Statement of

David L. Sobel
General Counsel
Electronic Privacy Information Center

Before the

House Committee on Transportation and Infrastructure
Aviation Subcommittee

"The Status of the Computer-Assisted Passenger Prescreening System (CAPPS II)"

March 17, 2004

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to address the privacy and civil liberties implications of the enhanced Computer Assisted Passenger Prescreening System ("CAPPS II") now under development within the Transportation Security Administration ("TSA"). The subcommittee's inquiry is critically important and goes to one of the most significant controversies surrounding the government's response to the tragic events of September 11, 2001. While most of the post-9/11 debate over security and liberty understandably has focused on the USA PATRIOT Act, the serious problems inherent in CAPPS II will have a more direct and immediate impact on most Americans. The CAPPS II mission – to conduct background checks on tens of millions of citizens – is unprecedented in our history. While we all agree that there is a clear need for enhanced aviation security, there are many reasons to question whether CAPPS II is the right approach, both from a security perspective and in terms of its detrimental impact on our traditional liberties.

The U.S. Supreme Court has long recognized that citizens enjoy a constitutional right to travel. Thus, in *Saenz v. Roe*, the Court noted that the "'constitutional right to travel from one State to another' is firmly embedded in our jurisprudence."[1] For that reason, any governmental initiative, such as CAPPS II, that conditions the ability to travel upon the surrender of privacy

[1] 526 U.S. 489 (1999), quoting *United States v. Guest*, 383 U.S. 745 (1966).

and due process rights requires particular scrutiny. I hope that today's hearing marks the beginning of a serious inquiry into the costs and claimed benefits of CAPPS II, and that there can be an informed public debate on the proposal – a debate that has not yet occurred. Critical elements of that discussion, which I will address today, include transparency, due process and adherence to established privacy principles.

The problems that are likely to arise if and when CAPPS II becomes operational are not hypothetical. For more than two years, an untold number of innocent airline passengers have been wrongly flagged as a result of TSA's secretive "selectee" and "no-fly" lists. Documents obtained by EPIC under the Freedom of Information Act detail the Kafkaesque dilemmas that scores of citizens have confronted when they attempt to learn why they are consistently flagged and seek to clear their names.[2] TSA refuses to provide these individuals with any explanations, and the agency's claimed procedure for addressing these problems, as USA Today noted, "is cumbersome, confusing and – the TSA concedes – doesn't guarantee success."[3]

Although few details of CAPPS II have been disclosed, the Privacy Act notice for the system that TSA published on August 1, 2003,[4] provides a basic outline of how it would operate. In essence, CAPPS II will be a secret, classified system that the agency will use to conduct background checks on tens of millions of airline passengers. The resulting "risk assessments" will determine whether individuals will be subject to invasive searches of their persons and belongings, or be permitted to board commercial aircraft at all. TSA will not inform the public of the categories of information contained in the system. It will include information that is not "relevant and necessary" to accomplish its stated purpose of improving aviation security. Individuals will have no judicially enforceable right to access information about them contained in the system, nor to request correction of information that is inaccurate, irrelevant, untimely or incomplete. It is important to note that this is precisely the sort of system that Congress sought to prohibit when it enacted the Privacy Act of 1974.[5]

---

[2] See http://www.epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html

[3] *Glitches Repeatedly Delay Innocent Air Travelers*, USA Today, June 25, 2003, Page 11A.

[4] Interim Final Privacy Act Notice, 68 Fed. Reg. 45265 (August 1, 2003).

[5] 5 U.S.C. § 552a.

Given its constitutional implications, and the massive scope of the system (which seeks to collect information about tens of millions of individuals), CAPPS II understandably has been the focus of concern within Congress and the general public. It has also engendered strong opposition abroad, where foreign governments and their citizens have resisted the demands of the U.S. government to provide detailed air passenger data as a condition of flight into the United States. Reflecting those concerns, a resolution was passed last September at the International Conference of Data Protection and Privacy Commissioners in Sydney, Australia calling for "an international agreement stipulating adequate data protection requirements, including clear purpose limitation, adequate and non-excessive data collection, limited data retention time, information provision to data subjects, the assurance of data subject rights and independent supervision" before such data transfers occur.[6]

Much of the controversy surrounding CAPPS II has centered on the system's secrecy and the lack of public information concerning the manner in which it will assess the security risks particular individuals are deemed to pose, and the types of data that TSA will use to make such assessments. When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal information that federal agencies could collect and, significantly, required agencies to be transparent in their information practices.[7] 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[.]"[8] Adherence to these requirements is critical for a system like CAPPS II.

