March 14, 2003

Documentary Services Division
Attention: Docket Section, Room PL401
Docket No. OST-1996-1437 Department
of Transportation, SVC-124,
Washington, DC 20590

RE: Docket No. OST-1996-1437 ASSR Regulations – Proposed exemptions from the Privacy Act of 1974

Dear Director,

The Electronic Frontier Foundation, PrivacyActivism, Privacy Rights Clearinghouse, CASPIAN and Michael Stollenwerk (the Commenting Parties) appreciate the opportunity to comment on the Department of Transportation's proposed exemption of records in the Aviation Security Screening Records (ASSR) system from the Privacy Act of 1974, as described in the Notice of Proposed Rules published in the Federal Register, January 15, 2003, (Volume 68, Number 10) ("the Notice").

For the reasons set out below, the Commenting Parties oppose the proposed exemptions. In particular, we consider that: (1) the proposed exemptions do not meet the justification requirements under sections 552a(k)(1) and (2) of the Privacy Act; (2) exempting risk assessments and all the information contained in them will have a seriously damaging effect on individuals' privacy rights and civil liberties, in various respects – primarily because the proposed exemption will preclude an individual from learning that information is being collected about him or her and from having any access to that data; (3) the proposed exemptions will have a significantly adverse effect on individuals' Constitutional right to freedom of travel, and (4) the proposed exemptions will not achieve the intended outcomes of improving the effectiveness of passenger screening and increasing national security.

For these reasons, we reiterate our request that both the proposed ASSR regulations establishing the system of records to be collected and maintained by TSA, together with the proposed exemptions from the Privacy Act, be withdrawn.

I. Scope of System proposed and Relationship to CAPPS II database

We also wish to re-emphasize our concern, expressed in our previous comments to the Department of Transportation (DoT) dated February 19, 2003, that it appears that ASSR will be used as one of the key component databases in the Computer Assisted Passenger Prescreening System II (CAPPS II). Given the nature and unlimited scope of the information proposed to be collected by the TSA under ASSR – including risk assessment reports, financial and transactional data, and both public and proprietary data about individuals, we believe it is incumbent upon the DoT to notify the American public if this data is intended to be used in the controversial CAPPS II system. In light of the broad exemptions proposed from the Privacy Act's provisions governing disclosure, access and accountability, it is particularly important that the TSA now clarify the

relationship between the ASSR and CAPPS II.

II. Specific Concerns about the Proposed Exemptions

1. Under the proposed exemptions, individuals would have no ability to learn whether the TSA has collected personal information about them and would be deprived of any ability to access their personal information held in the database, to verify its accuracy, or to correct any data errors

The Privacy Act was enacted to provide various specific procedural safeguards to protect individuals' privacy and to promote accountability by government record-holders. In particular, the Act requires a federal agency that collects and maintains personal data about an individual to:

- Notify the individual that he or she is listed in the database (§ 552a(f));
- Upon request, provide the individual with "access to his record or to any information pertaining to him which is contained in the system" for the purposes of review (§ 552a(d)(1)); and
- provide an opportunity for the individual to request an amendment or correction, if he or she believes the personal record is inaccurate, or the opportunity to challenge the federal agencies' decision to not amend the perceived inaccuracy (§552a(d)(2) – (4)).

The proposed amendments would remove all of these important procedural safeguards. Although the First Register notice purports to provide limited alternative procedures for access and contesting records, in the absence of a requirement that the TSA notify affected individuals, as provided for under §552a(f), these procedures are practically meaningless, for the reasons described in more detail below.

2. The Proposed Exemptions do not meet the justification requirements under § 552a(k)(1) and (2) of the Privacy Act.

The Privacy Act contemplates specific exemptions from these crucial procedural protections only where a federal agency meets the requirements of the relevant portions of §552a(k). The Commenting Parties consider that the TSA has not provided sufficient justification for the proposed exemptions.

