSA of matches to the No-fly and Selectee lists. Passengers who are matches to the Selectee list receive additional security screening before being permitted to board.

The proposed Secure Flight program is intended to move the watch list matching function from the airlines to TSA, with the final adjudication of potential matches by TSC. Moving watch list screening to the government is mandated by the Intelligence Reform and Terrorism Prevention Act<sup>12</sup> and is consistent with the recommendations of the 9-11 Commission.<sup>13</sup> Having sole responsibility for watch-list matching will permit TSA to

---

<sup>10</sup> U.S. Department of Justice (2005), p. 24.

<sup>11</sup> TSC briefing, Draft March 1, 2005, p. 10.

<sup>12</sup> P.L. 108-458, Section 4012 (a)(1).

<sup>13</sup> The National Commission on Terrorist Attacks Upon the United States, known as the 9-11 Commission, described the issue on p. 392 of its report: "Because air carriers implement the [watch list screening] program, concerns about sharing intelligence information with private firms and foreign countries keep the U.S. government from listing all terrorist and terrorist suspects who should be included."

enhance security of information used for screening by allowing TSA to retain control of the information. It will also allow TSA to apply improved screening procedures overall, will permit the use of consistent internal analytical procedures when automated resolution of potential matches is not possible, and will allow for more consistent procedures at airports for those passengers identified as potential matches.

As part of its mission to protect the borders of the United States, CBP screens passengers on international flights. CBP also screens cruise ship passengers and crews. Airlines screen passengers against TSA-provided No-fly and Selectee lists prior to departure. In addition, airlines are required to provide CBP with complete passenger information 15 minutes after departure of the airline from a foreign place. Crew manifest information is provided 60 minutes prior to departure. Vessel carriers must provide CBP with passenger and crew manifest information at least 24 hours and up to 96 hours prior to entry into a U.S. port. The manifests contain the information needed by CBP to compare individuals aboard air and sea vessels to No-fly and Selectee lists and other government law enforcement databases, and also to ascertain whether there are other reasons to prevent the entry of non-citizens under immigration laws, as applicable, or to designate individuals for additional inspection, because, for example, they are suspected drug smugglers, traveling on documents reported as lost or stolen, or suspected of violating other laws enforced by CBP.

Currently, CBP does not perform watch-list matching until it receives manifest data. However, under current rules, the manifest data is not received until after the craft is en route. As a result, several aircraft have been diverted when individuals on the No-fly list were found to be aboard.<sup>14</sup> Section 4012 of the Intelligence Reform and Terrorism Prevention Act requires DHS to promulgate a regulation to allow it to screen international passengers against the watchlist before departure of the flight. Several possible implementations of pre-flight screening are being considered with a goal of implementing an effective screening program that would have minimum disruptive impact on air operations. It is expected that pre-flight screening will result in fewer post departure diversions. Screening of cruise line passengers is, obviously, less of an issue in this respect because of longer transit times.

#### **IV. Experience of Individuals Whose Names Match No-Fly and Selectee Lists**

Experiences that individuals might have as a result of being matched -- correctly or incorrectly -- to a name on the No-fly or Selectee list vary, depending on whether the

---

<sup>14</sup> Stories about diverted aircraft have been published in newspapers around the world. See, for example, S. K. Goo, *U.S. Modifies Passenger List Proposal*, Washington Post, June 1, 2005, p. D02. The article mentions that three foreign airliners have been diverted during the previous four weeks.

individual is matched to the No-fly list or Selectee list, and on whether he or she is traveling domestically or internationally. Treatment received by someone who is matched or mis-matched to the list also depends on the way particular government and airline employees interpret and implement policies and procedures related to watch list matches.

As noted above, currently, screening of domestic and foreign passengers against watch lists is performed by airlines on the basis of lists provided by TSA, but maintained by TSC. If an individual appears to be a match to the No-fly list for a domestic flight, TSA coordinates with TSC, and law enforcement action is taken at check-in as appropriate. The individual is not permitted to board the airplane.

If an individual is matched to the Selectee list prior to boarding an aircraft, he or she is subject to additional screening, which may include questioning, body scanning, and luggage search. Depending on the results of this additional screening, the passenger may be allowed to board the aircraft or a law enforcement response may be required. If an individual feels that he or she has been unfairly denied boarding or singled out for screening, he or she can contact TSA's Office of Transportation Security Redress (OTSR),<sup>15</sup> the DHS Privacy Office, or DHS Office for Civil Rights and Civil Liberties (CRCL). The redress process and complaint processes are described in the section titled Redress Processes and Mechanisms.<sup>16</sup>

Individuals on international flights arriving into the United States are screened not only against the No-fly and Selectee lists, but also against other law enforcement databases. The screening is intended "to identify those passengers who (1) may pose a risk to the transportation industry, to other travelers and to the United States, (2) are identified as or suspected of being a terrorist or having affiliations to terrorist organizations, (3) have active warrants and warrants for criminal activity, (4) are currently inadmissible, or have been previously deported from the United States, or (5) are subject to other intelligence that may identify them as a security risk."<sup>17</sup> If an individual on an international flight bound for the United States is determined to be a match to a name on a watch list or

---

<sup>15</sup> The TSA Ombudsman's serves as an intake office for contacts to TSA and may forward inquiries and complaints concerning watch lists to OTSR.

