CENTER FOR DEMOCRACY & TECHNOLOGY
Working for Civil Liberties on the Internet

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

September 30, 2003

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Docket No. DHS/TSA-2003-01

COMMENTS OF THE CENTER FOR DEMOCRACY AND TECHNOLOGY
on Notice of Status of System of Records, Interim Final Notice,
68 Fed. Reg. 45265-01 (Aug. 1, 2003), Docket No. DHS/TSA-2003-01

The Center for Democracy and Technology (CDT) takes this opportunity to express its continuing – and in some ways heightened – concerns about the Transportation Security Administration's proposed Computer Assisted Passenger Prescreening System ("CAPPS II") as detailed in the Interim Final Privacy Act Notice dated August 1, 2003 ("Interim Notice" or "Notice").[1] We are distressed that the mission creep reflected in the latest proposal threatens both of the twin goals stated for the CAPPS II system: "serving our national security without sacrificing individual privacy."[2] The focus on those goals was lost when CAPPS II was expanded to serve general law enforcement interests not related to airline security, and privacy assurances offered over the course of the spring were diluted or left without sufficient detail. Herein, we respectfully offer our recommendations for getting CAPPS II back on target.

As an initial matter, CDT commends TSA for issuing an interim Privacy Notice that contains many improvements over the initial Privacy Notice issued on January 15, 2003.[3] In several respects, TSA has followed through on its promise of engaging in "an historic,

---

[1] Notice of Status of System of Records, Interim Final Notice, Docket No. DHS/TSA-2003-01, 68 Fed. Reg. 45265-01 (Aug. 1, 2003).

[2] Briefing Room, *TSA Selects Lockheed Martin Management and Systems to Build TSA Passenger Pre-Screening System* (rel'd Feb. 28, 2003) (available at http://www.tsa.gov/public/display?theme=44&content=248). *See also Can the Use of Factual Data Analysis Strengthen National Security? – Part One: Hearings Before the Subcomm. on Tech., Info. Policy, Intergovernmental Relations, and the Census of the House Comm. on Gov't Reform*, 108th Cong. at 1-2 (May 6, 2003) (statement of Admiral James M. Loy) ("Loy H.R. Stat."); James M. Loy, *Privacy Will Be Protected*, USA TODAY, Mar. 12, 2003, at 12A ("Security and privacy are the guiding principles behind [CAPPS II]").

[3] *See* Privacy Act of 1974: System of Records, 68 Fed. Reg. 2101 (Dep't of Trans. 2003) ("First Privacy Act Notice" or "First Notice").

responsible dialogue with the traveling public" and privacy advocates,[4] and has provided significant details in the new notice about the proposed operation and use of CAPPS II. It is readily apparent that TSA has made genuine efforts to confront concerns expressed by previous commenters, including CDT.

Furthermore, CDT states at the outset that it would support establishment of a narrowly focused and privacy-sensitive passenger screening system. We have no doubt that terrorists pose an ongoing, extremely serious threat to civilian aviation. Passenger screening is a necessary component of an airline security program. The CAPPS I system is broken and needs to be replaced; it currently serves neither security nor civil liberties very well. However, it is precisely because the threat is so acute that we oppose the dilution of the CAPPS II mission and urge attention to the privacy and due process procedures that will not only protect individual rights but also make CAPPS II more effective.

I. THE PROPOSED SYSTEM EXCEEDS TSA'S STATUTORY MISSION, DILUTES THE EFFECTIVENESS OF PASSENGER SCREENING, AND RISKS MORE PRIVACY AND DUE PROCESS ERRORS.

CDT is particularly concerned about the expansion of the scope of CAPPS II in the Interim Notice. According to the Interim Notice, CAPPS II would be used not only to identify individuals (including U.S. citizens) with ties to international terrorist organizations but also: (1) individuals with ties to domestic terrorist organizations, in the absence of any indication that domestic terrorists pose a threat to civil aviation; (2) individuals with outstanding federal or state arrest warrants for crimes of violence; and (3) potentially, visa and immigration violators. Each of these expansions goes beyond the scope of TSA's statutory authority, dilutes the focus of the system, and creates significant risk of privacy and due process violations.

TSA has invoked three statutory sections as authority for the CAPPS II system: 49 U.S.C. §§ 114, 44901, and 44903. But under those sections, the scope of TSA's authority is specifically and unambiguously linked to transportation security. Under Section 114, TSA's mission is expressly limited to providing "for security in all modes of transportation." 49 U.S.C. § 114(d); *see also id.* § 114(f) (enumerating 15 "duties and powers" all expressly directed only to the provision of security in transportation).[5] Specifically with regard to the "management of security information," TSA is authorized to:

> (1) enter into memoranda of understanding with Federal agencies or other entities to share or otherwise cross-check as necessary data on individuals identified on Federal agency databases *who may pose a risk to transportation or national security*;

---

[4] *See, e.g.*, Briefing Room, *Joint Statement on CAPPS II by Nuala O'Connor Kelly and Admiral James M. Loy* (rel'd Aug. 25, 2003) (available at <http://www.tsa.gov/public/display?theme=44&content=667>) ("Aug. 25 Briefing").