The Notice states that the TSA proposes exemption of information in the system, including "information regarding TSA's conduct of risk assessments", as:

(a) "properly classified information", pursuant to §552a(k)(1); and

(b) "investigatory material compiled for law enforcement purposes", pursuant to§552a(k)(2).

However, the Notice provides no justification for these exemptions. The Notice merely states that "the system may be used, generally, to review, analyze, and assess threats to transportation security and respond accordingly".

Accordingly, it is by no means clear that the exemptions in §552a(k)(1) and (2) have been properly invoked, and there is no mechanism for the public to review the information to assess the appropriateness of the claim to exemption on these bases.

In light of the deficiencies in the first Federal Register Notice, upon which we have already commented, and the absence of further information about the nature and

sources of the information to be collected and the purposes for which it will be used, the Commenting Parties are concerned that TSA's claim to exemptions may amount to an improper attempt to avoid appropriate accountability and the ongoing heated public debate regarding secret data surveillance systems. [1]

3. The Proposed Exemptions are Overbroad

Although the Notice refers to "TSA's conduct of risk assessments", as worded, the exemption proposed would cover the entire system established by ASSR (the ASSR system). The proposed exemptions are overbroad in several respects.

.(1) the scope of the exemption is not limited to, or proportional with, the categories of exemptable records within the proposed ASSR system;
.(2) the exemptions would allow the TSA to collect and store an extensive range ofrecords on *all* individuals, because the apparent limitation on the categories of records to be collected based on the ability to distinguish two separate classes of individuals is meaningless; and
.(3) the wide scope of the exemptions would permit the TSA to collect, store anduse types of records beyond the two nominated exemptable categories of records, including information such as potentially subjective risk assessment reports and credit ratings provided by private data agencies.

a) The scope of exemption is likely to be out of proportion with the categories of exemptable records

The proposed exemption raises a general policy issue about proportionality and compliance with the spirit and intent of the Privacy Act. The Notice purports to exempt the entire ASSR system on the basis of exemptions (k)(1) and (2). However, the wording in the Notice invokes both of those exemptions "to the extent that ASSR contains [the relevant category of exempted information]" but fails to identify what proportion of the records in the system are either "properly classified" or "investigatory material compiled for law enforcement purposes".

Accordingly, the Commenting Parties are concerned that the DoT may be attempting an administrative sleight of hand, by relying on a small volume of exemptable documents to inappropriately obtain a blanket exemption for the entire system. The entire scheme of the Privacy Act – and in particular, the careful description of the seven permissible categories of exemptable documents in s§552a(k) – is designed to prevent such blanket system-wide exemptions. The Notice's failure to disclose any information about the proportion of the system records that fall within these categories makes it impossible for the public to assess the appropriateness of the purported exemption of the entire system from the procedural safeguards of the Privacy Act.

---

[1] Apart from the overwhelming level of public concern about the proposed use of pre-screening databases, the travel industry has also expressed strong concern. *See for instance*, the letter from the Executive Director of the National Business Travel Association to the Undersecretary of Transportation Security dated March 5, 2003, describing travel industry concerns about TSA passenger pre-screening and requesting a "privacy impact analysis" of the proposed CAPPSII, available at http://www.nbta.org (visited March 12. 2003), and *Travel Industry and Privacy Groups Object to Screening Plan for Airline Passengers*, David Jones, NY TIMES, March 6, 2003.

b) The exemptions would allow the TSA to collect and store an extensive range of records on all individuals

At first glance, the first Federal Register notice published on January 15, 2003 appears to establish a two-tier record collection system. The first Federal Register notice describes two classes of affected individuals - "[I]ndividuals traveling to, from, or within the United States.. by passenger air transportation" (namely, all airline passengers) and "individuals who are deemed to pose a possible risk to transportation or national security, a possible risk of air piracy or terrorism, or a potential threat to airline or passenger safety, aviation safety, civil aviation or national security." For "passengers", the information to be collected is Passenger Name Records "and associated data" and reservation and manifest information of passenger carriers. By comparison, for "deemed individuals", the categories are much broader, and include "risk assessment reports, financial and transactional data; public source information; proprietary data; and information from law enforcement and intelligence sources."