<sup>16</sup> The Department is in the process of reevaluating these processes in connection with the development of the Secure Flight regulation. TSA is now statutorily required by the IRTPA to have a redress process in place and the new Secure Flight rule should address these issues.

<sup>17</sup> Privacy Impact Assessment for the Advance Passenger Information System (APIS), March 21, 2005, at p. 4, available at < [http://www.dhs.gov/interweb/assetlibrary/privacy\\_pia\\_cbpapis.pdf](http://www.dhs.gov/interweb/assetlibrary/privacy_pia_cbpapis.pdf)>.

otherwise in a law enforcement database, the response can vary from additional questioning and screening to removal from the flight or denial of admission into the United States.

The reported experiences of individuals whose names appear to match names on the No-fly and Selectee lists can be trying and unpleasant. Complaints filed with CRCL have alleged that individuals have experienced long delays, have been separated from members of their family and given no explanation or conflicting explanations about what is going on. Some complaints alleged that officers have asked travelers questions about their religion and national origin, whether one traveler knew anyone at his mosque who hates Americans or disagrees with current policies, targeted a traveler for additional screening because she wore traditional Muslim attire and told another traveler that he and his wife and children were subjected to body searches because he was born in Iraq, is Arab, and Muslim. Other complaints alleged misconduct or disrespect by airline, law enforcement, TSA or CBP officials.

## **V. Privacy and Civil Liberties Concerns in the Use of No-Fly and Selectee Lists**

### **A. Overview**

Since the 1960s the federal government has made it unlawful to engage in behavior that threatens or endangers transportation security and safety.<sup>18</sup> The terrorist watch lists, and No-fly and Selectee lists, are useful tools for preventing terrorist activity which could endanger the safety of airline passengers and others. Nevertheless, the use of these tools raises privacy and civil liberties implications. To perform matching with reasonable quality and to correct mistakes, the entities that use watch lists must collect personal information from everyone who travels, raising concerns that this information will be used inappropriately if adequate safeguards are not in place. Additionally, as described in a previous section of this report, individuals who are mistakenly put on watch lists or who are misidentified as being on these lists can potentially face consequences ranging from inconvenience and delay to loss of liberty, depending on the law enforcement action taken as a result of the match.<sup>19</sup>

---

<sup>18</sup> T. Tatelman, *Interstate Travel: Constitutional Challenges to the Identification Requirement and Other Transportation Security Regulations*, CRS Report to Congress, RL32664, December 21, 2004, p. 1.

<sup>19</sup> Although the “right to travel” generally has been found to be protected by the Constitution, there is no guarantee that one may travel by one’s preferred mode of transportation. If alternative modes of transportation are available, the courts have found that restrictions on air travel do not constitute a violation of a constitutional right. See, e.g., *Cramer v. Skinner*, 931 F.2d 1020, 1031 (5<sup>th</sup> Cir. 1991).

A concern that was identified at the time this report was written with the use of No-fly and Selectee watch lists pertains to the quality of information on the lists.<sup>20</sup> This concern arises directly from questions about the standards for putting individuals on the watch list and taking them off the list, and, indirectly, from questions about the quality of the underlying intelligence. This concern also touches on the framework for access to the information in the databases in order to make corrections and to perform redress. Subsequent steps have been taken to establish uniform criteria for nomination to the list.

A second concern is the operation of No-fly and Selectee lists. No technology works perfectly, and all systems, computerized or human, are prone to errors. Even if the lists themselves were perfect, matching systems would still involve a risk of misidentification.<sup>21</sup> These risks are magnified by the fact that watch lists contain names derived from languages and alphabets other than English and for which there may not be a universal transliteration standard.

The fact that personal information is required for screening individuals against the No-fly and Selectee lists raises the question about the appropriate entities to perform screening. Of course, if travel-related screening is performed by the government, the government needs to collect personal information from all individuals who wish to travel, raising questions about collection limitations, appropriate use and the ground rules that govern the extent to which information collected for screening purposes may be used for other government applications. That said, if screening continues to be performed by private companies, such as airlines, it is possible that the security of the lists may be compromised and their effectiveness reduced.<sup>22</sup> Indeed, Congress has mandated that TSA begin testing an advanced passenger screening system to assume the performance of comparing passenger data information, as defined by the Assistant Secretary for TSA, that utilizes all appropriate records in the consolidated and integrated terrorist watchlist maintained by the Federal government. DHS is addressing this mandate by developing

---

<sup>20</sup> GAO, *Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System is Further Developed*, GAO-05-356, March 2005, p. 30-31, discusses the uncertainty about the quality of the data in the TSDB. A CRS report notes that the standards for creating and maintaining watch lists do not appear to have been made publicly available. (T. Tatelman, 2004).

<sup>21</sup> B. Elias, W. Krouse and E. Rappaport, pp. 13-15 (2005).

