COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

DEPARTMENT OF HOMELAND SECURITY
TRANSPORTATION SECURITY ADMINISTRATION
Docket Nos. TSA-2007-28972, TSA-2007-28572

I. INTRODUCTION

By notices published on August 23, 2007, the Department of Homeland Security ("DHS") announced a new system of records notice, notice of proposed rulemaking, proposed rule, and revised Privacy Impact Assessment ("PIA") for the Secure Flight passenger prescreening program run by the Transportation Security Administration ("TSA").[1] According to DHS, under Secure Flight "TSA would receive passenger and certain non-traveler information, conduct watch list matching against the No Fly and Selectee portions of the Federal Government's consolidated terrorist watch list, and transmit boarding pass printing instructions back to aircraft operators."[2]

The Electronic Privacy Information Center ("EPIC") has submitted a series of comments concerning traveler screening systems undertaken by federal entities. Earlier this month, we urged DHS to curtail the revised Automated Targeting System ("ATS"), a federal screening system that creates secret, terrorist ratings on tens of millions of

---

[1] Dep't of Homeland Sec., *Notice of proposed rulemaking: Implementation of Exemptions; Secure Flight Records*, 72 Fed. Reg. 48,397 (Aug. 23, 2007) [hereinafter "Secure Flight NPRM"], *available at* http://edocket.access.gpo.gov/2007/E7-15963.htm; Dep't of Homeland Sec., *Secure Flight Plan; Proposed Rule*, 72 Fed. Reg. 48,355 (Aug. 23, 2007) [hereinafter "Secure Flight Proposed Rule"], *available at* http://edocket.access.gpo.gov/2007/E7-15960.htm; Dep't of Homeland Sec., *Notice to establish system of records: Secure Flight Records,* 72 Fed. Reg. 48,392 (Aug. 23, 2007), *available at* http://edocket.access.gpo.gov/2007/E7-15964.htm; and Privacy Office, Dep't of Homeland Sec., *Privacy Impact Assessment for the Automated Targeting System*, Aug. 9, 2007 [hereinafter "Secure Flight Revised Privacy Impact Assessment"], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_secureflight.pdf.

[2] Secure Flight Proposed Rule at 48,356, *supra* note 1.

American citizens.[3] (Last year, EPIC led a coalition of 29 organizations and 16 privacy and technology experts that detailed significant privacy and security risk in ATS.[4]) In February 2007, we explained that TSA's "internal quality assurance procedures" were not working, and urged the agency to fully apply Privacy Act requirements of notice, access, and correction to the new traveler redress program called "TRIP" and its underlying watch list system.[5]

In May 2006, we recommended that Customs and Border Protection ("CBP") substantially narrow the Privacy Act exemptions prior to the revision and expansion of the Global Enrollment System, a database full of individuals' biometric and biographic data, which would be used to determine individual eligibility for the "Trusted Traveler" program.[6] In December 2005, EPIC detailed privacy and security flaws in the Registered Traveler program and recommended DHS suspend the passenger prescreening program.[7]

In October 2004, EPIC submitted comments on the original Secure Flight system of records notice.[8] We detailed numerous security and privacy flaws in the system. In February 2006, TSA suspended Secure Flight for a "comprehensive review." Though the program has been substantially changed, significant problems remain. Today, we write to

---

[3] EPIC, *Comments on Docket Nos. DHS-2007-0042 and DHS-2007-0043 Concerning the Automated Targeting System* (Sept. 5, 2007), *available at* http://www.epic.org/privacy/travel/ats/epic_090507.pdf.
[4] Thirty Orgs. & 16 Privacy & Tech. Experts, *Comments on Docket No. DH6-2006-0060: Notice of Privacy Act System of Records* (Dec. 4, 2006), *available at* http://epic.org/privacy/pdf/ats_comments.pdf.
[5] EPIC, *Comments on Docket Nos. DHS-2007-0003: Implementation of Exemptions; Redress and Response Records System* (Feb. 20, 2007) [hereinafter "EPIC Comments on TRIP"], *available at* http://www.epic.org/privacy/airtravel/profiling/trip_022007.pdf.
[6] EPIC, *Comments on Docket No. DHS-2005-0053: Notice of Revision and Expansion of Privacy Act System of Records* (May 22, 2006), *available at* http://www.epic.org/privacy/airtravel/ges052206.pdf.
[7] EPIC, *Comments on Docket Nos. TSA-2004-19166 and TSA-2004-17982: Notice to Alter Two Existing Systems of Records; Request for Comments* (Dec. 8, 2005), *available at* http://www.epic.org/privacy/airtravel/profiling/rt120805.pdf.
[8] EPIC, *Comments on Docket No. TSA-2004-19160: Privacy Act Notice and Privacy Impact Assessment, Secure Flight Test Records*, (Oct. 25, 2004) [hereinafter EPIC's 2004 Secure Flight Comments"], *available at* http://www.epic.org/privacy/airtravel/sf_comments_tsa.pdf.