However, the supposed distinction between the different classes of individuals disappears on closer analysis. Therefore, in practice, it seems likely that the TSA would be authorized to collect a very wide range of information about *all* traveling individuals. The first Federal Register notice does not specify any criteria that the TSA will use to identify which members of the traveling public are "deemed individuals". If, as may appear to be the case, the documents collected as part of ASSR are to be used to assess whether an individual should be deemed risky, then using the "deemed risk" of an individual as the criteria for deciding which type of documents can be collected in the first instance, is completely meaningless.

In addition, even if there were a meaningful way for TSA to distinguish "passengers" from "deemed individuals", the range of documents that TSA could gather about a non-deemed "passenger" is still unacceptably broad. The first Federal Register Notice states that the TSA would be charged with collecting "Passenger Name Records and *associated data*". "Associated data" is not defined in the Notice, and the Commenting Parties are very concerned that it will be construed broadly enough to include all kinds of information that is neither classified for national security nor investigatory material compiled for law enforcement purposes. If so, it is possible that all individuals will be subject to a vague, and practically unlimited data collection process. All individuals would also then be at risk of having adverse decisions made against them on the basis of frequently inaccurate or outdated information, such as third party credit ratings.

c) The wide scope of the exemptions would permit the TSA to collect, store and use types of records beyond the two nominated exemptable categories of records, including information such as potentially subjective risk assessment reports and credit ratings provided by private data agencies.

On the basis of what little information has been disclosed, it appears that the ASSR system will include information that is not classified and that would not be considered "investigatory material compiled for law enforcement purposes". On our reading of the first Federal Register notice, the categories of records to be collected for use in pre-screening would be broad enough to include such non-

classified information and non-investigatory material as an individual's credit history or credit rating, provided to the TSA by a private third party data agency, such as Experian.

The Notice refers specifically to "TSA's conduct of risk assessments". As noted in our previous comments, the TSA has not indicated what information would be used to form these risk assessments, or what process will be used for assessing risk. As a result, it is obviously difficult to assess and verify the DoT's claim for exemption on these bases.

If the proposed rules are allowed to go forward, there would be no accountability of the agency to individuals usually provided by the Privacy Act (sec.(c)(3)); no access to information about the individual (sec. (d)); no restriction to relevant information (sec. (e)(1); no notification to the individual if there is a file about him or her in the database, nor any ability to see the categories of information (sec. (e)(g & h); there will be no procedures for access (sec. (f)); and finally, an exemption for investigatory materials as well (sec. 552a(k) (1) and (2).

This proposal fails to take into account the likelihood of incorrect information in risk assessment reports, and does not provide individuals any recourse in that case. For example, information could be included in a risk assessment report based on a (potentially-erroneous) public record stating that an individual lived in a certain place at a certain time. If the information in that record is inaccurate, an erroneous conclusion may be drawn about that person. Similarly, if an investigatory report was made about an individual that contained erroneous information, again an incorrect conclusion may be drawn about that person. If this same individual was a victim of identity theft (not an uncommon occurrence) and the identity thief committed crimes in the victim's name[2], again bad information would be added to the assessment report.

In any of these cases, there would be no way for the aggrieved passenger to know what information contributed to his negative profile, nor would he or she be able to correct the information.

4. Even if the Proposed Exemption under §552a(k)(2) is justified, the limited alternative access procedures provided are deficient and there are insufficient procedural safeguards for individuals' privacy

The proposed regulations and exemptions do not meet the important proviso in §552a (k)(2) that:

> " … if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the government under an express promise that the identity of the source would be held in confidence.."