<sup>22</sup> The 9-11 Commission report, p. 392.

the Secure Flight program for air travel that will migrate screening from the airlines to the government.<sup>23</sup>

This section of the report discusses each of these challenges and how they would be magnified if No-fly and Selectee lists were applied to other modes of transportation.

**B. Standards for Putting Individuals on No-Fly and Selectee Lists and for Taking Them Off Lists**

Since the existence of No-fly and Selectee lists became public in October 2002, the media have reported allegations that individuals are being put on these lists because of their political beliefs or activities or because of their race, religion or national origin.<sup>24</sup> CRCL has received complaints containing similar allegations. The allegations have apparently arisen because criteria and standards for placing individuals on watch lists have not been made publicly known.<sup>25</sup> To date, the Department has not found that any of the allegations could be substantiated. It is important to understand that the criteria cannot be made public without compromising intelligence and security or inviting subversion of these lists by individuals who will seek ways to adjust their behavior to avoid being identified as a threat to aviation. Thus, the success of this antiterrorism tool depends in part on the confidentiality of the protocols for inclusion on a No-fly or Selectee list.

Appropriate standards for putting individuals on No-fly and Selectee lists and for taking them off such lists are nevertheless essential for assuring civil liberties of the traveling public. If the standards are overly broad, vague, and not related to the threat that the No-fly and Selectee lists are supposed to address, individuals who do not present a threat may be prevented from exercising their ability to travel. In an attempt to resolve this issue, TSA has issued direction to air carriers on using the lists and resolving name conflicts on the list.

---

<sup>23</sup> Section 4021 of the IRTPA requires the Transportation Security Administration (TSA) to assume passenger prescreening functions from air carriers, and TSA is developing a passenger pre-screening program called Secure Flight.

<sup>24</sup> See, for example, New York Advisory Committee to the U.S. Commission on Civil Rights, *Civil Rights Implications of Post-September 11 Law Enforcement Practices in New York*, p. 7, available at <<http://www.usccr.gov/pubs/sac/ny0304/ny0304.pdf>>, last visited June 7, 2005.

<sup>25</sup> See, for instance, A. Ramasastry, *A New ACLU Lawsuit Challenges "No-fly" and "Selectee" List Procedures*, FindLaw's Legal Commentary, available at <<http://writ.corporate.findlaw.com/ramasastry/20040413.html>>, last visited on June 7, 2005.

Concerns about the quality of TSDB data are significant because the quality of the No-fly and Selectee lists depends on the overall quality of the data in the TSDB. From its inception, TSC had established general standards for the nominations that it will accept into the TSDB and that are intended to minimize misidentification and prevent profiling. During its review several months ago, the Department of Justice Inspector General's report on watch lists questioned these standards. The report stated that "to err on the side of caution, individuals with any degree of a terrorism nexus were included on the consolidated watch list, as long as minimum criteria was [*sic*] met (i.e., the person's name was partially known plus one other piece of identifying information, such as the date of birth)." <sup>26</sup> Furthermore, the auditors "determined that the TSC could not ensure that the information in that database was complete and accurate. We found instances where the consolidated database did not contain names that should have been included on the watch list. In addition, we found inaccurate information related to persons included in the database." <sup>27</sup> The auditors also found records whose source could not be identified <sup>28</sup> and records that were not assigned to appropriate watch lists. <sup>29</sup> The IG report reviewed TSC operations through November of 2004; since that time the TSC has instituted more stringent quality control procedures, including an ongoing manual review of every record in the TSDB. <sup>30</sup> The TSC also has a Privacy Officer, who works on data quality issues and the redress process.

In late 2004, the White House Homeland Security Council (HSC) approved new criteria for inclusion of names on No-fly and Selectee lists. TSC prepared a list of terrorist subjects who were assigned to these lists within the TSDB, and the FBI JTTF case agents and other nominating agencies reevaluated their subjects' status and adjusted status as appropriate to comply with the new criteria. <sup>31</sup> In January 2005, TSC implemented guidance for placing individuals on No-fly and Selectee lists. The guidance provides specific criteria for nominating individuals for No-fly and Selectee lists and includes examples of appropriate and inappropriate nominations, which are tied directly to aviation security and terrorism.

---

<sup>26</sup> U.S. Department of Justice (2005), p. 30.

<sup>27</sup> U.S. Department of Justice (2005), p. xi.

<sup>28</sup> U.S. Department of Justice (2005), p. 52.

<sup>29</sup> U.S. Department of Justice (2005), p. 65.

<sup>30</sup> U.S. Department of Justice (2005), p. 100.

<sup>31</sup> U.S. Department of Justice (2005), p. 99.

The Privacy Office believes that the current TSC standards for No-fly and Selectee lists are sufficiently narrow, while still broad enough to be effective for screening purposes. In reaching this conclusion, the Privacy Office primarily examined the standards from a privacy and fair information principles perspective rather than from a law enforcement perspective because the law enforcement decision about the risk to aviation security posed by an individual or his associates is for other offices to make. The more the lists expand beyond individuals who are believed to pose a potential threat to civil aviation, however, the greater the likelihood that some individuals, whose relationship to aviation security threats is highly speculative, will be subjected to additional screening or prevented from traveling. If there is no relationship between the threat to civil aviation and the placement of an individual on a list that bars the individual's ability to travel, there may be an insufficient predicate reason to interfere with travel.