urge DHS and TSA to substantially revise its Privacy Act notice for the Secure Flight system to address these problems. Further, Secure Flight should remain suspended and the agency should not acquire personal data, even for testing purposes, until it has revised its Privacy Act notice as we describe below.

II. WHAT IS SECURE FLIGHT?

Under the Aviation and Transportation Security Act of 2002, the Transportation Security Administration was authorized to maintain watch lists of names of individuals suspected of posing "a risk of air piracy or terrorism or a threat to airline or passenger safety."[9] Documents obtained in 2002 by EPIC from TSA under the Freedom of Information Act established that the agency administers two lists: a "no fly" list and a "selectee" list.[10] The airlines run passenger names against the watch lists.

When a passenger checks in for a flight, he may be labeled a threat if his name matches an entry on one of the watch lists, even if he is not the person actually on the list. A match to the "no fly" list requires the airline to notify TSA and to call a law enforcement officer to detain and question the passenger. In the case of a Selectee, an "S" or special mark is printed on the individual's boarding pass and the person receives additional security screening. Customs and Border Protection also uses the lists to screen travelers. Many travelers have reported problems with being mistakenly matched to names on watch lists.

TSA introduced Secure Flight in August 2004, shortly after the agency abandoned plans for its predecessor, the second generation Computer Assisted Passenger

[9] Pub. L. No. 107-71, 115 Stat. 597 (2002).
[10] EPIC, *Documents Show Errors in TSA's "No-Fly" Watchlist*, http://www.epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html.

Prescreening System ("CAPPS II"). Secure Flight was intended to compare passenger information from Passenger Name Records ("PNRs"), which contain data given by passengers when they book their flights, against watch lists maintained by the federal government. However, Secure Flight morphed from a simple system of comparing names to watch lists to a complex system where profiles are created on passengers in order to assess the threat that they pose.[11] TSA sought to identify "suspicious indicators associated with travel behavior" in passengers' itinerary PNR data.[12]

TSA began testing Secure Flight in early 2005, and officials claimed the program would solve the numerous problems of innocent travelers being mistakenly matched to watch list names. However, a Government Accountability Office ("GAO") report and testimony found that TSA approved Secure Flight to become operational in September 2005 despite inconclusive risk assessments and 144 known security vulnerabilities.[13] In addition to criticizing Secure Flight's lack of privacy and security safeguards, GAO noted that the documents underlying the program "contained contradictory and missing information."[14] In February 2006, the head of TSA told a congressional committee that Secure Flight was suspended for a comprehensive review of the program's information security measures following the critical GAO report.[15]

---

[11] Dep't of Homeland Sec., *Notice to Establish System of Records, Secure Flight Test Records*, 69 Fed. Reg. 57,345 (Sept. 24, 2004), *available at* http://edocket.access.gpo.gov/2004/04-21479.htm.
[12] *Id*. at 57,346.
[13] Cathleen Berrick, Dir., Homeland Sec. & Justice, Gov't Accountability Office, *Statement at a Hearing on TSA's Secure Flight and Registered Travelers Programs Before the S. Comm. on Commerce, Science & Transportation*, 109th Cong. (Feb. 9, 2006), *available at* http://www.gao.gov/new.items/d06374t.pdf.
[14] *Id*.
[15] Edmund S. "Kip" Hawley, Nominee for Assistant Sec'y of Homeland Sec., Transp. Sec. Admin., Dep't of Homeland Sec., *Testimony at Hearing on TSA's Secure Flight and Registered Travelers Programs Before the S. Comm. on Commerce, Science & Transportation*, 109th Cong. (Feb. 9, 2006).

In August, TSA detailed a revised Secure Flight program in which "TSA would receive passenger and certain non-traveler information, conduct watch list matching against the No Fly and Selectee portions of the Federal Government's consolidated terrorist watch list, and transmit boarding pass printing instructions back to aircraft operators."[16] TSA said Secure Flight would return to its original purpose and be used to conduct watch-list matching.