In remarks before the international conference of data protection and privacy officials, the Chief Privacy Officer of the Department of Homeland Security assured the delegates that

> [u]nder the Privacy Act, in concert with the Freedom of Information Act and the E-Government Act, citizens, legal residents, and visitors to the United States have been afforded almost unequalled transparency into the federal government's activities and the federal government's use of personal information about them.[9]

---

[6] Resolution Concerning the Transfer of Passengers' Data, 25th International Conference of Data Protection & Privacy Commissioners (September 12, 2003) (available at http://www.epic.org/ news/Comm03.html).

[7] S. Rep. No. 93-1183, at 1 (1974).

[8] *Id*.

[9] Remarks of Nuala O'Connor Kelly Before the 25th International Conference of Data Protection and Privacy Commissioners, Sydney Australia, September 11, 2003 ("Kelly Remarks").

Unfortunately, the Department of Homeland Security and TSA have fallen far short of such transparency in the realm of aviation security.

The Lack of Transparency Surrounding CAPPS II

Soon after enactment of the Aviation and Transportation Security Act, Pub. L. No. 107-71, and the creation of TSA, EPIC began requesting information from the agency under the Freedom of Information Act seeking information on the potential privacy impact of CAPPS II. TSA has strenuously resisted the disclosure of virtually all relevant information, so there is only a sparse public record concerning the system's proposed operation.

One of EPIC's FOIA requests sought the release of TSA's Privacy Impact Assessment ("PIA") and the "Capital Asset Plan and Business Case" for the CAPPS II project. On September 25, 2003, TSA responded to the request and advised EPIC that both documents exist only in draft form and that "final versions . . . are not expected until early 2004."[10] To date, these documents have not been made public. The fact that the PIA and Business Case have not been finalized is significant because their preparation for a system such as CAPPS II is mandated by the E-Government Act and Office of Management and Budget ("OMB") regulations, respectively. The E-Government Act requires that agencies "*shall* conduct a privacy impact assessment . . . *before* . . . initiating a new collection of information that . . . will be collected, maintained, or disseminated using information technology."[11] Likewise, OMB regulations require agencies, when proposing "major" or "significant" information technology projects, to address privacy and security issues in their Business Case submissions and to prepare PIAs.[12]

In his testimony before Congress on May 6, 2003, then-TSA Administrator Loy stated that "TSA is mindful that privacy protections must be built into the CAPPS II system from its very foundation" and said that the agency was "working to finalize its CAPPS II business case, which will detail how privacy and security are built into the system" and "also will conduct a

[10] Letter from Patricia M. Riep-Dice to David L. Sobel, September 25, 2003 (available at http://www.epic.org/privacy/airtravel/pia-foia-response.pdf).

[11] Pub. L. No. 107-347 (December 17, 2002), § 208 (emphasis added).

[12] OMB Circular A-11, part 3, Planning, Budgeting and Acquisition of Capital Assets (July 2000); Memorandum from Joshua B. Bolton, "Implementation Guidance for the E-Government Act of 2002" (August 1, 2003) (available at http://www.whitehouse.gov/omb/memoranda/m03-18.pdf).

Privacy Impact Assessment."[13] It is thus surprising to find TSA continuing to move ahead with CAPPS II before the privacy implications of the system have been fully addressed and disclosed to the public. Indeed, the recent General Accounting Office ("GAO") report on CAPPS II underscores that fact. The GAO, in a report on another DHS information system, noted that "OMB requires that IT projects . . . perform a system privacy impact assessment, so that relevant privacy issues and needs are understood and appropriately addressed *early and continuously* in the system life cycle."[14] CAPPS II has been under development for more than two years; it is clear that TSA has failed to meet its obligation to address the privacy implications "early and continuously," as federal law requires. We cannot have an informed public debate on the implications of CAPPS II unless and until TSA publishes a Privacy Impact Assessment and discloses other information about the system. Unfortunately, as I will explain in my discussion of the CAPPS II Privacy Act notice issued by TSA, lack of transparency is likely to be a key characteristic of the system.

CAPPS II Contravenes the Intent of the Privacy Act

The Privacy Act was intended to guard citizens' privacy interests 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."[15] 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.[16]

DHS's Chief Privacy Officer recently touted the protections afforded by the Privacy Act, explaining that the law

[13] Testimony of Admiral James Loy before House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census (May 6, 2003) ("May 6 Loy Testimony").