### **C. Matching Errors**

All systems for matching names against watch lists are prone to errors. There is a potential for two types of errors that result from improper matching between an individual and a record on a watch list. A "false positive" occurs when the system signals that someone is on a watch list when the individual is not on the list. A "false negative" occurs when the system does not signal that an individual is on a watch list when the individual is actually on the list. In the context of terrorism screening, false positives give rise to privacy and civil liberties concerns because they can result in a range of consequences for innocent individuals. False negatives, on the other hand, give rise to security concerns because they allow known or suspected terrorists to slip through the detection system.

System designers must perform a trade-off between false positives and false negatives generated by a system—as one type of error decreases, the likelihood of the other type tends to increase, because a correlation tends to exist between these two types of errors. In other words, if a system is designed to minimize false negatives, it will produce a larger number of false positives, and vice versa. In terrorist screening systems, false negatives are potentially very costly in terms of lives that might be lost and in terms of economic damage resulting from acts of terrorism. However, there are very few individuals on watch lists compared to the number of individuals who are matched against these lists, so a system that is very sensitive to false negatives has the potential to produce a large number of false positives.<sup>32</sup>

---

<sup>32</sup> For example, let us say that a system is 99.9 percent effective in doing its matches. With approximately 1.8 million passengers flying in the United States daily, the 99.9 percent accuracy rate would produce 1,800 errors per day.

False positives resulting from aviation screening have received wide media attention. As a result, Congress has directed TSA to demonstrate that its design of the Secure Flight program will minimize false positives.<sup>33</sup> However, names, alone or in combination with other attributes, do not always allow for identification of particular individuals, so TSA will need to collect additional personal information in order to distinguish misidentified individuals from those who are on the No-fly or Selectee lists.<sup>34</sup> The challenge, consistent with the principle of limited and appropriate data collection and use, is to determine what additional personal information will actually improve matching and reduce misidentification by a screening program. Empirical testing can demonstrate the usefulness of various data elements for screening against watch lists.

The redress process, which is described in greater detail below, requires collection of additional personal information from individuals who believe that they were misidentified during screening. Congress has authorized TSA to maintain a misidentified persons list.<sup>35</sup> Of course, the fact that additional personally identifiable information will be collected raises concerns about ensuring appropriate safeguards over the privacy of that information. Strict rules for accessing information, as well as defined retention periods for screening data related to individuals who are not on the No-fly and Selectee lists or misidentified persons list, can help ameliorate these concerns.

Another potential misidentification issue arises because names from other languages that appear on the No-fly and Selectee lists may be written in different ways.<sup>36</sup> There are many algorithms for matching words in computer databases, and many of them are designed specifically for matching names. Matching algorithms fall into two broad classes: orthographic algorithms, which compare strings of letters without regard to sound, and phonological algorithms, which compare strings of letters on the basis of

---

<sup>33</sup> P.L. 108-458, Section 4012 (a).

<sup>34</sup> The National Academy of Sciences report *Who Goes There: Authentication Through the Lens of Privacy* (2003) discusses the use of identifiers, alone or in combination, to point to specific individuals. Chapter 2 discusses how several “weak” identifiers, i.e., identifiers that do not point to a unique individual, may be combined to identify specific persons. However, even a combination of several attributes may not be sufficient for definitive identification.

<sup>35</sup> P.L. 108-458, Sec. 4012(a)(1)(G)(ii).

<sup>36</sup> Congress recognized the difficulty presented by variation in transliteration of foreign names in Section 7205 of the Intelligence Reform and Terrorism Prevention Act, where it found that the lack of a universal transliteration standard for Arabic names contributed to the difficulty of identifying September 11 hijackers. As a result of the finding, the Congress encouraged the President to enter into international negotiations to establish a universal transliteration standard into the Roman alphabet.

phonetic representation.<sup>37</sup> Both classes of algorithms are useful in matching of passengers against the lists, but each algorithm produces a different set of matches and all algorithms have significant error rates.

Recognizing this problem, programs that perform matching against terrorist watch lists can use multiple algorithms.<sup>38</sup> Nevertheless, even with the use of multiple algorithms, matching programs must use additional information to increase the quality of matches in order to minimize false negatives (i.e., to ensure that those on the list do not escape detection) while producing a reasonable number of false positives. The need for additional information raises privacy concerns, particularly if this information is retained by the screening entity.

If the use of No-fly and Selectee lists is expanded to modes of transport other than air and cruise ships, the number of individuals being screened will increase significantly and, therefore, the number of matching errors could also increase.