III. SECURE FLIGHT GATHERS AND RETAINS VAST AMOUNT OF DATA

Under Secure Flight, TSA will gather "Secure Flight Passenger Data (SFPD) from certain U.S. aircraft operators and foreign air carriers for the purpose of passenger watch list matching against the No Fly and Selectee list components of the Terrorist Screening Database."[17] The required and "voluntary" data gathered and retained by TSA under Secure Flight could lead to traveler dossiers.

TSA will "require" the passenger and airlines to submit the traveler's full name, "reservation control number, the record sequence number, the record type, the passenger update indicator, the traveler reference number, and the itinerary information" at least 72 hours before the flight.[18] TSA will also "require" aircraft operators to request from the individual "date of birth, gender, redress number (if available), known traveler number (if implemented and available), and passport information (if available)."[19]

It is doubtful that submission of this personal data would truly be "voluntary." Aircraft operators are required to request this data from passengers and post this privacy notice:

---

[16] Secure Flight Proposed Rule at 48,356, *supra* note 1.
[17] Secure Flight Revised Privacy Impact Assessment at 2, *supra* note 1.
[18] Secure Flight Proposed Rule at 48,371, *supra* note 1.
[19] Secure Flight Revised Privacy Impact Assessment at 2, *supra* note 1.

> The Transportation Security Administration requires us to collect information from you for purposes of watch list matching, under the authority of 49 U.S.C. sec. 114, and the Intelligence Reform and Terrorism Prevention Act of 2004. Providing this information is voluntary; *however, if it is not provided, you may be subject to additional screening or denied transport or authorization to enter a sterile area.* TSA may share information you provide with law enforcement or intelligence agencies or others under its published system of records notice. For more on TSA Privacy policies or to view the system of records notice and the privacy impact assessment, please see TSA's Web site at http://www.tsa.gov. (emphasis added)[20]

The "privacy notice" required by TSA includes the ominous statement that if an individual does not "volunteer" this information, "you may be subject to additional screening or denied transport or authorization to enter a sterile area."[21] It hardly seems voluntary, but more like TSA is stating, "Give us your data or else."

Indeed, if the traveler has submitted such data to the airline in another capacity, such as through the airline's frequent flier program, the data would be transmitted to TSA without the traveler's knowledge.[22] The DHS Privacy Office states in its Privacy Impact Assessment of the Secure Flight proposal:

> A covered aircraft operator may, in the ordinary course of business and as part of its reservation process, input data that TSA requires covered aircraft operators to request from individuals, but that the individual did not provide at the time of reservation, such as data from a passenger profile stored by the aircraft operator. In these situations, the aircraft operator would be required to include that data as part of the SFPD transmitted to TSA . . .[23]

This is not voluntary submission of personal data by the traveler, but secret gathering by TSA. It is questionable for a government agency to surreptitiously gather data on an individual that resides in commercial data files, especially when the agency has told the individual that she has a right to refuse to submit this data.

---

[20] Secure Flight Proposed Rule at 48,372, *supra* note 1.
[21] *Id*.
[22] *Id*. at 48,364.
[23] Secure Flight Revised Privacy Impact Assessment at 7, *supra* note 1.

Also, it is strange that TSA would force such data from travelers, as the data itself is not crucial to Secure Flight. As TSA explains in the Secure Flight proposal, "[f]or the vast majority of individuals, a decision to forgo providing these data elements should have no effect on their watch list matching results and will result in less information being held by TSA."[24]

Forced accumulation of data is the first step toward creating dossiers on travelers under Secure Flight. The second step concerns the proposed redress and known traveler numbers. As defined by TSA, the known traveler number "would be a unique number assigned to 'known travelers' for whom the Federal Government has already conducted a terrorist security threat assessment and has determined do not pose a terrorist security threat. The known traveler number would enable TSA to identify these 'known travelers.'"[25] The redress number would be a similar "unique number" to identify those who had used the DHS Traveler Redress Inquiry Program.[26] With such unique numbers, TSA could track the travel records of these individuals though they have proven themselves to be mistakenly matched or listed on the watch lists used by Secure Flight.