[14] INFORMATION TECHNOLOGY: Homeland Security Needs to Improve Entry Exit System Expenditure Planning, GAO-03-563 (June 2003) (emphasis added).

[15] Pub. L. No. 93-579 (1974).

[16] *Id.*

> provides substantial notice, access, and redress rights for citizens and legal residents of the United States whose information is held by a branch of the federal government. The law provides robust advance notice, though detailed "system of records" notices, about the creation of new technological or other systems containing personal information. The law also provides the right of access to one's own records, the right to know and to limit other parties with whom the information has been shared, and the right to appeal determinations regarding the accuracy of those records or the disclosure of those records.[17]

TSA, however, has sought to exempt CAPPS II from nearly all of the Privacy Act provisions Ms. O'Connor Kelly described.[18]

1. TSA Will Not Disclose the Sources of Information Fed Into CAPPS II

Under the Privacy Act, government transparency is the rule rather than the exception. TSA has frustrated that intent by exempting the CAPPS II system of records from the requirement that it publish "the categories of sources of records in the system."[19]

The legislative history of the Privacy Act unequivocally demonstrates that government agencies must be open about their information collection practices unless they can show that exceptional circumstances require secrecy. One key objective of the Privacy Act is to ensure that agencies "give detailed notice of the nature . . . of their personal data banks and information systems . . . ."[20] The Senate Report notes that "it is fundamental to the implementation of any privacy legislation that no system of personal information be operated or maintained in secret by a Federal agency."[21] In those few instances in which a limited exemption for national security and law enforcement was recognized, the exemption was "not intended to provide a blanket exemption to all information systems or files maintained by an agency which deal with national defense and foreign policy information."[22] Rather, the agency must show that the

---

[17] Kelly Remarks.

[18] Indeed, TSA has invoked exemptions for *all* of the requirements that the Privacy Act permits an agency to invoke.

[19] 5 U.S.C. § 552a(e)(4)(I); Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45269.

[20] S. Rep. No. 93-1183, at 2 (1974).

[21] *Id*. at 74.

[22] *Id*.

implementation of specific Privacy Act provisions would "damage or impede the purpose for which the information is maintained."[23]

In its authoritative guidance on implementation of the Privacy Act, OMB explained that "[f]or systems of records which contain information from sources other than the individual to whom the records pertain, the notice should list the types of sources used."[24] While "[s]pecific individuals or institutions need not be identified," the Act contemplates that general categories, such as "financial institutions" or "educational institutions" should be listed.[25]

Despite the Privacy Act's clear emphasis on transparency and TSA's claimed dedication to preserving individuals' privacy, the agency seeks to avoid the requirement that it inform the public of the sources of information that will feed into the CAPPS II system. TSA has not even attempted to meet its burden of demonstrating that the publication of such basic information about the system would somehow impede its presumed effectiveness.

In the supplementary material accompanying its Privacy Act notice, TSA asserted that it "will not use measures of creditworthiness, such as FICO scores, and individual health records in the CAPPS II traveler risk determination."[26] That assurance rings hollow, however, in light of the agency's stated intention to keep secret the sources of information that will eventually be fed into the system.

TSA's determination that CAPPS II will be exempt from the requirement of publishing categories of sources of records is at odds with specific assurances the agency provided to Congress. When asked about this issue last May, Admiral Loy indicated that such information would, in fact, be disclosed:

> Senator Byrd: Will the new notice name the precise databases of information that CAPPS II will collect about air passengers?
>
> Admiral Loy: I don't know that we have any reason not to name those in the privacy notice . . . .[27]

---

[23] *Id*. at 75.

[24] OMB Guidelines at 28964.

[25] *Id.*

[26] Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45267.

[27] *The Fiscal Year 2004 Appropriations for the Bureau of Customs and Border Security; Transportation Security Administration and Federal Law Enforcement Training Center, Hearing Before the Homeland Security*

If TSA cannot articulate any reason to exempt CAPPS II from publishing categories of sources of records, it should not exempt the system from that requirement. The Privacy Act does not permit such secrecy unless an agency can demonstrate that it is absolutely necessary for reasons of national security and law enforcement.