Implementing screening programs using the No-fly and Selectee lists for other modes would also be logistically and administratively difficult in some cases. Rail and surface transportation networks are vast, complex, open and generally accessible to the public by design and their operations are highly fragmented. According to the Bureau of Transportation Statistics, a component of the Department of Transportation, there were 83 air carriers in the US in 2002 but approximately 6,000 transit systems that operate buses, rail systems, ferry boats and other modes of passenger transport.<sup>39</sup> Allowing other modes of transportation to conduct screening through distribution of some version of the

---

<sup>37</sup> B.J. Dorr, *Computational Linguistics Meets the FDA: Techniques for Identifying Sound-alike Drug Names*, University of Maryland, July 2003, available at <<http://www.umiacs.umd.edu/~bonnie/Drugname-Talk-2003.ppt>>, last visited on June 3, 2005. An example of an orthographic algorithm is one that compares names character by character after removing spaces and punctuation and transforming the name into all capital letters. An example of a phonological algorithm is Soundex, created in the 19<sup>th</sup> century and still in use for genealogical research. Soundex transforms each name into a four-character index representing the sound of the name when spoken. This allows matching of names that sound alike but are spelled differently. There have been many improvements on Soundex. One of the improved algorithms, Double Metaphone, allows coding not only of the American pronunciation of the name but also of the native pronunciation. Research on matching algorithms continues.

<sup>38</sup> See, for example, discussion of name search capability in the U.S. Department of Justice report (2005), pp. 26-27.

<sup>39</sup> U.S. Department of Transportation, Bureau of Transportation Statistics, National Transportation Statistics 2004, Appendix A, Transit Profile (updated April 2005), available at <[http://www.bts.gov/publications/national\\_transportation\\_statistics/2004/html/table\\_transit\\_profile.html](http://www.bts.gov/publications/national_transportation_statistics/2004/html/table_transit_profile.html)>, last visited June 13, 2005. The figure represents the number of transit agencies; some agencies operate more than one mode of transport.

No-fly and Selectee lists may pose a security risk by virtue of the number of entities that would be involved. Bringing screening into the government for additional modes of transport would introduce not only an increased workload and expense to screening programs, but also increased operational complexity.

**D. Matching in an Environment Where Identity Theft and Synthetic Identities May Be Present**

Matching identities to individual identifiers contained within the consolidated terrorist watch list can help to flag individuals suspected of terrorism. However, a suspected terrorist or an individual considered to be a threat to aviation may be using a false identity and not travel under his or her own name. Conducting a match based on an assumed identity may result in a false negative.

Identity theft, the appropriation of another person's identity, has become increasingly common. Stolen identities are most often used for financial fraud, such as opening and using credit card accounts, accessing bank accounts, and purchasing vehicles on credit.<sup>40</sup> The Federal Trade Commission reports 246,570 complaints of identity theft during calendar year 2004.<sup>41</sup>

A somewhat different but related problem is the creation of synthetic identities. While a stolen identity is an identity of a real person, a synthetic identity is a blend of fact and fiction.<sup>42</sup> For example, a synthetic identity may be a combination of an individual's actual address with a name and social security number issued to someone who died in childhood. A synthetic identity is more useful than "true-name" identity theft for purposes that do not involve financial fraud because there is no "owner" of the identity to uncover the fraud and report the theft.<sup>43</sup>

---

<sup>40</sup> See, for example, Government Accountability Office, *Consumers Understood Credit Reporting But Could Benefit From Targeted Education*, GAO-05-223, March 2005, p. 2.

<sup>41</sup> Federal Trade Commission, *National and State Trends in Fraud & Identity Theft, January – December 2004*, February 1, 2005, p. 4, available at <<http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf>>. last visited June 6, 2005. The report states that the number of identity theft complaints reported may increase over time as other agencies add their data to the FTC database.

<sup>42</sup> Federal Deposit Insurance Corporation, *Putting an End to Account-Hijacking Identity Theft*, available at <<http://www.fdic.gov/consumers/consumer/idtheftstudy/background.html#foot2>>, last visited on June 6, 2005.

<sup>43</sup> T. Oscherwitz, *Synthetic Identity Fraud: Unseen Identity Challenge*, Bank Security News, Vol. 3, No. 7, April 2005, available at <[http://www.idanalytics.com/pdf/Bank\\_Security\\_News.pdf](http://www.idanalytics.com/pdf/Bank_Security_News.pdf)>, last visited June 6, 2005.

A third type of identity-related fraud is identity “rental.” This phenomenon involves the temporary use of a legal identity, with the consent of its owner, by someone other than the owner. The transaction generally involves a legal immigrant who “rents” his identity to an illegal immigrant while the legal immigrant stays outside the country. The illegal immigrant works in the U.S. under the “rented” identity and pays taxes under that identity, making the fraud difficult to detect.<sup>44</sup>

In the context of travel-related terrorism screening that relies significantly on identity verification, risks associated with the use of false identities through identity theft, identity “rental” and use of synthetic identity need to be recognized in order to plan for mitigation techniques that may reduce the possibility that wanted individuals could escape detection. At least three mechanisms have been proposed as a way to determine whether someone is using a false identity: using commercial data to compare information provided for travel with information available about the individual in other contexts; using biometric identifiers; and requiring the use of more reliable identification documents. None of these is foolproof. For instance, there have been documented concerns about the quality of data in commercial databases used for identity verification. Biometrics have been found to be a reliable method of positive identification. Nevertheless, biometrics can result in identification errors, although the number of such efforts appears to be small compared to the total number of biometric identifications made. In addition, identity documents may rely on foundational or “breeder” documents that themselves may not be reliable in certain circumstances.<sup>45</sup> That said, depending upon their implementation, the three mechanisms could potentially significantly improve confidence that the individual claiming an identity is entitled to that identity.