The data retention proposal also raises the possibility of tracking these innocent travelers. Though the majority of travelers' data will be retained for only seven days, "for individuals who are potential matches would be retained for seven years after the completion of the individual's directional travel."[27] As individuals would likely acquire "known traveler numbers" or "redress numbers" only after they have already been mistakenly matched to the watch lists, this could mean that each time the "known

[24] Secure Flight Proposed Rule at 48,363, *supra* note 1.
[25] *Id*. at 48,365.
[26] *Id*. at 48,359.
[27] *Id*. at 48,363.

traveler" boards a plane, TSA will have a detailed profile including their personal data and travel records for seven years at a time.

IV. SECURE FLIGHT COULD RESTRICT INDIVIDUALS' RIGHT TO TRAVEL

The Supreme Court has long recognized that citizens enjoy a constitutional right to travel. In *Saenz v. Roe*, the Court noted that the "'constitutional right to travel from one State to another' is firmly embedded in our jurisprudence."[28] Indeed, in 2003, then-DHS Deputy Secretary Admiral James Loy observed that "the founding fathers . . . had mobility as one of the inalienable rights they were talking about."[29] For that reason, any government initiative that conditions the ability to travel upon the surrender of privacy rights requires particular scrutiny. Secure Flight would affect "more than 2.4 million passengers per day," more than 876 million individuals per year.[30] Secure Flight could bar individuals from air travel completely if the person does not present a "verifying identity document," as defined by TSA, even if the person does not pose a definable security threat.

Under the Secure Flight proposal, there are circumstances in which, if a passenger does not present a "verifying identity document," then "the covered aircraft operator must not issue a boarding pass or give authorization to enter a sterile area to that individual and must not allow that individual to board an aircraft or enter a sterile area, unless otherwise authorized by TSA."[31] A "verifying identity document," is defined by TSA as "an unexpired passport issued by a foreign government or an unexpired document issued by a

[28] 526 U.S. 489 (1999), quoting *United States v. Guest*, 383 U.S. 745 (1966).
[29] Admiral James L. Loy, Deputy Sec'y, Dep't of Homeland Sec., *Testimony before H. Gov. Reform Subcom. on Tech., Info. Policy, Intergovernmental Relations and the Census*, 106th Cong. (May 6, 2003).
[30] Secure Flight Proposed Rule at 48,360, *supra* note 1.
[31] *Id.* at 48,390.

government (Federal, State, or tribal) that includes the following information for the individual: (1) Full name. (2) Date of birth. (3) Photograph of the individual."[32]

Currently, if a person does not present valid identification such as a state driver's license because he lost, forgot or had stolen his identification document, then the person can choose to submit to "secondary screening" in order to gain admittance to his flight.[33] "Secondary screening" is a more extensive search of a person and her belongings.

There are questions as to whether travelers will be able to present what DHS defines as a valid "verifying identity document." Travelers may not be able to afford such a document, which would be either a REAL ID compliant identity card or an expensive passport. REAL ID is a national identification system in which DHS imposes federal technological standards and verification procedures on state driver's licenses and identification cards, many of which are beyond the current capacity of the federal government, and mandates state compliance by May 2008.[34]

In May, EPIC and 24 experts in privacy and technology submitted comments on DHS's draft regulations for the REAL ID Act warning the federal agency not to go forward with the national identification system.[35] The group said that the ill-conceived plan would create new security risks for the American public, such as increasing the risk of and the damage caused by identity theft. "DHS has the obligation to protect the privacy of citizens affected by this system and must do more than the feeble attempts set

---

[32] *Id*. at 48,388.
[33] *Gilmore v. Gonzales*, 435 F.3d 1125 (9th Cir. 2006).
[34] *See generally*, EPIC, Spotlight on Surveillance, *Federal REAL ID Proposal Threatens Privacy and Security* (Mar. 2007), http://www.epic.org/privacy/surveillance/spotlight/0307/.
[35] EPIC and 24 Experts in Privacy and Technology, *Comments on Docket No. DHS 2006-0030: Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes* (May 8, 2007), *available at* http://www.epic.org/privacy/id_cards/epic_realid_comments.pdf.

out in the draft regulations," the group said.[36] Seventeen states have passed legislation against REAL ID.[37] There are bills to repeal REAL ID in the U.S. House and Senate.

In a speech to the National Conference of State Legislatures in August, DHS Secretary Michael Chertoff said that although REAL ID "is not a mandate," states would be punished for non-compliance.[38] He said that citizens in states that do not implement REAL ID would have to use passports for federal purposes, such as entering courthouses or flying domestically.[39] Passports currently cost $97 each, and the State Department admitted in July that there is a significant backlog in processing passports because of, among other things, "inept planning, underfunded preparations, and popular misunderstanding of poorly crafted government advertising."[40]

Secure Flight's "verifying identity document," would be a REAL ID national identity card or a high-cost passport, which would be prohibitively expensive for some. In some situations under the proposal Secure Flight would require that an airline prevent an individual who does not present a "verifying identity document" from boarding a flight "unless otherwise authorized by TSA."[41] It is unknown what measurements TSA would use to "otherwise authorize[]" an individual to board.