[5] The subsequently enacted Homeland Security Act of 2002 does not expand upon this authority. *See* Pub. L. No. 107-296, § 423(c)(1) ("Nothing in this Act may be construed to vest in the Secretary [of Homeland Security] or any other official in the Department any authority over transportation security that is not vested in the Under Secretary of Transportation for Security, or in the Secretary of Transportation under chapter 449 of title 49, United States Code, on the day before the date of enactment of this Act.").

(2) establish procedures for notifying the Administrator of the Federal Aviation Administration, appropriate State and local law enforcement officials, and airport or airline security officers of the identity of individuals *known to pose, or suspected of posing, a risk of air piracy or terrorism or a threat to airline or passenger safety*;
(3) in consultation with other appropriate Federal agencies and air carriers, establish policies and procedures requiring air carriers—
  (A) to use information from government agencies to identify individuals on passenger lists who *may be a threat to civil aviation or national security*; and
  (B) if such an individual is identified, notify appropriate law enforcement agencies, prevent the individual from boarding an aircraft, or take other appropriate action with respect to that individual; and
(4) consider requiring passenger air carriers to share passenger lists with appropriate Federal agencies for the purpose of identifying individuals *who may pose a threat to aviation safety or national security*.

49 U.S.C. § 114(h) (emphasis added). TSA's statutory authorization with regard to an information-based security system like CAPPS II is therefore directly linked to aviation security and national security by Section 114. Likewise, Sections 44901 and 44903 provide TSA with no authority beyond aviation security and national security.

Consistent with this congressional mandate, Admiral Loy stated this past spring that the purpose of CAPPS II was "to identify foreign terrorists and those with links to foreign terrorists that pose a threat to civil aviation security" by "identify[ing] passengers for enhanced screening before those passengers are permitted to board a commercial aircraft."[6] Indeed, in an effort to quell mounting public concerns over the scope of CAPPS II, Admiral Loy assured the public that the "bottom line" goal of CAPPS II would be "keeping foreign terrorists off airplanes."[7] Even the Interim Notice states the purpose of CAPPS II is to "ensure passenger and aviation security."[8] Unfortunately, the Interim Notice expands beyond aviation security the purposes for which CAPPS II will use and disclose personal passenger information. As written, the Notice goes far beyond TSA's congressionally authorized mission, which is limited to providing for security in transportation.

A. OUTSTANDING WARRANTS

The first example of this mission creep is TSA's plan to disclose personal passenger information to federal, state, local, international or foreign authorities where DHS "becomes aware of an outstanding state or federal arrest warrant for a crime of violence."[9] This proposed

[6] Loy H.R. Stat. at 1.

[7] *See* Loy, USA TODAY.

[8] *Interim Notice*, 68 F.R. at 45265, 45267.

[9] *Id.* at 45268, 45268, Routine Use 1. This Routine Use is somewhat ambiguous; it does not make clear whether information will be shared *only* where "DHS becomes aware of an outstanding state or federal arrest warrant for a crime of violence," or whether that is simply one of the circumstances in which information might be shared. In future publications, TSA should clarify that issue.

use is unauthorized under the ATSA, violates the Privacy Act, and will divert TSA's resources away from aviation security.

As stated above, TSA's sole authorized mission is to provide for security in modes of transportation. Proposed Routine Use 1, however, does not even purport to be concerned with transportation security. Instead, it expands CAPPS II into an all-purpose law enforcement tool designed not to provide security in transportation or to keep terrorists off planes, but to assist general law enforcement authorities in arresting suspected criminals. At any given time, there are thousands of outstanding arrest warrants nationwide. Proposed Routine Use 1 will divert TSA's resources away from its core mission of airline security. Expanding the use of CAPPS II for the purpose of arresting persons with outstanding warrants, no matter how compelling it may seem, will reduce the effectiveness of CAPPS II for ensuring aviation security, and is beyond the scope of TSA's congressionally mandated authority.[10]

Proposed Use 1 also is unlawful under the Privacy Act of 1974, which prohibits TSA from disclosing passenger information to other agencies except under specifically enumerated circumstances. *See* 5 U.S.C. § 552a. The only relevant exceptions would be § 552a(b)(7), for authorized law enforcement purposes, or § 552a(b)(3), for "routine uses." Neither of these applies here. Section (b)(7) is inapplicable because it allows disclosure only upon the "written request" of the agency receiving the personal information, *id*. § 552a(b)(7), while under the Interim Notice it would be TSA's decision what to disclose. Federal courts have routinely enforced this requirement strictly.[11] Here, Routine Use 1 purports to authorize disclosure of passenger information upon no request at all – let alone a "written request" – from the relevant law enforcement authority.

Section (b)(3) of the Privacy Act, exempting disclosures for "routine uses," is equally inapplicable. TSA cannot shoehorn its intended unlawful disclosure of passenger information into this exception merely by deeming it a "routine use." To meet this exception, the "routine use" must be "compatible with the purpose for which it was collected." 5 U.S.C. § 552a(a)(7). As we have shown, TSA has no statutory authority to collect passenger information for ordinary law enforcement activities, and TSA has not indicated that it will use warrants to identify only those individuals who pose a threat to aviation security. At most, TSA may have authority to collect information on outstanding arrest warrants in calculating a passenger's risk assessment score for purposes of determining whether extra pre-boarding screening is appropriate. But *nothing* in TSA's mandate authorizes it to collect such information *for the purpose* of executing

---

[10] To the degree that ATSA grants TSA any of its own law enforcement powers, it does so only "to fulfill the responsibilities of this section," 49 U.S.C. § 114(q), which as discussed above are limited to aviation security and national security.