2. TSA Will Not Provide Meaningful Citizen Access to Personal Information

In its Privacy Act notice, TSA has exempted CAPPS II from all Privacy Act provisions guaranteeing citizens the right to access records containing information about them. The Privacy Act provides, among other things, that

- an individual may request access to records an agency maintains about him or her;[28] and
- the agency must publish a notice of the existence of records in the Federal Register, along with the procedures to be followed to obtain access.[29]

In lieu of the statutory, judicially enforceable right of access provided by the Privacy Act, TSA plans to establish the "CAPPS II Passenger Advocate," apparently to act as a sort of ombudsman, to receive and process requests for access. According to the supplementary information accompanying TSA's notice, "passengers can request a copy of *most* information contained about them in the system from the CAPPS II passenger advocate."[30] The formal notice section, however, states that "[a]ll persons may request access to records containing information *they* provided," which presumably would include only the name, address, and telephone number given to an airline when making a travel reservation.[31] In addition, the notice provides that the system of records "may not be accessed for purposes of determining if the

---

Subcommittee of the Senate Appropriations Committee, 108th Cong. (May 13, 2003) (testimony of Admiral James Loy).

[28] 5 U.S.C. § 552a(d)(1). Individuals may seek judicial review to enforce the statutory right of access provided by the Act. 5 U.S.C. § 552a(g)(1).

[29] 5 U.S.C. §§ 552a(e)(4)(G), (e)(4)(H), (f).

[30] Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45267 (emphasis added).

[31] *Id*. at 45269 (emphasis added).

system contains a record pertaining to a particular individual."[32] Such limited, discretionary access to information is an inadequate substitute for the access provisions set forth in the Privacy Act, and TSA offers no explanation why such restricted access is necessary in the context of CAPPS II.

TSA's "passenger advocate" acting as middleman is no substitute for the judicially-enforceable access rights provided by the Privacy Act. TSA's notice states that access to one's personal information may be obtained "by sending a written request to the CAPPS II Passenger Advocate" and that "to the greatest extent possible and consistent with national security requirements, such access will be granted."[33] No time guidelines are specified for the procedure. However, TSA explains that "in most cases, the response to a record access request will very likely be that no record of the passenger exists in the system" because records are maintained for too short a time, although "[t]he duration of data retention" for non-U.S. persons "is still under consideration," and "[e]xisting records obtained from other government agencies, including intelligence information, watch lists, and other data will be retained for three years, or until superseded."[34]

As a practical matter, therefore, the only information a passenger would be able to access is the information he provided to the airlines himself. Moreover, even this information may not be accessible, as that information will likely be destroyed in the time it takes a passenger to contact the passenger advocate. In most cases, a passenger will be unable to gain access to records about him kept by the agency, and, in many cases, he will not even be able to learn that a record pertaining to him exists. In fact, the only indication a passenger may have that the government is keeping records about him is if he is subjected to extra scrutiny at the security gate (or, of course, detained and arrested there). TSA's weak access provisions are in direct conflict with the purposes of the Privacy Act, which sought to provide citizens with an enforceable right of access to personal information maintained by government agencies.

[32] *Id.*

[33] *Id.*

[34] *Id.*

3. TSA Will Not Provide Citizens Meaningful Opportunities to Correct Inaccurate, Irrelevant, Untimely and Incomplete Information

Companion and complementary to the right to access information is the right to ensure that it is accurate. TSA's Privacy Act notice establishes a system that provides neither adequate access nor the ability to amend or correct inaccurate, irrelevant, untimely and incomplete records. The agency has exempted the CAPPS II system from the Privacy Act requirements that define the government's obligation to allow citizens to challenge the accuracy of information contained in their records, such as:

- an agency must correct identified inaccuracies promptly;[35]
- an agency must make notes of requested amendments within the records;[36] and
- an agency must establish procedures to handle disputes between the agency and individual as to the accuracy of the records.[37]

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, timeliness, and completeness as is reasonably necessary to assure fairness to individuals in making determinations about them.[38]

Instead of the judicially enforceable right to correction set forth in the Privacy Act,[39] TSA has established its own, discretionary set of procedures for passengers to contest the accuracy of their records. TSA's notice states that "[a] passenger who, having accessed his or her records in this system, wishes to contest or seek amendment of those records should direct a written request

[35] 5 U.S.C. § 552a(d)(2)(B), (d)(3).

[36] 5 U.S.C. § 552a(d)(4).

[37] 5 U.S.C. § 552a(f)(4).

[38] H.R. Rep. No. 93-1416, at 15 (1974).