[2] "The Darkest of ID Theft: When imposters are arrested, victims get criminal records" http://www.msnbc.com/news/877978.asp?0si=-&cp1=1

The routine uses described in the first Federal Register notice include several ways that information in the system may be used to deny an individual access to a right, privilege, or benefit to which he would otherwise be eligible. For instance, routine use (5) covers "the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant or other benefit." It is possible that ASSR will include records or information provided by a source who furnished it to the government under an express promise of confidentiality – for instance, it is conceivable that this type of information could be found in "investigatory material compiled for law enforcement purposes". However, the information disclosed thus far by DoT gives no indication whether such information exists, or if so, what proportion of the total system of records it comprises. As a result, it is difficult to assess whether the proposed exemption triggers the proviso in §552a(k)(2). To the extent that the proviso is triggered, it requires the system to provide access procedures for categories of information that could be used to deny individuals access to rights, privileges or benefits that they would otherwise enjoy.

The first Federal Register notice provides for a limited alternative access procedure. It states that:

> "U.S. Citizens or Permanent Resident Aliens may request access to records containing information they provided by sending a written request to the System Manager. In the case of air passengers, this data is contained in the passenger name record (PNR). The request must identify the system from which the individual is seeking records, and include a general description of the records sought, the requester's full name, current address and date and place of birth. …"

However, in practice, this limited procedure would not meet the requirements of the proviso in §552a(k)(2) for three reasons. First, most of the information to be incorporated in the ASSR system does not appear to be provided by individuals and so would fall outside the scope of this procedure. As a result, there is no mechanism for individuals to access the substantial additional categories of information about an individual that would be exempted under the Notice. Second, as the TSA is proposing to exempt the system from the Agency notification requirements in §552a(f) of the Privacy Act, an individual would have no way to learn either that he or she was included in the ASSR system, or that adverse decisions or negative assumptions were being made against the individual, based on inaccurate and uncorrectable data.

5. There is no basis to suggest that the System will be efficacious to achieve its intended purpose

Finally, we question whether the ASSR and the proposed exemptions will actually serve the intended goals of increased ability to identify potential terrorists, and "persons who pose a possible risk to national security" or " a potential threat to airline or passenger safety" amongst the traveling public. It is not clear to us that the nature of the records being compiled will provide a qualitative improvement in the range of data currently available to the TSA from the CAPPS I system and the airlines' passenger data.

More importantly, exempting both the process by which TSA arrives at risk assessments and the nature of information used to form risk assessments from scrutiny by affected individuals and the general public is likely to make the system less, not more, secure, because there will be no ability to notice and correct the inevitable errors in

component data and inaccurate assumptions in risk assessment methodology.

6. Conclusion

While the commenting parties acknowledge that the Privacy Act provides federal agencies with the ability to exempt records from the Act's procedural safeguards where national security and other strong governmental interests are in issue, it is not at all clear that the proposed exemptions qualify. Moreover. the proposed exemptions are dangerously overbroad and do not provide individuals with any meaningful safeguards against improper incursions into their Constitutional privacy rights. The overbroad scope of the information proposed to be collected under ASSR, together with the failure to clearly identify all uses to which that information may be put, the unusually wide proposed "routine uses", and lack of sufficient justification provided for the claimed exemptions, are all of major concern to the Commenting Parties. Most importantly, the proposed exemptions would provide the framework to legitimize the very thing that the Privacy Act was enacted to prevent – the creation and ongoing storage of extensive secret files of sensitive personal information about all U.S. citizens and permanent resident aliens.

For these reasons, we respectfully request that the DoT and TSA withdraw the proposed ASSR system and the proposed exemptions from the Privacy Act for that system.

Thank you for your consideration.

Sincerely,

Lee Tien, Esq., Senior Staff Attorney
Gwen Hinze, Esq., Staff Attorney
Electronic Frontier Foundation

Deborah Pierce, Esq., Executive Director
PrivacyActivism

Beth Givens, Director Privacy Rights
Clearinghouse

Katherine Albrecht, CASPIAN

Michael Stollenwerk

For contact purposes, please contact:
Lee Tien Senior Staff Attorney Electronic Frontier Foundation 454 Shotwell Street, San Francisco, CA 94110 tien@eff.org Tel: (415) 436 9333 x 102 • Fax: (415) 436 9993