WORLD **PRIVACY** FORUM

Comments of the World Privacy Forum regarding docket number DHS-2007-0040; Border Crossing Information

to

Department of Homeland Security, Office of the Secretary

Via fax and federal e-rulemaking portal www.regulations.gov

Hugo Teufel III, Chief Privacy Officer,
Privacy Office,
Department of Homeland Security,
Washington, DC 20528

August 21, 2008

The World Privacy Forum appreciates the opportunity to comment on the Department of Homeland Security's notice of a new Privacy Act of 1974 system of records at 73 Federal Register 43457-43462 (July 25, 2008). The new system would be called Border Crossing Information (BCI).

The World Privacy Forum is a non-partisan, non-profit public interest research and consumer education organization. Our focus is on conducting in-depth research and analysis of privacy issues, in particular issues related to information privacy. More information about the activities of the World Privacy Forum is available at <http://www.worldprivacyforum.org>.

These comments focus mostly on the Routine Uses proposed for the new system of records and on other technical deficiencies of the proposal. The WPF has not evaluated and is not commenting in this letter on the legality of the underlying data collection or the justification for maintenance of information in the proposed new system of records.

I. DHS needs to reissue all DHS systems of records that predate the establishment of the Department

The publication of the proposed system of records only underscores existing confusion about the status of unrevised Department of Homeland Security (DHS) systems of records. DHS notes in its description of the proposed new system of records that the system was previously "covered by the Treasury Enforcement Communications System (TECS) 'system of records notice.' See 66 FR 52984, dated October 18, 2001." If DHS adopts the new system of records notice, then the existing notice for the TECS system becomes immediately out of date. We have not searched

exhaustively for a revised notice for the TECS system of records, but we would have expected that DHS (or perhaps the Treasury Department) would have proposed a revised TECS system of records notice concurrently with the proposal for the new system of records. The adoption of the new system of records notice puts some agency that we cannot precisely identify out of compliance with the Privacy Act of 1974 for the TECS system of records.

Of course, since the TECS system has not been republished since 2001, it is already substantially out of date because of changes in the structure of the Customs Service. DHS's continuing lack of compliance with basic Privacy Act of 1974 publication requirements is troubling. Our confusion about who "owns" the TECS system of records only underscores the immediate need for reissuance of all DHS systems of records that predate the establishment of the Department.

II. Routine Use A does not meet OMB standards and is inconsistent with Privacy Act requirements

Routine Use A would allow disclosure: "To appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where CBP believes the information would assist enforcement of civil or criminal laws or regulations."

The comparable Routine Use from the TECS system is narrower in a significant way. It would only allow disclosure *where the disclosing agency becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.* The proposed new Routine Use is both broader and more vague in that it would allow disclosures to merely assist enforcement of any law, civil or criminal. Nothing in the published notice explains or justifies the change in the scope of this routine use.

The Act requires that a Routine Use be "compatible with the purpose" for which the record was collected. It is impossible to determine that a disclosure that would assist virtually any law enforcement agency anywhere in the world to enforce any civil or criminal law meets this standard. The proposed Routine Use A allows disclosures that bear no relationship with the purpose of collection and is therefore overbroad and illegal. We recommend that the proposed Routine Use A be amended to return to the standard in the TECS system. Adopting this routine use as it is currently proposed will result in embarrassing litigation that the Department will lose, perhaps at significant expense to the government.

We suggest that someone at the Department review the existing OMB guidance that contains specific instructions on how to handle these disclosures. The original OMB Privacy Act Guidelines – still in force and still valid – state expressly that an agency can disclose information to a law enforcement agency on its own motion only "when a violation of law is suspected." 40 Federal Register, 28955 (July 9, 1975). The proposed Routine Use A does not meet the OMB standard and is not consistent with the Act's requirements. There is also case law that clearly restrains an agency's ability to disclose records for law enforcement, and the proposed Routine Use is not consistent with that case law.

III. Routine Use B does not comply with OMB guidance or current DOJ policy or practice

Routine Use B would allow disclosure: "To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations, or in response to a subpoena, or in connection with criminal proceedings."

Existing OMB guidance contains specific instructions on how to handle these disclosures. In particular, the May 24, 1985 guidance – available at <http://www.defenselink.mil/privacy/pdfdocs/PrivActGuidncUpdate_05241985.pdf> -- describes the proper way to deal with court and discovery disclosures. The currently proposed Routine Use B does not comply with OMB guidance or current Department of Justice policy and practice.

IV. Routine Use D is overbroad and unnecessary

Routine Use D would allow disclosure: "To an agency, organization, or individual for the purposes of performing audit or oversight operations as authorized by law; but only such information as is necessary and relevant to such audit or oversight function."

This Routine Use is so broad as to be meaningless. It would allow, for example, disclosure to any auditor of any agency, corporation, or institution anywhere in the world. The audit need bear no relationship to any activity or function of DHS. The audit need only be *authorized* by law rather than *required* by law. The disclosure need only be assessed in relation to the information's relevancy to the audit or oversight and not to the purpose for which the information was originally collected by DHS. If this Routine Use were limited to audit and oversight operations relevant to DHS or even other federal agencies, it would still be too broad to meet the compatibility requirement of the Act.

As written, Routine Use D authorizes disclosures that bear no relationship to the purpose of the system of records or any function of the federal government. If challenged, there is no chance that this Routine Use would be upheld by a judge. DHS can write a narrower Routine Use that addresses its core interest in auditing and oversight, if it needs one at all, since disclosures to the Department's Inspector General, to the Government Accountability Office, and to the Congress are authorized by the Act without a Routine Use.