[11] *See DOE v. DiGenova*, 779 F.2d 74, 85 (D.C. Cir. 1985) ("[A]lthough the [Privacy] Act permits disclosure to another governmental agency for civil or criminal law enforcement activity, it conditions the disclosure on the written request of the head of the agency, thereby assuring some high level evaluation of the need for the information."); *Doe v. Naval Air Station*, 768 F.2d 1229, 1232-33 (11th Cir. 1985) (court found Privacy Act violation where request for information was not in writing but by telephone); *Britt v. Naval Investigative Service*, 886 F.2d 544, 548 (3rd Cir. 1989) ("It is unlikely that the NIS can, through its publication of Blanket Routine Uses, avoid the [written request] restrictions of section 552a(b)(7), which were not met in this case."); *Word v. United States*, 604 F.2d 1127, 1129 (8th Cir. 1979) (no written request).

arrest warrants. Accordingly, because TSA possesses no statutory authority to collect such information, the disclosure of such information cannot be justified as compatible with a *lawful* purpose for which it was collected.

For these reasons, CDT strongly recommends that the Notice's proposed routine use regarding outstanding warrants unrelated to airline security be eliminated.

B. "DOMESTIC TERRORISTS"

A second example of mission creep is the Notice's stated purpose for CAPPS II of identifying "domestic terrorists." This past spring, Admiral Loy assured Congress and the public that CAPPS II would be used only to identify *foreign* terrorists and prevent them from boarding airplanes, because that is the source of the threat to aviation security.[12] Now, with no stated justification, TSA has broadened CAPPS II's purposes to identifying *domestic* terrorists and those associated with domestic terrorist organizations.

We would not be opposed to including certain domestic terrorists if there were evidence that they posed a threat to aviation safety. However, the Interim Notice cites no such threat. In the absence of intelligence suggesting such a threat, the expansion of CAPPS II into the realm of domestic terrorism places TSA in the role of having to evaluate the political activities of Americans. The FBI's definition of who is a domestic terrorist has often been quite broad. In the absence of a specific threat, how does TSA decide who is a domestic terrorist who should be flagged by CAPPS II? Does the term "domestic terrorist" include an anti-abortion activist who breaks the law by blocking access to abortion clinics or who may be organizationally or ideologically related to those who have killed doctors or committed arson at clinics? Does it include members of Earth First or other radical environmental groups that have engaged in illegal acts and have been investigated by the FBI as domestic terrorist organizations? The Interim Notice leaves the term undefined, and does not state how TSA will determine whether an individual is a domestic terrorist.

This concern is amplified by the fact that the only statutory definition of "domestic terrorism" in the U.S. Code is overbroad. As defined in the USA PATRIOT Act, the term "domestic terrorism" casts a wide net, and potentially covers political protesters engaging in civil disobedience.[13] This broad definition blurs the line between "terrorism" and aggressive or unseemly political activity protected by the First Amendment. Singling out passengers based on "links" with groups that have engaged in such activities would trample First Amendment liberties and might even subject TSA to constitutional challenges.

Accordingly, CDT recommends that the Notice's proposed purpose of identifying passengers with "identifiable links" to purely "domestic terrorist organizations" be narrowed substantially, so that it is limited to situations, if and when they arise, when information indicates that specific domestic terrorists pose a threat to civil aviation. Until then, TSA should refrain

---

[12] *See* Loy, USA TODAY; *see also* Loy H.R. Stat. at 1-5 (repeatedly assuring Congress that the purpose of CAPPS II would be to identify "foreign terrorists").

[13] *See* Pub. L. No. 107-56, § 802, codified at 18 U.S.C. § 2331(5).

from screening passengers based on other agencies' characterization of who is and is not a domestic terrorist.

C. IMMIGRATION USES

The Interim Notice suggests that TSA might associate CAPPS II with the U.S. Visitor and Immigrant Status Indicator Technology ("US-VISIT") program. The Notice contains only one sentence on this topic, noting that "[i]t is further anticipated that CAPPS II will be linked to the [US-VISIT] program at such time as both programs become fully operational, in order that the processes at both border and airport points of entry and exit are consistent."[14] This vague sentence appears to be a "placeholder." As such, it is inadequate for purposes of this notice process. If at some future date, TSA believes that it should link CAPPS to the US-VISIT system, then at that time TSA should specify how this proposed link would work, what information in the US-VISIT database TSA would use, and how accessing such information would advance the mission of airline security.

In the meantime, CDT urges TSA not to shoulder any immigration role not directly relevant to aviation security. With each additional task that TSA takes on, its resources for its core mission will be diluted.

II. EFFECTIVENESS: TSA MUST ASSESS CAPPS II'S EFFECTIVENESS IN PROTECTING AVIATION SECURITY BEFORE IT ADOPTS THE SCREENING SYSTEM.