V. SECURE FLIGHT'S BROAD EXEMPTIONS CONTRAVENE INTENT OF PRIVACY ACT OF 1974

Adherence to Privacy Act requirements is critical for a system such as Secure Flight, which seeks to allow or deny the ability to travel for all air travelers (domestic at

[36] *Id*. at 8.
[37] *See generally*, EPIC's page on National ID Cards and the REAL ID Act, http://www.epic.org/privacy/id_cards/.
[38] Eliott C. McLaughlin, *Federal ID plan raises privacy concerns,* CNN, Aug. 16, 2007.
[39] *Id*.
[40] *Official takes blame for passport mess*, Associated Press, July 23, 2007.
[41] Secure Flight Proposed Rule at 48,390, *supra* note 1.

this time, though TSA expects to phase in the international portion at a later date). TSA proposes to exempt Secure Flight from key fair information practices, such as the requirements that an individual be permitted access to personal information, that an individual be permitted to correct and amend personal information, and that an agency assure the reliability of personal information for its intended use.[42] It is inconceivable that the drafters of the Privacy Act would have permitted such a system to be granted broad exemptions from Privacy Act obligations.

Though we detailed in our October 2004 comments the many ways in which Secure Flight's exemptions contravened the intent of the Privacy Act of 1974, broad exemptions remain in this new system of records notice.[43] TSA proposes exempting Secure Flight from all Privacy Act provisions guaranteeing citizens the right to access records containing information about them and provisions defining the government's obligation to allow citizens to challenge the accuracy of information contained in their records. TSA does not assert exemptions "with respect to information submitted by or on behalf of individual passengers or non-travelers in the course of making a reservation or seeking access to a secured area under the Secure Flight program."[44]

The exemptions proposed by TSA are: "5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (5), and (8); (f), and (g))" pursuant to 5 U.S.C. 552a(j)(2) and (k)(2))."[45] These provisions of the Privacy Act ensure:

- an agency must give individuals access to the accounting of disclosure of their records[46];

[42] Secure Flight NPRM at 48,399, *supra* note 1; *see generally* 5 U.S.C. § 552a (1974).
[43] *See generally* EPIC's 2004 Secure Flight Comments, *supra* note 8.
[44] Secure Flight NPRM at 48,399, *supra* note 1.
[45] *Id*.
[46] 5 U.S.C. § 552a(c)(3).

- any agency or individual to whom the records are disclosed must also receive "any correction or notation of dispute"[47];

- individual may request access to records an agency maintains about him or her[48];

- an agency must correct identified inaccuracies promptly;[49]

- an agency must make notes of requested amendments within the records;[50]

- an agency must ensure it only collects data "relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive order of the President"[51];

- an agency must "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs"[52];

- each individual must be informed whom the agency asks to supply information[53];

- an agency must publish a notice of the existence of records in the Federal Register, along with the procedures to be followed to obtain access[54];

- an agency must establish procedures to handle disputes between the agency and individual as to the accuracy of the records[55]; and,

- an individual may seek judicial review to enforce the statutory right of access provided by the Act.[56]

As we have previously explained, when it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal data that Federal agencies could collect and required agencies to be transparent in their information practices.[57] In 2004,

[47] 5 U.S.C. § 552a(c)(4).
[48] 5 U.S.C. § 552a(d)(1).
[49] 5 U.S.C. § 552a(d)(2)(B), (d)(3)
[50] 5 U.S.C. § 552a(d)(4).
[51] 5 U.S.C. § 552a(e)(1).
[52] 5 U.S.C. § 552a(e)(2).
[53] 5 U.S.C. § 552a(e)(3).
[54] 5 U.S.C. §§ 552a(e)(4)(G), (e)(4)(H), (f).
[55] 5 U.S.C. § 552a(f)(4).
[56] 5 U.S.C. § 552a(g)(1).
[57] S. Rep. No. 93-1183 at 1 (1974).

the Supreme Court underscored the importance of the Privacy Act's restrictions upon agency use of personal data to protect privacy interests, noting that:

> [I]n order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary . . . to regulate the collection, maintenance, use, and dissemination of information by such agencies." Privacy Act of 1974, §2(a)(5), 88 Stat. 1896. The Act gives agencies detailed instructions for managing their records and provides for various sorts of civil relief to individuals aggrieved by failures on the Government's part to comply with the requirements.[58]

The Privacy Act is intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government[.]"[59] It is also intended to protect the privacy interests of citizens and lawful permanent residents against government intrusion. Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[60] It thus sought to "provide certain protections for an individual against an invasion of personal privacy" by establishing a set of procedural and substantive rights.[61]

The rights of access and correction were central to what Congress sought to achieve through the Privacy Act:

> The committee believes that this provision is essential to achieve an important objective of the legislation: Ensuring that individuals know what Federal records are maintained about them and have the opportunity to correct those records. The provision should also encourage fulfillment of another important objective: maintaining government records about individuals with such accuracy, relevance,

[58] *Doe v. Chao*, 540 U.S. 614, 618 (2004).
[59] S. Rep. No. 93-1183 at 1.
[60] 5 U.S.C. § 552a.
[61] *Id.*

> timeliness, and completeness as is reasonably necessary to assure fairness to individuals in making determinations about them.[62]

DHS's notice establishes a system that provides neither adequate access nor the ability to amend or correct inaccurate, irrelevant, untimely and incomplete records. TSA allows individuals to petition through the Traveler Redress Inquiry Program or through Privacy Act requests to access any passenger name record ("PNR") data that the individual himself gave to an air carrier or travel agent, but no other information in Secure Flight files.[63] By refusing to allow access to all Secure Flight data except that which the individual has personally provided, the Department of Homeland Security seeks to keep Secure Flight determinations opaque and arbitrary.[64]

VI. WATCH LISTS USED BY SECURE FLIGHT ARE RIDDLED WITH ERRORS

According to the Privacy Impact Assessment for Secure Flight, the DHS Privacy Office states TSA will gather "Secure Flight Passenger Data (SFPD) from certain U.S. aircraft operators and foreign air carriers for the purpose of passenger watch list matching against the No Fly and Selectee list components of the Terrorist Screening Database."[65] EPIC and others have repeatedly explained that the Terrorist Screening Database and its watch lists are filled with errors, inaccurate and incomplete data.

Earlier this month, the Justice Department's Inspector General's review of the Terrorist Screening Center found that the government's watch lists of known or suspected terrorists remain filled with errors that the Inspector General said could obstruct the

[62] H.R. Rep. No. 93-1416, at 15 (1974).
[63] Secure Flight Revised Privacy Impact Assessment at 23-24, *supra* note 1.
[64] *See* Section VI: Secure Flight's Redress Procedures Are Inadequate and Flawed, *infra*.
[65] Secure Flight Revised Privacy Impact Assessment at 2, *supra* note 1.

capture of terrorists.[66] "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."[67]

The Inspector General was highly critical of the system, detailing a number of errors in the watch lists and said the data collection and dissemination structure helped cause "inaccurate and incomplete watchlist records."[68] In fact, problems at the Center meant that "several known or suspected terrorists" were not on the lists, though they should be.[69] The Inspector General said, "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*" (emphasis added).[70]

Since the watch lists were created in 2004, they have more than quadrupled to include more than 700,000 records as of April, and they continue "to increase by an average of over 20,000 records per month."[71] Accuracy and reliability problems were in part caused by this massive number of records and the Terrorist Screening Center's "weak quality assurance process."[72] The Justice Department Inspector General found the Center "continues to lack important safeguards for ensuring data integrity, including a

---

[66] Office of Inspector General, Dep't of Justice, *Follow-Up Audit of the Terrorist Screening Center, Audit Report 07-41 (Redacted for Public Release) (*Sept. 2007) [hereinafter "Justice Dept. Report on Watch Lists"], *available at* http://www.usdoj.gov/oig/reports/FBI/a0741/final.pdf.
[67] *Id*. at iii.
[68] *Id*. at ii-iii, 61.
[69] *Id*. at ii.
[70] *Id*. at xxii.
[71] Justice Dept. Report on Watch Lists at iii, *supra* note 66.
[72] *Id*.

comprehensive protocol outlining the agency's quality assurance procedures and a method for regularly reviewing the work of its staff."[73]