As noted already, the use of any proposed identity verification scheme requires collection of personal information from all travelers in addition to the information that would be needed strictly to match an individual to a watch list. This additional information collection presents privacy concerns because it raises the risk that, if adequate safeguards are not in place, information will be used inappropriately. Furthermore, each method for identity verification results in tighter association of the identity with the individual. As identity information becomes more tightly “bound” to the individual and as this identity

---

<sup>44</sup> E. Porter, *Social Security: Migrants Offer Numbers for Fee*, The New York Times, June 7, 2005.

<sup>45</sup> National Academy of Sciences, *Who Goes There: Authentication Through the Lens of Privacy*, Chapter 6, (2003).

information propagates to more data sources, errors can become more difficult to correct,<sup>46</sup> with the attendant implications for individuals affected by the errors.

Therefore, these risks need to be recognized. It is important to address and plan for ways to detect the use of false identities in the screening process and to continuously improve the integrity of data used for purposes of identity verification, recognizing that identity screening is just one layer in a multi-layered approach to screening that also includes physical screening.

## **VI. Redress Processes and Mechanisms**

### **A. Overview**

An effective redress program can mitigate to a measurable extent the privacy and civil liberties concerns with the use of No-fly and Selectee lists for airline screening. Currently, individuals have several possible venues for requesting redress if they feel they are unfairly singled out by No-fly and Selectee lists, but the procedures are not uniform and public awareness of some of the options appears to be limited.

TSA and CBP have redress offices that interact directly with individuals who contact them. In addition, individuals can contact the DHS Office for Civil Rights and Civil Liberties (CRCL) and the DHS Privacy Office. Individuals also pursue redress indirectly through the Freedom of Information Act by requesting copies of documents that they believe contain information relevant to their screening experience. Although TSC does not interact directly with the public, it has a Quality Assurance /Redress Branch that works with agencies on redress issues and then works within TSC to ensure that information gained through the redress process is transmitted to nominating agencies and appropriately used within TSC. This Branch receives direct guidance and oversight from the TSC Privacy Officer.

### **B. Redress at TSA<sup>47</sup>**

The Office of Transportation Security Redress (OTSR) within TSA is independent of the program offices. TSA also has an Office of the Ombudsman that oversees the TSA Contact Center. Individuals may also contact TSA's Office of Civil Rights (OCR). If an individual alleges that he was subjected to additional scrutiny unrelated to his/her presence on a list, because of some discriminatory factor, OCR will conduct an

---

<sup>46</sup> Commercial data aggregators, many using information from public sources, disclaim responsibility for errors in their data because they collect data from multiple sources, often receiving automated data feeds.

<sup>47</sup> The information related to redress processes and functions at TSA was accurate at the time the report was written.

investigation to determine if there is evidence of intentional discrimination and, where appropriate, recommend corrective action.

Redress at TSA is a multi-step process. A passenger who feels repeatedly and unfairly targeted due to having a name similarity to an individual on the watch lists or due to actually being on the watch lists contacts the TSA Contact Center or visits the TSA public website for the information necessary to begin the redress process. The office responds by mailing the individual a Privacy Act Notice and a Passenger Identity Verification Form (PIVF).<sup>48</sup> The passenger has an unlimited amount of time to submit the executed Privacy Act Notice and PIVF. The PIVF requires a passenger to submit notarized or certified photocopies of three identification documents. When the PIVF package is received, TSA compares the passenger's information against the watch lists. The OTSR notifies the passenger in writing if his or her name is cleared and contacts the appropriate parties, including the airlines, in an effort to streamline future check-ins.

In cases where an individual's name is on a watch list, the OTSR works with the TSC and the nominating agency to determine if the derogatory information is accurate and if the name is on the list appropriately.

In cases where an individual's name matches a name on the watch lists, but it is determined not to be the suspected individual, then the name is entered into the cleared list.

The current TSA redress process, including the use of the cleared list, is not always effective because the ability and consistency of individual carriers in applying the cleared list varies widely. In published news reports and complaints to CRCL, individuals who have gone through the process have stated that they continue to experience inconvenience, while their identities are verified.<sup>49</sup> The effectiveness of the redress process is expected to increase significantly when screening responsibilities are taken over by the U.S. Government in connection with the Secure Flight rule.

### **C. Redress at CBP**

CBP has a Customer Satisfaction Unit that is responsible for handling complaints from the public about interaction with CBP. The Customer Satisfaction Unit addresses all complaints and does not track complaints about No-fly and Selectee lists separately.

---

<sup>48</sup> Available at <[http://www.tsa.gov/interweb/assetlibrary/PIV\\_Form.pdf](http://www.tsa.gov/interweb/assetlibrary/PIV_Form.pdf)>, last visited June 9, 2005.