Under the Privacy Act, TSA should gather personal data on air passengers only if the collection of such information furthers a legitimate government interest – here, aviation and passenger security. The government interest in protecting transportation security justifies the adoption of CAPPS II only if the screening system is effective in accomplishing that goal. Thus, as TSA has recognized, the effectiveness of CAPPS II is "among the underpinnings of evaluating such a system's impact on an individual's privacy."[15]

The TSA's commitment to test the effectiveness of the proposed system is an important, and commendable, first step. However, the Interim Notice provides only a limited description of the testing process, and does not spell out the methodology and criteria that TSA will employ during the 180-day testing period. For example, how will TSA measure the effectiveness of CAPPS II – is there a threshold of reliability and/or accuracy that must be met prior to the system's adoption? What factors will be considered during the testing process? Will TSA evaluate the different pieces of CAPPS II – the identity verification, the watch list checking, and the dynamic algorithm analysis – separately to determine whether certain aspects of the system should be implemented while others should not? What effect does identity theft have on the effectiveness of the system?

---

[14] *Interim Notice*, 68 F.R. at 45266.

[15] *Id.* at 45267.

None of these questions is easy, but we urge TSA to clarify these issues by publicly announcing in the Final Notice the standards that it will apply, so that Congress, the airline industry, the traveling public, and privacy groups may more completely assess the effectiveness of the CAPPS II system and its component parts. In addition, this will aid the GAO in its analysis of "the efficacy and accuracy of all search tools in CAPPS II" to ensure "that CAPPS II can make an accurate predictive assessment of those passengers who may constitute a threat to aviation," as required by the Department of Homeland Security Appropriations legislation recently passed by the House and Senate.[16] We will work with GAO and Congress to further define measures of effectiveness and we urge TSA to be publicly explicit about its evolving evaluation standards.

III. PRIVACY CONCERNS REMAIN NOT FULLY ADDRESSED.

The remainder of these comments are organized around critical areas in which CDT believes that the Interim Notice has fallen short of principles recognized as critical to the proper protection of privacy and due process with respect to the collection and use of personal information. These "Fair Information Principles" appear in the Privacy Act and have been agreed upon by the federal government, privacy experts and industry groups. They are: (i) notice; (ii) collection limitation; (iii) use and disclosure limitations; (iv) data retention limitations; (v) data quality protection; (vi) access and an opportunity to correct errors; (vii) redress and other enforcement procedures; and (viii) system security safeguards. Each of these fundamental principles as they pertain to CAPPS II is discussed in turn below.

A. NOTICE: TSA SHOULD PROVIDE PASSENGERS WITH NOTICE OF ITS COLLECTION OF THEIR PERSONAL DATA.

CDT commends the TSA for its commitment to inform passengers what personal information it is collecting and for what purpose.[17] Alerting passengers of the purpose for which their information will be gathered – for security purposes as opposed to, say, airline marketing – should give travelers an incentive to provide accurate information when booking air travel.

However, TSA should also provide passengers with more detailed information about the other sources of information it will rely on to evaluate them. What commercial and government databases does TSA intend to check? What information will be collected or access from those records? If a passenger knows that a certain name and address database will be checked, the passenger can attempt to prevent or rectify errors in those databases if, for example, the customer has recently moved. In this regard, providing travelers with notice also increases the reliability and accuracy of the sources that TSA employs.

---

[16] H.R. 2555, Section 519(a)(3) (passed by House and Senate Sept. 24, 2003).

[17] *See Interim Notice*, 68 F.R. at 45266 ("Consistent with fair information principles, The Department of Homeland Security will work towards adequate notice to the passenger when that passenger provides information that will be used for security purposes.").

B. DATA COLLECTION LIMITATION: TSA SHOULD COLLECT ONLY THAT INFORMATION RELEVANT TO ITS AVIATION SECURITY GOALS.

The TSA's collection of passengers' personal information as part of the CAPPS II screening system should be limited to that data necessary to accomplish the purpose at hand: here, screening airline passengers to promote aviation security. Although the First Privacy Act Notice appeared to contemplate the use of sweeping categories of information about travelers, TSA in the months following that First Notice assured the public that its collection of passenger information would be more limited. Specifically, TSA Administrator Admiral James Loy identified the passenger's name, address, phone number and date of birth (collectively "name plus three") as the sole categories of information that would be collected from travelers at the time they purchase tickets for the purpose of CAPPS II.[18] TSA's intent to use passengers' name plus three was a reasonable means of balancing the goals of aviation security and the privacy rights of passengers. Limiting the collection of data to those categories would be an appropriate means of "minimiz[ing] the amount of information on travelers that ever comes into the system, [and] using only the information that is necessary to conduct an identity authentication and risk assessment."[19]

But the Interim Notice proposes that the scope of passenger information accessed under CAPPS II be expanded to include the entire passenger name record ("PNR").[20] The Interim Notice lists the "name plus three" and the passenger's travel itinerary as the *minimum* PNR data that will be used, leaving open the possibility that other unspecified data would be collected. The PNR contains numerous additional pieces of information that have no apparent significance to the aviation security goals that CAPPS II is designed to promote, and that TSA should not gather from the airlines and travel agents who generate PNRs. For example, a PNR may contain a passenger's meal preferences (which can reveal religious affiliation), credit card number, need for a wheelchair or special assistance, seating preference, and frequent flier membership. TSA cannot access elements of the PNR beyond name plus the three that have been specified without first explaining the purpose for which those categories of data will be used, and how their collection is necessary and relevant to the aviation security goals of the proposed passenger screening system.