In August, it was revealed that "the government's terrorist screening database flagged Americans and foreigners as suspected terrorists almost 20,000 times last year. But only a small fraction of those questioned were arrested or denied entry into the United States."[74] Customs and Border Protection logged about 10,000 of those encounters, but only "turned back or handed over to authorities 550, most of them foreigners."[75]

There have been myriad stories about mistakes associated with the watch lists, with sometimes chilling results. An April 2006 report by the Department of Homeland Security's Privacy Office on the impact of the watch lists explained that "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."[76] The report described complaints "alleg[ing] misconduct or disrespect by airline, law enforcement, TSA or CBP officials" toward people mistakenly matched.[77] According to the Privacy Office:

> 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

---

[73] *Id*.
[74] Fed. Bureau of Investigations, Dep't of Justice, *FY 2008 Authorization Budget Request to Congress* (2007), *available at* http://www.fas.org/irp/agency/doj/fbi/2008just.pdf; Ellen Nakashima, *Terror Suspect List Yields Few Arrests*, Wash. Post, Aug. 25, 2007.
[75] *Id*.
[76] Privacy Office, Dep't of Homeland Sec., *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* i (Apr. 27, 2006), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_nofly.pdf.
[77] *Id*. at 18.

> asked […] 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.[78]

Also, documents obtained by EPIC under the Freedom of Information Act show nearly a hundred complaints from airline passengers between November 2003 and May 2004 about the government's traveler screening security measures.[79] The complaints describe the bureaucratic maze passengers encounter if they happen to be mistaken for individuals on the list, as well as the difficulty they encounter trying to exonerate themselves through the redress process. One person named in the documents, Sister Glenn Anne McPhee, U.S. Conference of Catholic Bishops' secretary for education, spent nine months attempting to clear her name from a TSA watch list. The process was so difficult, Sister McPhee told a reporter, "Those nine months were the closest thing to hell I hope I will ever experience."[80]

In January, at a hearing of the Senate Commerce Committee, Sen. Ted Stevens complained that his wife, Catherine, is frequently mismatched to the watch list name "Cat Stevens."[81] Senators Ted Kennedy and Don Young are among those who have been improperly flagged by watch lists.[82] Sen. Kennedy was able to resolve the situation only by enlisting the help of then-Homeland Security Secretary Tom Ridge.

---

[78] *Id.*
[79] Transp. Sec. Admin., Dep't of Homeland Sec., *Complaint Log: Nov. 2003 to May 2004,* obtained by EPIC through FOIA litigation, *available at* http://www.epic.org/privacy/airtravel/foia/complaint_log.pdf.
[80] Ryan Singel, *Nun Terrorized by Terror Watch*, Wired News, Sept. 26, 2005.
[81] Beverley Lumpkin, *Aviation Security Chief Says No-Fly List is Being Reduced by Half*, Associated Press, Jan. 18, 2007.
[82] *See, e.g.,* Sara Kehaulani Goo, *Committee Chairman Runs Into Watch-List Problem*, Wash. Post, Sept. 30, 2004; Leslie Miller, *House Transportation Panel Chairman Latest to be Stuck on No-Fly List*, Associated Press, Sept. 29, 2004; Shaun Waterman, *Senator Gets a Taste of No-Fly List Problems*, United Press Int'l, Aug. 20, 2004.

In 2005, Congress ordered the Government Accountability Office to investigate TSA's airline passenger screening programs. GAO found significant problems with handling of personal information and violations of privacy laws.[83] In September, GAO reviewed the watch list system and found "about half of the tens of thousands of potential matches sent to the center between December 2003 and January 2006 for further research turned out to be misidentifications."[84] According to the GAO, these misidentifications are a significant problem, and they:

> highlight the importance of having a process -- often referred to as redress -- for affected persons to express their concerns, seek correction of any inaccurate data, and request other actions to reduce or eliminate future inconveniences. Similarly, such a process would apply to other persons affected by the maintenance of watch list data, including persons whose names are actually on the watch list but should not be ("mistakenly listed persons") as well as persons who are properly listed.[85]

Also, according to the director of TSA's redress office, "some customers (air passengers) call and complain about having problems even though they have taken the necessary steps to be placed on the cleared list."[86] Multiple government assessments state that the watch lists remain filled with errors. The Justice Department Inspector General has said this indicates "a deficiency in the integrity of watchlist information."[87] These watch lists are used to screen "approximately 270 million individuals . . . each month."[88] Accuracy and reliability problems need to be resolved before they are used in yet another passenger profiling system to restrict the movement of U.S. citizens.