[39] 5 U.S.C. § 552a(g)(1).

to the CAPPS II Passenger Advocate."[40] Further, "[i]f the matter cannot be resolved by the CAPPS II Passenger Advocate, further appeal for resolution may be made to the DHS Privacy Office."[41] Notably, TSA reserves the right to alter even these minimal, discretionary procedures: "These remedies for all persons will [be] more fully detailed in the CAPPS II privacy policy, which will be published before the system becomes fully operational."[42] In addition, "DHS is currently developing a robust review and appeals process, to include the DHS privacy office."[43]

The notice provides TSA the discretion to correct erroneous information upon a passenger's request, but does not obligate the agency to do so. Significantly, there would be no right to judicial review of TSA's determinations. This correction process offers a token nod to the principles embodied in the Privacy Act, but does not provide a meaningful avenue to pursue correction and is subject to change at TSA's whim. Furthermore, the agency presents no explanation why judicially-enforceable Privacy Act correction procedures would be inappropriate in the context of CAPPS II. Denying citizens the right to ensure that the system contains only accurate, relevant, timely and complete records will increase the probability that CAPPS II will be an error-prone, ineffective means of singling out passengers as they seek to exercise their constitutional right to travel.

4. CAPPS II Will Not Be Limited to Collection of Information That Is "Relevant and Necessary"

Incredibly, TSA has exempted CAPPS II from the fundamental Privacy Act requirement that an agency "maintain in its records only such information about an individual as is relevant and necessary" to achieve a stated purpose required by Congress or the President.[44] TSA does not even attempt to explain why it would be desirable or beneficial to maintain information in the CAPPS II system that is irrelevant and unnecessary, although it apparently intends to do so. Such open-ended, haphazard data collection plainly contradicts the objectives of the Privacy Act

[40] Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45269.

[41] *Id.*

[42] *Id.*

[43] *Id.*

[44] 5 U.S.C. § 552a(e)(1); Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45269.

and raises serious questions concerning the likely impact of the CAPPS II rating process on millions of law-abiding travelers.

In adopting the Privacy Act, Congress was clear in its belief that the government should not collect and store data without a specific, limited purpose. The "relevant and necessary" provision

> reaffirms the basic principles of good management and public administration by assuring that the kinds of information about people which an agency seeks to gather or solicit and the criteria in programs for investigating people are judged by an official at the highest level to be relevant to the needs of the agency as dictated by statutes . . . . This section is designed to assure observance of basic principles of privacy and due process by requiring that where an agency delves into an area of personal privacy in the course of meeting government's needs, its actions may not be arbitrary[.][45]

As OMB noted in its Privacy Act guidelines, "[t]he authority to maintain a system of records does not give the agency the authority to maintain any information which it deems useful."[46]

The Privacy Act's "relevant and necessary" provision thus seeks to protect individuals from overzealous, arbitrary and unnecessary data collection. It embodies the common sense principle that government data collection is likely to spiral out of control unless it is limited to only that information which is likely to advance the government's stated (and legally authorized) objective. Like TSA's other deviations from customary Privacy Act requirements, the "relevant and necessary" exemption will serve only to increase the likelihood that CAPPS II will become an error-filled, invasive repository of all sorts of information bearing no relationship to its stated goal of increasing aviation security.

5. Broad "Routine Uses" of CAPPS II Data Will Exacerbate the System's Privacy Problems

TSA's Privacy Act notice identifies six categories of "routine uses" of the information that will be collected and maintained in the CAPPS II system of records.[47] These include anticipated disclosure to a broad range of individuals and entities, such as "Federal, State, local,

[45] S. Rep. No. 93-3418, at 47 (1974).

[46] OMB Guidelines at 28960.

[47] Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45268.

international, or foreign agencies or authorities . . . contractors, grantees, experts, or consultants . . . airports and aircraft operators."[48] As noted, the information that would be disclosed is likely to include material about individuals that is not "relevant and necessary" to any legitimate aviation security requirements. Nor would such information be subject to a meaningful and enforceable process to ensure that it is accurate, relevant, timely or complete. The broad dissemination of CAPPS II information that TSA anticipates underscores the need for full transparency (and resulting public oversight) and judicially-enforceable rights of access and correction.