C. DATA USE AND DISCLOSURE LIMITATION: TSA SHOULD USE AND DISCLOSE DATA ONLY FOR THE PURPOSE OF AVIATION SECURITY, AND SHOULD FURTHER CLARIFY HOW IT WILL USE PASSENGER INFORMATION.

In addition to the "mission creep" problems identified above, the Interim Notice also contains a number of vague and undefined uses and disclosures that TSA should clarify before

---

[18] *See* Loy, USA TODAY; Loy H.R. Stat. at 2.

[19] Loy H.R. Stat. at 4.

[20] *See Interim Notice*, 68 F.R. at 45266.

putting CAPPS II into practice. First, CDT is seriously concerned about what governmental information TSA will use. The Interim Notice states that CAPPS II will contain "some information" from governmental databases, and TSA has indicated in the past that this unidentified government information – what CDT and others have referred to as the "Black Box" – will include immigration data and intelligence information that will be analyzed using a dynamic intelligence-based algorithm to determine whether any particular passenger constitutes a risk to aviation security. It is crucial that TSA provide more information about this process and the government data it intends to rely on. Consistent with national security interests, TSA should clarify what governmental information and databases it intends to access, and should indicate why it believes that such information and databases will advance the mission of airline security. Doing so will allow appropriate oversight by Congress and the public, engender more trust in the system, and allow passengers to understand the full ramifications if they discover errors in government information about them.

Second, TSA should clarify exactly what passenger-provided information will be disclosed to commercial vendors. The Notice identifies "selected" information, but offers no further guidance. As explained above, the passenger PNRs that TSA has stated it will collect often provide much more information than name, address, phone number and date of birth. They may include credit card payment information, indication of disabilities or handicaps, or evidence of religious affiliation from meal preferences. If TSA intends to pass such information on to commercial vendors, it should make that intention clear and explain why it is necessary.

Third, TSA also should specify what other commercial information its vendors will rely on for the passenger identity verification process. CDT certainly applauds TSA for making clear that neither it nor its commercial vendors will not use creditworthiness and health information, but the Notice is silent on what information they *will* rely on.

Fourth, TSA should clarify the consequences to passengers, including under what circumstances a passenger can be designated a "yellow" or a "red," and what happens to a passenger in both scenarios. Can a passenger become a "red" if they are *not* matched to a terrorist watch list entry? Are yellows subjected to different levels of scrutiny depending on their score, such as having their bags physically searched for "low" yellows and being pulled aside and questioned for "high" yellows? Passengers should understand the potential consequences of the system – the ultimate use of their information – before it is implemented.

Fifth, TSA must limit any consequences to passengers during the testing phase. The Notice currently states that, during the 180-day test period, if an "indication of terrorist or potential terrorist activity is revealed, . . . appropriate action will be taken."[21] But recent legislative action, likely to become law soon, indicates that during testing "no information gathered from passengers, foreign or domestic air carriers, or reservation systems may be used to screen aviation passengers, or delay or deny boarding to such passengers."[22] CDT believes this legislation appropriately limits any actions against passengers before CAPPS II is proven reliable.

---

[21] *Id*. at 45267.

[22] H.R. 2555, § 519(b) (passed by House and Senate Sept. 24, 2003).

D. DATA RETENTION: TSA SHOULD NOT RETAIN DATA FOR ANY LONGER THAN NECESSARY TO ENSURE AVIATION SECURITY.

CDT commends TSA for limiting its retention of data in the Interim Notice, which states that the government would retain data about a U.S. citizen or permanent resident alien only for a "certain number of days" after the person's travel has been completed – not the 50 years indicated by the First Notice. We note, however, that until the publication of the Interim Notice TSA had been saying that passenger data would be purged immediately after the safe completion of a flight. TSA should explain why it needs passenger data for several days after a flight has already (safely) landed, and it should also explain why it needs to retain the data between the two legs of a passenger's roundtrip, particularly if several weeks or months pass between those legs. Furthermore, the indeterminacy of the retention of data on persons who are neither U.S. citizens nor lawful permanent residents is a troubling ambiguity, and one that TSA should clarify and justify. As it is, it appears that CAPPS II is to be used to collect intelligence on the travels of non-citizens for reasons unrelated to airline security.

As to the retention of CAPPS II-related data by commercial vendors conducting passenger identify verifications, CDT is pleased that TSA intends to ensure that private companies will not be permitted to retain the data provided by TSA or use it for any other purposes. TSA should put similar limitations on the use and retention of data collected solely for security purposes by the ticketing agents and airlines that generate PNRs.

E. DATA QUALITY: TSA SHOULD USE THE TESTING PROCESS TO ESTABLISH STANDARDS FOR MEASURING AND ENHANCING THE QUALITY OF THE DATA COLLECTED BY CAPPS II.

As TSA has recognized, gauging the quality and accuracy of the data used in the CAPPS II screening system is a crucial component of the testing process. Unless TSA's data sources are complete, current, and accurate, innocent passengers may be labeled as risks, and/or dangerous passengers will appear harmless. Accordingly, TSA must develop standards for measuring the accuracy and completeness of the databases from which it obtains or accesses information, should not rely on any data sources that do not meet those standards, and should develop safeguards to protect against, and compensate for, any remaining shortcomings in the quality of that data.