---

[83] Gov't Accountability Office, *Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public*, GAO-05-864R (July 22, 2005), *available at* http://www.gao.gov/new.items/d05864r.pdf.
[84] Gov't Accountability Office, *Terrorist Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public,* GAO-06-1031 (Sept. 2006), *available at* http://www.gao.gov/new.items/d061031.pdf.
[85] *Id*. at 2.
[86] *Id*. at 34.
[87] Justice Dept. Report on Watch Lists at xxii, *supra* note 66.
[88] *Id*. at v.

VII. SECURE FLIGHT'S REDRESS PROCEDURES ARE INADEQUATE AND FLAWED

DHS proposes in its Federal Register notices to exempt Secure Flight from the judicially enforceable rights of access and correction under the Privacy Act. In its place, DHS proposes poor substitutes. The individual may petition for access to his PNR data in Secure Flight through a "Privacy Act Access Request" sent to TSA FOIA Office or through the Traveler Redress Inquiry Program ("TRIP").[89]

It is especially important for individuals to have judicially enforceable rights of access and correction, because government reviews have found that there is "a high rate of error in watchlist records" and the Terrorist Screening Center's redress procedure is inadequate.[90] In the Justice Department Inspector General's review of the watch lists, the Center's redress procedures were criticized. The Inspector General found that "it took the TSC, on average, 67 days to close its review of a redress inquiry."[91] Also, the Inspector General said:

> 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.[92]

As we have detailed, inaccurate and untimely data on the watch lists have caused significant problems for innocent individuals. In Secure Flight, DHS offers inadequate alternatives to the Privacy Act's rights of judicially enforceable access and correction.

---

[89] Secure Flight Revised Privacy Impact Assessment at 23-24, *supra* note 1.
[90] Justice Dept. Report on Watch Lists at xix, *supra* note 66.
[91] *Id.*
[92] *Id.* at xx.

In February comments to the Department of Homeland Security, EPIC detailed the many privacy and security problems in TRIP, and urged DHS to fully apply Privacy Act requirements of notice, access, correction, and judicially enforceable redress to TRIP and the underlying system of watch lists.[93] Full application of the Privacy Act requirements to government record systems is the only way to ensure that data is accurate and complete, which is especially important in the context of watch lists and Secure Flight, where mistakes and misidentifications are costly.

TRIP is described as "a central gateway to address watch list misidentification issues, situations where individuals believe they have faced screening problems at immigration points of entry, or have been unfairly or incorrectly delayed, denied boarding or identified for additional screening at our nation's transportation hubs."[94] EPIC explained in February that, because TRIP provides a central system for submitting, directing and tracking but not resolving complaints, it fails to resolve the significant problems in current traveler redress procedures.[95]

It is unknown how a person would know that there is incorrect information in Secure Flight when the system cannot be accessed under the Privacy Act for inspection. In fact, the only indication a traveler may have that she is on the watch list is if she is subjected to extra scrutiny, refused permission to board a plane, or detained or arrested at the airport. This secrecy conflicts with the purpose of the Privacy Act, which was intended to provide an enforceable right of access to personal information maintained by government agencies. Neither the restrictive opportunity to petition the TSA Freedom of

[93] *See* EPIC Comments on TRIP, *supra* note 5.
[94] Press Release, Dep't of Homeland Sec., DHS to Launch Traveler Redress Inquiry Program, Jan. 17, 2007, *available at* http://www.dhs.gov/xnews/releases/pr_1169062569230.shtm.
[95] EPIC Comments on TRIP at 4-5, *supra* note 5.

Information Office nor TRIP is an adequate replacement for the complete judicially enforceable rights of access and correction enshrined in the Privacy Act.

VIII. CONCLUSION

In February 2006, TSA suspended Secure Flight for a comprehensive review following several critical reports. Though TSA has made substantial changes to Secure Flight, for the reasons detailed above, EPIC urges the agency to continue to ground the program until these problems are solved. If the program goes forward, the Department of Homeland Security must revise its Privacy Act notice for Secure Flight to 1) provide individuals judicially enforceable rights of access and correction and 2) limit the collection and distribution of information to only those necessary for the screening process. The recent changes to Secure Flight are not enough to ensure the protection of the privacy and civil liberty rights of citizens.

Respectfully submitted,

_____

Marc Rotenberg
Executive Director

_____

Melissa Ngo
Senior Counsel

ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, DC 20009
(202) 483-1140

Filed: September 24, 2007