<sup>49</sup> See, for example, the experience of ACLU attorney David Fathi described in S. Waterman, *Senator Gets a Taste of No-fly List Problems*, Washington Times, August 20, 2004, available at <<http://www.washingtontimes.com/upi-breaking/20040819-082444-1551r.htm>>, last visited June 7, 2005.

The office is usually contacted by letter. It performs research on the issue raised in the complaint, sometimes contacting the complainant by telephone or letter to gather additional information. In cases where other agencies are involved, the Customer Satisfaction Unit either forwards the complaints to the appropriate agency or works with other agencies to address the complaint.

When an individual is found to have been misidentified on the No-fly or Selectee list, the individual is sent a letter, stating that CBP has taken appropriate action. If the letter is not recognized by officers of CBP at the port of entry or exit, the individual can either complain directly to the Port Director or can arrange pre-clearance in order to facilitate travel from the specific port. If research indicates that the individual was appropriately identified as being on the list, the Customer Satisfaction Unit works with field offices to determine whether the record continues to be valid.

#### ***D. Redress at CRCL***

In addition to contacting the agencies themselves, individuals who feel that they are being unfairly denied boarding or being singled out for screening have contacted the DHS Office for Civil Rights and Civil Liberties (CRCL). CRCL is authorized by statute to receive and review complaints from the general public related to allegations of discrimination and violations of due process and to oversee Departmental compliance with constitutional, statutory, regulatory, and policy requirements relating to the civil rights and civil liberties of individuals.

The bulk of the complaints received by CRCL in relation to No-fly and Selectee lists are from citizens who have been delayed at airports because they have been selected for additional screening, have been told that they cannot board a plane, or have been removed from a plane. Most of the complaints include an implication (if not an outright allegation) that the complainant was targeted because of his or her religion, race or national origin. For example, CRCL has received complaints alleging that officers have asked travelers questions about their religion and national origin, whether one traveler knew anyone at his mosque who hates Americans or disagrees with current policies, targeted a traveler for additional screening because she wore traditional Muslim attire and told another traveler that he and his wife and children were subjected to body searches because he was born in Iraq, is Arab, and Muslim. Other complaints alleged misconduct or disrespect by airline, law enforcement, TSA or CBP officials. CRCL has also received several complaints regarding children who are alleged to have appeared on No-fly and Selectee lists. These complaints are generally accompanied by implicit claims of racial, ethnic, or religious profiling.

Most of the complaints received by CRCL include allegations that indicate that airline or TSA employees may be somewhat inconsistent in the manner in which they discuss

Selectee and No-Fly Lists issues with the public. From these allegations, the possibility emerged that employees and agents might be unsure about what they should or can say to travelers regarding the Selectee or No Fly Lists. Inconsistent statements regarding the lists can breed unfounded suspicion that race, religion, or national origin serve as the basis for placement on these lists. Thus, continuing guidance may be needed for TSA employees and agents to ensure consistent statements to the public regarding Selectee and No-Fly List issues.

When CRCL receives complaints, it works to resolve them with the appropriate component within DHS. For example, when complaints arose regarding children who allegedly appeared on No-fly and Selectee lists, CRCL worked with the TSA Office of the Chief Counsel, TSIS, the TSA Ombudsman, the TSA Office of Civil Rights, and the American-Arab Anti-Discrimination Committee (ADC) to increase awareness to ensure that airlines use sound judgment in determining whether a name on a No-fly List is reasonably connected to an individual seeking to board a plane.<sup>50</sup>

#### ***E. Redress Through the DHS Privacy Office***

In addition to contacting the agencies themselves, individuals who feel that they are being unfairly denied boarding or being singled out for screening have contacted the DHS Privacy Office. The Privacy Office is authorized by statute to receive complaints from the general public related to allegations of privacy violations, including mis-handling or mismatching of personal information and violations of the Privacy Act notices or Privacy Impact Assessments of the various programs.

The bulk of the complaints received by the Privacy Office in relation to No-fly and Selectee lists are from individuals concerned about the use of personal information in the screening process. These complaints emanate from U.S. persons as well as international persons and foreign data protection authorities acting on behalf of nationals of their countries. These complaints are premised on allegations that too much data is being collected, or that data that is inaccurate or that pertains to another individual is being associated with a particular traveler.

When the DHS Privacy Office receives complaints, it works to resolve them with the appropriate component within DHS. For example, when concerns were expressed regarding CBP's processing of international passengers, the DHS Privacy Office worked with CBP's Office of Legal Counsel and Office of Field Operations to review the

---

<sup>50</sup> *TSA Improves 'No Fly' List Procedures*, April 17, 2005, available at <<http://www.adc.org/index.php?id=2484>>, last visited on July 7, 2005.

substance and amount of data used in passenger vetting and worked to respond to several international data protection commissioners.