TSA has wisely recognized that there may be inaccuracies in data collected from commercial sources, and that the testing period must be used to develop methods of addressing those data quality shortcomings.[23] TSA must develop standards for assessing and verifying the accuracy of each source of commercial data on which it relies. When making that assessment, TSA should ask several questions, including: (1) How often is each data source updated? (2) How complete is the information the sources contain? (3) How accurate is that information? (4) How does the accuracy, completeness, and currency of the data sources affect the TSA's use and disclosure of the information drawn from the source? (5) How do the data sources protect against and/or mitigate the possibility of identity theft?

[23] *Interim Notice*, 68 F.R. at 45266-67.

It is important that TSA also evaluate the reliability and accuracy of the government databases from which CAPPS II draws information. The Interim Notice anticipates that CAPPS II will access government data sources, such as immigration databases, when conducting its risk assessment.[24] But those databases may also contain inaccuracies that would diminish or eliminate their usefulness in screening out passengers that pose a threat to aviation security. For example, it is well-documented that immigration databases often contain outdated and incorrect information.[25] If CAPPS II will rely on data from those databases, TSA must assess the reliability of the databases, refuse to rely on those that do not meet certain requirements, and develop mechanisms to correct for any remaining inaccuracies.

TSA should also adopt standards to assess the reliability of the PNRs that it gathers. Errors may be made when a passenger's information is input; *e.g.*, a name might be misspelled or a number in a date of birth may be transposed. These innocent mistakes could impair TSA's ability to authenticate passengers' identity. TSA should therefore use the testing period to develop methods to identify and in the future avoid these potential inaccuracies.

The adoption of data quality standards and safeguards is even more critical where CAPPS II relies on information contained in terrorist watch lists. Although watch lists can be powerful tools, they are only effective if subjected to stringent quality standards and maintained and updated in accordance with those standards. Numerous reports have confirmed that current watch lists are deeply flawed.[26] As an FBI official explained to a congressional subcommittee with respect to FBI watch lists, "many times there is insufficient data that [could be used to] accurately make a determination that it was in fact [the person on the list] because there's no date of birth, biographical data or other relational type of data."[27]

CDT understands that TSA does not create these watch lists, but rather is a consumer of them. Nonetheless, CDT urges TSA to be a smart consumer. TSA will have direct contact with the American public and – as has already occurred – will receive the brunt of the criticism if the

---

[24] *Id.* at 45266. The Notice also provides that the records in the system will include: "watch lists and government databases containing information on known terrorists and terrorist associates, or other information pertinent to the detection of terrorists and their associates, or pertinent to the detection of outstanding state or federal warrants for crimes of violence." *Id.* at 45268.

[25] *See generally, e.g.,* GAO, *Homeland Security: Justice Department's Project to Interview Aliens After September 11, 2001*, GAO-03-459 (April 2003), *available at* www.gao.gov/news.items/d03459.pdf; GAO, *Homeland Security: INS Cannot Locate Many Aliens Because It Lacks Reliable Address Information*, GAO-03-188 (Nov. 2002), *available at* www.gao.gov/highlights/d03188high.pdf.

[26] *See* documents obtained by the Electronic Privacy Information Center through FOIA, *available at* http://www.epic.org/privacy/airtravel/foia/watchlist foia analysis.html; GAO, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*, GAO-03-322 (April 2003), *available at* www.gao.gov/new.items/d03322.pdf; Ann Davis, *Boarding Impasse: Why a 'No Fly List' Aimed At Terrorists Delays Others*, Wall St. J. (Apr. 22, 2003), at A1; Farhad Manjoo, *"Please Step To the Side Sir*," Salon (Apr. 10, 2003), *available at* http://archive.salon.com/tech/feature/2003/04/10/capps/index.html.

[27] *See Can the Use of Factual Data Analysis Strengthen National Security? – Part One: Hearings Before the Subcomm. on Tech., Info. Policy, Intergovernmental Relations, and the Census of the House Comm. on Gov't Reform*, 108th Cong. at 9 (May 6, 2003) (statement by William L. Hooten).

watch lists result in any significant number of false positives. Accordingly, TSA should adopt its own internal standards as to what constitutes an "adequate" watch list entry that it will use as part of CAPPS II. Such standards might include the following requirements:

- Each watch list entry used by TSA shall contain both the first and last name of an individual.
- Each watch list entry used by TSA must include at least one piece of identifying information beyond the individual's name.
- Each watch list entry used by TSA shall contain an indication that it was reviewed for accuracy and necessity within the past year.

F. ACCESS AND OPPORTUNITY TO CORRECT: TSA SHOULD PROVIDE PASSENGERS SOME DEGREE OF ACCESS TO THE RECORDS THAT CONTAIN THEIR PERSONAL DATA AND AN OPPORTUNITY TO CORRECT INACCURACIES IN THAT DATA.

CDT appreciates TSA's "commit[ment] to providing access to the information that is contained in the CAPPS II system to the greatest extent feasible consistent with national security concerns."[28] Such a commitment is consistent with the Fair Information Principles of access and the right to correct, which indicate that passengers be given some degree of access to the information used to evaluate their status as potential security risks, and that they have an opportunity to submit corrections where necessary. Principles of fairness and due process also suggest that where passengers face adverse consequences based on information tapped by the CAPPS II system, they should have the right to know the basis for the determination and the ability to challenge the adverse action. Giving passengers access to, and the ability to correct, information on which the government relies also promotes the efficacy of the screening system. The Interim Notice provides only a short overview of this issue, however, and several questions remain unanswered. Prior to implementing CAPPS II, TSA should explain further how the commitment to passenger access will be effectuated.