Related to the breadth of the routine uses is the issue of "mission creep" – the tendency of government agencies to expand the use of personal information beyond the purpose for which it was initially collected. Admiral Loy discussed the issue in Congressional testimony, stating that "mission creep, if you will, is one of those absolute parameters that . . . I am enormously concerned about and we will build such concerns into the privacy strategy that we will have for CAPPS II."[49] Three months before the notice was published, Admiral Loy assured Congress that CAPPS II was designed as an aviation security tool, and not as a law enforcement tool.[50]

Despite those assurances, the CAPPS II system already contains a carve-out for a purpose beyond its original mission. The Privacy Act notice states that "[a]fter the CAPPS II system becomes operational, it is contemplated that information regarding persons with outstanding state or federal arrest warrants for crimes of violence many also be analyzed in the context of this system."[51] While the government clearly has a legitimate interest in apprehending accused felons, there are innumerable reasons why it may want to locate particular individuals. Such uses of CAPPS II data, however, are plainly beyond the authorized scope of TSA's mission of

---

[48] *Id.*

[49] May 6 Loy Testimony.

[50] *Id*. Admiral Loy stated:

> [w]e are not searching [the National Crime Information Center database] as part of the . . . data that we're looking at . . . . [A]t the moment we are charged with finding in the aviation sector foreign terrorists or those associated with foreign terrorists and keep[ing] them off airplanes. That is our very limited goal at the moment. . . . [E]ven as heinous as it sounds, the axe murderer that gets on the airplane with a clean record in New Orleans and goes to Los Angeles and commits his or her crime, that is not the person we are trying to keep off that airplane at the moment.

[51] Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45266.

ensuring aviation security. It is crucial that TSA define the purpose of CAPPS II, at the outset, more strictly and limit the use of collected information to its core mission.

Testing of CAPPS II Should Not Proceed Until TSA's Notice is Revised

While TSA has stated that "[a] further Privacy Act notice will be published in advance of any active implementation of the CAPPS II system,"[52] it also indicated in its August notice that "[w]ith the publication of this notice, internal systems testing will begin, using this System of Records."[53] According to the agency, "[d]uring these tests, TSA will use and retain [Passenger Name Record] data for the duration of the test period."[54] It has been reported that TSA is contemplating the issuance of a security directive requiring U.S. airlines to provide the agency with passenger information for use in the testing process.[55] Such data acquisition would place in the agency's hands personal information concerning millions of individuals without, as I have discussed, meaningful rights of access or correction. TSA has articulated no reason why such rights should not be provided and, as such, even limited use of personal information for testing purposes would raise significant privacy issues. Acquisition of personal data should not proceed until TSA revises its policies and practices to bring them into conformance with the intent of the Privacy Act.

---

[52] *Id*.

[53] *Id*. at 45265-45266.

[54] *Id*. at 45267.

[55] Sara Kehaulani Goo, *TSA May Try to Force Airlines to Share Data*, Washington Post, September 27, 2003, Page A11. It is unclear whether TSA plans to compel passenger data from airlines through a security directive or a proposed rulemaking. The GAO report on CAPPS II states:

> TSA officials stated that they are continuing to seek needed passenger data for testing, but believe they will continue to have difficulty in obtaining data for both stress and other testing until TSA issues a Notice of Proposed Rulemaking to require airlines to provide passenger data to TSA. This action is currently under consideration within TSA and DHS.

AVIATION SECURITY: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges, GAO-04-385 (February 2004).

Conclusion

As the recent GAO report found, TSA has failed to adequately address the very real privacy and due process issues that permeate the proposed system. Based upon TSA's Privacy Act notice for the system, I believe there is reason to doubt whether the system, as currently envisioned, can ever function in a manner that protects privacy and provides citizens with basic rights of access and redress. In order for CAPPS II to pass muster from a privacy and civil liberties perspective, TSA must, at a minimum: 1) ensure greater transparency through the establishment of a non-classified system; 2) provide individuals enforceable rights of access and correction; 3) limit the collection of information to only that which is necessary and relevant; and 4) substantially limit the routine uses of collected information. Further, development of the system should be suspended until TSA prepares a final Privacy Impact Assessment, discloses it to the public and receives public comments. Finally, the agency should not acquire personal information, even for testing purposes, until it has revised its policies and procedures as suggested above.

Thank you for the opportunity to address the serious privacy and due process implications of CAPPS II, and for your consideration of the critical issues raised by the proposed system. I encourage the subcommittee to continue its inquiry and to ensure that the privacy and due process rights of airline passengers are preserved as we develop effective and appropriate aviation security measures.