#### ***F. Redress at the TSC***

The TSC does not deal directly with the public and currently has no plans to establish an Office of the Ombudsman.<sup>51</sup> Nevertheless, it has a role in redress. Screening agencies work with TSC to determine whether an individual who has complained about unfair targeting is appropriately included in watch lists. TSC works with its own data and with the nominating agencies to examine the case and to make a determination. TSC is also working with screening agencies to create a set of processes that would help misidentified persons<sup>52</sup> and has established a Redress office to facilitate the process among and between federal agencies.<sup>53</sup>

#### **VII. Issues for Consideration**

Based on our current findings, we offer the following issues and recommendations for consideration in the operation of No-fly and Selectee lists and possible expansion of these lists to other modes of transport. These recommendations reflect our belief that an effective screening program would enhance the nation's ability to fight terrorism.

- **Standards for No-Fly, Selectee, and Other “No Transport” Lists** As these lists are used in more contexts, there is a potential that criteria for putting individuals on these lists will become less focused. Criteria for inclusion on such lists must be strong and consistently applied. Further, routine auditing and appropriate oversight of standards for inclusion of individuals on the consolidated terrorist watch list or the export of that individual identity for inclusion on one of its subsets, such as the No-fly and Selectee lists, is necessary, particularly at the nominating agency level. Consistent oversight of the application of the subsets of the consolidated watch list to screening processes and other operations is necessary to ensure adherence to privacy and fair information principles, as well as for consideration of other civil liberties impact. Procedures should be in place to periodically review the lists in order to determine whether those who are on the list continue to be appropriately listed, and to ensure continued relevance of the criteria to the use of the list.

---

<sup>51</sup> U.S. Department of Justice (2005), p. 97.

<sup>52</sup> U.S. Department of Justice (2005), pp. 74-75.

<sup>53</sup> U.S. Department of Justice (2005), p. 97.

- **Screening in Modes Other Than Aviation** The 9-11 Commission recommended that aviation-related watch list screening be performed by the government in order to improve security of watch lists and to permit the government to use all available terrorism-related information. Consideration should be given to which are the appropriate entities to collect travel-related information and to use it for screening in other modes of transportation. The questions of relevance of the selection criteria, the amount of actual data contained on the lists, and the impact on privacy and civil liberties must be routinely considered going forward if the use of the No-fly and Selectee lists is expanded to other modes of transportation beyond aviation. Expanding the use of No-fly and Selectee lists for screening many or all transportation systems, because of its potential to deprive individuals of all means of travel, has greater legal and personal implications than the use of these lists to screen solely airline passengers. Additionally, the logistics, cost and practicality of using watch lists in other modes must be given serious consideration.
- **Other Appropriate Uses for Information Collected for Terrorist Screening Purposes** In order to effectively perform screening, the government must collect personal information. It must also compare this information to information available in various databases, including general law enforcement databases. This raises the concern that terrorist screening programs will possibly evolve into routine law enforcement tools for other purposes. Such evolution from terrorism screening to routine, general law enforcement tools for unspecified purposes would raise concerns about further privacy incursion. The question of appropriate uses of screening information and appropriate oversight for such programs must be considered on an ongoing basis, not only at the inception of a program, but throughout its operation.
- **Appropriate Mechanisms and Venues for Redress in the Case of Misidentified Individuals or Individuals Who Are Placed on Watch Lists Improperly.** Access and redress are fundamental components of a program's adherence to fair information principles, and the resulting public trust that ensues from such policies. Currently different agencies have different redress processes, and these processes vary in effectiveness. A robust redress program is essential for any federal program that uses personal information in order to grant or deny to individuals a right, privilege or benefit. If watch-list screening is applied to modes of transport other than aviation, quick and effective redress will become increasingly important. Inclusion of a robust, effective redress process should be an essential element of any current or future federal screening program.

The Privacy Office believes that the current TSC standards for No-fly and Selectee lists are sufficiently narrow, while still broad enough to be effective for screening purposes. In reaching this conclusion, the Privacy Office primarily examined the standards from a privacy and fair information principles perspective rather than from a law enforcement perspective because the law enforcement decision about the risk to aviation security posed by an individual or his associates is for other offices to make.

The more the lists expand beyond individuals who are believed to pose a potential threat to civil aviation, however, the greater the likelihood that some individuals, whose relationship to aviation security is only speculative, will be subjected to additional screening or prevented from traveling. If there is no relationship between the threat to civil aviation and the placement of an individual on a watch list that restricts the individual's ability to travel, there may be an insufficient predicate reason to interfere with the ability to travel.

#### **VIII. Conclusion**

The Privacy Office again recognizes the excellent work and collaboration of the Terrorist Screening Center leadership and the Department of Homeland Security leadership in preparing this report to Congress on the Privacy and Civil Liberties Impact of the No-fly and Selectee lists.

At this time, the Privacy Office believes that great progress has been made in the government's operation of No-fly and Selectee lists to enhance aviation security while respecting personal privacy. Challenges certainly remain in partnering effectively with the private sector and translating this information to end uses in a manner that minimizes the impact on innocent travelers. The Privacy Office looks forward to working with the TSC, the TSA, and the Department of Homeland Security leadership as we work to improve the accuracy and the adequacy of screening mechanisms and the underlying information sources in a manner that is at once successful and efficient as well as respectful of the privacy of our citizens and visitors to this country.