CDT is pleased that TSA intends to provide passengers the ability to access their PNR data.[29] But the TSA's decision to exempt CAPPS II from the provisions of the Privacy Act that *require* that individuals have access to their records seems unwise. The Privacy Act confers important rights upon those individuals whose data is collected by the government, including an opportunity for judicial review of certain agency decisions regarding that data.[30] TSA could comply with those rules without sacrificing its concerns about national security. CDT urges TSA to reconsider this proposed exemption, and to adhere to the Privacy Act access standards.

TSA's proposal to limit individuals' access to the PNR data that is provided to TSA also seems ill-advised. TSA has stated that CAPPS II will use several additional sources of data to make its risk assessment, such as commercial databases and government records. The privacy

---

[28] *Interim Notice*, 68 F.R. at 45267-68.

[29] *See id.* at 45269.

[30] 5 U.S.C. § 552a(d)(3), (g)(1)(A).

and fairness principles that require passenger access to PNR apply equally to those other sources. If, for example, a commercial vendor gives a customer a low identity score, the passenger will likely be deemed a "yellow" and subjected to increased screening. But that low score may result from an error, the fact that the passenger has recently moved, or some other innocent cause. If passengers cannot access that information and correct it, they will be subjected to the same error on multiple occasions. This undermines the reliability of CAPPS II, and eliminates a potentially valuable means of enhancing the accuracy of the data on which the system relies. TSA should therefore include language in its contracts with commercial data vendors that anticipates and provides for passenger access to and correction of that data.

For similar reasons, TSA should permit passengers to access and correct the records that appear in government data sources that are not classified. CDT understands that in certain circumstances national security concerns will prevent the government from revealing intelligence information that adversely impacts a passenger. But where problems arise from an unclassified government source such as an immigration database, granting passengers access to the record, and the ability to correct errors therein, would not pose any problems that would warrant denying passengers that right. Indeed, under the Privacy Act, the government routinely must provide individuals with access to many systems of records.[31] However, passengers should not be without redress when the system uses classified information to deem them a security risk. In such circumstances, passengers should be able to enlist the Passenger Advocates to review and address any inaccuracies in the records. TSA should include these protections in its Memoranda of Understanding with other government agencies.

TSA's data retention policies, which CDT supports, do make it more difficult for passengers to obtain access to their information. As TSA has recognized, the fact that TSA only retains the PNR for a matter of days means that, as a practical matter, "in most cases, the response to a record access request will very likely be that no record of the passenger exists in the system."[32] While CDT agrees that TSA should only keep data for very short periods of time, that policy should not deprive passengers of a meaningful opportunity to access and correct errors in the data on which CAPPS II relies. Accordingly, TSA should adopt measures to protect passengers' right to access the information notwithstanding the data retention policies, such as allowing passengers to give TSA permission to retain their data for future flights so that it can be analyzed to determine why the passenger is consistently labeled a "yellow."

---

[31] *See, e.g.*, *id*. § 552a(d).

[32] *Interim Notice*, 68 F.R. at 45269.

G. PASSENGER REDRESS AND OTHER ENFORCEMENT PROCEDURES: TSA SHOULD ESTABLISH PROCEDURES THAT ALLOW PASSENGERS THAT BELIEVE THEY HAVE BEEN INCORRECTLY IDENTIFIED AS A SECURITY RISK TO OBTAIN REVIEW AND REDRESS, AND SHOULD IMPLEMENT OTHER CONTROLS TO ENSURE OVERSIGHT OF CAPPS II.

1. Passenger Redress

TSA has appropriately committed to develop a "robust review and appeals process" to protect passengers' ability to seek redress where incorrect information causes them to be subjected to heightened scrutiny at the airport.[33] As part of that process, TSA has indicated that it will create a Passenger Advocate, who will act on behalf of the passenger and investigate complaints.[34] TSA should elaborate upon the details of that process in the subsequent Privacy Act Notice, and should consider the following issues.

First, TSA must establish procedures to govern the Passenger Advocates' review of a passenger's complaint. If the traveler has been designated "yellow" based on commercial data, the Passenger Advocate should first review the complaining passenger's identity verification score and determine if that score contributed to the passenger's "yellow" status. (CDT is assuming that no one could become a "red" based solely on commercial data; TSA should confirm that in future publications.) If so, the Passenger Advocate should examine the data on which the score was based. As discussed above, the Passenger Advocate should provide the passenger with access to the commercial information relied upon so that the passenger can point out any inaccuracies or incomplete information. To facilitate this review process, TSA's contracts with commercial vendors should require them to investigate any information challenged by a passenger, using procedures based on the provisions of the Fair Credit Reporting Act that allow consumers to have access to their consumer reports and the right to correct them.[35]

TSA should also develop procedures for the Passenger Advocate to follow when a traveler has been designated a "yellow" or a "red" based on government data. First, the Advocate should be given authority to determine whether the increased scrutiny of that passenger resulted from a watch list match. If so, the Advocate should request that the agency that maintains the watch list investigate to determine whether the complaining passenger actually is the person on the watch list. If the match is a false positive, the Advocate should have access to a TSA mechanism that prevents the passenger from being "matched" in the future. If the match appears valid, the Advocate should nonetheless request that the agency maintaining the watch list verify that the passenger should be on that list.

TSA should also give the Passenger Advocate the authority to review any other intelligence and government data relied upon to produce a "red" or "yellow" designation. If, for

---

[33] *Id.* at 45267.

[34] *Id.* at 45269.

[35] *See* 15 U.S.C. §§ 1681g-1681i.

instance, the data is classified, TSA will be unable to permit the passenger to directly access the information sources. The Passenger Advocate's role is particularly important in such situations; the Advocate should either review the relevant information and correct for errors, if any, or direct the agency that maintains the information to perform the same task.

2. Other Controls and Oversight Mechanisms

Auditing must also be an important part of the CAPPS II system. CDT recommends that CAPPS II undergo an annual audit jointly conducted by the DHS Inspector General, the Privacy Officer, and the Civil Rights and Civil Liberties Officer. Of necessity, the auditors should have security clearances enabling them to access all relevant information, including classified data. The auditors could conduct spot checks of actual screenings and retain some passenger records for the duration of the audit process. To the extent the auditing report relies on classified information, portions of the report may need to remain classified, but CDT would urge that as much of any auditing report be made public as possible.

TSA's commitment to the retention limitation principles discussed above should not hinder auditors' ability to examine the system. Auditors can collect statistical information – such as a percentage of "yellows" and/or "reds" – without reviewing personally identifiable information about particular passengers. Random surveys would allow the audit to include passengers' perspective on their experiences with the system without linking the assessment to data retained in CAPPS II. Auditors should also consult with passengers who have filed complaints regarding their experiences with the screening and redress process.

CDT commends TSA for proposing a real-time auditing function that will monitor who accesses the system. That is an important protection against security breaches, and ensures that only the Passenger Advocate, auditors, and other authorized individuals have access to the system. When tracking and auditing its personnel's access to the CAPPS II system, however, TSA should avoid collecting personally identifiable information about passengers.

Other forms of independent oversight of CAPPS II are also essential to an effective privacy protection scheme. When TSA met with privacy advocates last spring, it indicated its intention to provide an annual public report to Congress. CDT believes that such an annual public report should include: (1) an explanation of the CAPPS II privacy policies; (2) a description of how those policies have been implemented; (3) a list of the types of passenger complaints that have been filed, with descriptions of how they have been resolved; and (4) changes that TSA is making to minimize any identified problems. Other oversight mechanisms that TSA should consider are independent evaluations of the program by outside auditors, periodic consultations with privacy advocates, the collection of statistical information, surveys of passengers to learn about their experiences with CAPPS II, and penalties for TSA employees who violate its privacy principles.

H. SYSTEM SECURITY: TSA SHOULD EXPLAIN ITS PLANS TO MAINTAIN THE SECURITY OF THE SCREENING SYSTEM.

CDT commends TSA for recognizing that safeguards are necessary to protect the security of the system from which records can be accessed.[36] But the Interim Notice does not provide sufficient detail to allow commenters to evaluate the system security measures that TSA intends to adopt. TSA has previously indicated that it will use technology such as firewalls, Virtual Private Network (VPN) technology, encryption and access rules to ensure system security and protect against abuse.[37] TSA has also stated that it will adopt a system with real-time auditing, limit access to the system to those with an appropriate need, develop internal mechanisms so that the system can monitor and identify who access the system, when it was accessed, and for how long.[38] These are good steps, but TSA should spell out in further detail the security measures for CAPPS II.

CONCLUSION

In sum, our comments are these:

- TSA's proposed uses of CAPPS II go far beyond aviation security, representing "mission creep" even before CAPPS II becomes operational.
- These additional uses of the system unlawfully extend TSA's activities beyond the Congressional grant of authority to TSA in the Aviation and Transportation Security Act.
- Other uses of the system set out in the Interim Notice would violate the Privacy Act.
- Many terms and proposed uses articulated in the Notice are so vague and undefined that they threaten the fundamental effectiveness of CAPPS II and jeopardize the public's confidence in TSA's ability to implement CAPPS II in a way that respects important privacy concerns.
- TSA's reliance on unspecified government databases of uncertain accuracy to evaluate whether passengers are risks to aviation security remains a leading cause for concern.

Each of these issues must be addressed and remedied before TSA can achieve its twin goals of implementing a lawful passenger screening program that is efficient and effective while simultaneously protecting the privacy rights of the nation's air travelers.

---

[36] *See Interim Notice*, 68 F.R. at 45269.

[37] *See, e.g.*, Loy H. R. Stat. at 3 ("Strict firewalls and access rules will protect a traveler's information from inappropriate use, sharing, or disclosure.").

[38] *Id.* at 4.

Respectfully submitted,

James X. Dempsey, Executive Director
Lara M. Flint, Staff Counsel
Center for Democracy and Technology
1634 I Street, NW, Suite 1100
Washington, DC 20006
(202) 637-9800
http://www.cdt.org

Michael B. DeSanctis
Robin M. Meriweather
JENNER & BLOCK, LLC
601 13th Street, NW, Suite 1200
Washington, DC 20005
(202) 639-6000