V. Routine Use E contravenes the Privacy Act and is illegal

Routine Use E would allow disclosure: "To a Congressional office, for the record of an individual in response to an inquiry from that Congressional office made at the request of the individual to whom the record pertains."

The proposed Routine Use E would be greatly improved if it required that the request from the data subject to the congressional office be *in writing*. This change would protect the individual, the congressional office, and DHS.

VI. Routine Use G directly contravenes the Privacy Act and is illegal

Routine Use G would allow disclosure: "To an organization or individual in either the public or private sector, either foreign or domestic, where there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, to the extent the information is relevant to the protection of life or property and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure."

Section (b)(8) of the Privacy Act of 1974 authorizes disclosure in compelling circumstances affecting the health or safety of an individual, and it requires notice to be sent to the last known address of the subject of the record. The proposed Routine Use G *impermissibly duplicates and weakens the statutory condition of disclosure and omits the requirement for notice*. On those grounds, the routine use directly contravenes the Act and is illegal. We recommend that the routine use be dropped entirely.

VII. Routine Use J is unnecessary and overbroad

Routine Use J would allow disclosure: "To an appropriate Federal, state, local, tribal, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit and when disclosure is appropriate to the proper performance of the official duties of the person making the request."

There is no reason for this proposed Routine Use to cover hiring decisions, contract awards, or security clearance determinations. Disclosures for these purposes should be accomplished with the consent of the data subject. There may be some disclosures allowed by the Routine Use for which consent is not likely to be appropriate. The Routine Use should be narrowed to cover only those disclosures that are not beneficial to the data subject and for which the data subject might not give consent.

Further, we are at a loss to determine how DHS can possibly assess whether information is *necessary for* a decision by a requesting agency.

VIII. Routine Use K is either unnecessary and/or may even be too narrow

Routine Use K would allow disclosure: "To appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, for purposes of assisting such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or for combating other significant public health threats."

These disclosures are appropriate, but only in accordance with the standards and procedures in subsection (b)(8) of the Act covering compelling circumstance affecting health or safety. We also note that (b)(8) allows for disclosures to persons other than government agencies, and this broader range of possible disclosure may be entirely appropriate in the case of communicable diseases.We suggest that the Routine Use be dropped.

IX. Routine Use M is standardless and meaningless

Routine Use M would allow disclosure: "To appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, under the terms of a memorandum of understanding or agreement, where CBP is aware of a need to utilize relevant data for purposes of testing new technology and systems designed to enhance border security or identify other violations of law."

This proposed Routine Use is objectionable because there is no reason for the use of identifiable data about real persons in testing. Further, the standard is so vague as to be meaningless. CPB need only be *aware of a need* for the data.

The standard does not even call for any finding or determination by any accountable official at CPB. If a GS-2 employee reads a statement by an anonymous person on a blog on the Internet, that might be enough to meet the standard and allow a disclosure. We would prefer to see the Routine Use dropped altogether, but at a minimum a stronger standard would help considerably. For example, we suggest a standard like this: "Where an Assistant Secretary at CPB determines that there is a reasonable need to utilize…." It would also be appropriate for all disclosures under this Routine Use be contingent on guarantees for security of the data and on a complete prohibition on further use and disclosure.

X. Routine Use N needs to be significantly narrowed

Routine Use N would allow disclosure: "To appropriate agencies, entities, and persons when (1) It is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, harm to the security or integrity of this system or other systems or programs (whether maintained by CBP or another agency or entity), or harm to the individual that rely upon the compromised information; and (3) the disclosure is made to such agencies, entities, and persons who are reasonably necessary to assist in connection with the CBP's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm."

We are at a loss to understand why information in this system is so sensitive that it requires an exemption from the Privacy Act of 1974, yet the Department proposes to authorize the disclosure of all of the information in the system to virtually anyone in the world in the event of a security breach. We would much prefer a narrower routine use for this purpose. We filed extensive comments on a similar routine use proposed by the Department of Justice. Our comments can be

found at <http://www.worldprivacyforum.org/pdf/DOJ_RU_11172006fs.pdf>, and we incorporate those comments here by reference.

XI. Routine Use O is vague and entirely inappropriate

Routine Use O would allow disclosure: "To the news media and the public and as appropriate, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of or is necessary to demonstrate the accountability of officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy."

We repeat the previous comment. Why is this system exempt if it includes a Routine Use that allows the Department to release the entire database in a press release?

The standards in the Routine Use are a mess. The standard of *legitimate public interest* is too vague to meet the standard of the Act. The standards of *necessary to preserve confidence* and *necessary to demonstrate the accountability* are virtually impossible to meet. We would actually be happy if DHS kept those standards because they would provide useful grounds for any data subject who decided to litigate over a disclosure made under this proposed Routine Use.

We would object further, but the final clause swallows the entire Routine Use. The Department would surely refuse to disclose any identifiable element in the system if requested under the Freedom of Information Act on grounds of unwarranted invasion of personal privacy. Nothing that the Department would care to say in its own defense would overcome the privacy standard in the FOIA. However, if it disclosed personal information under the standard in the Routine Use, the Department would expose all the records to disclosure under the FOIA.

The transparent purpose of the Routine Use is to let the Department use any information in the system to defend itself if criticized. This is totally inappropriate. The presence of the Routine Use only serves to show the disingenuousness of the Department in seeking to reserve the right to override privacy interests to protect itself from criticism. If criticism could justify disclosure of Privacy Act records, then many of DHS's records would already be in the public domain. The Department can and does defend itself without disclosing the identifiable information of individual travelers. We suggest that the Department drop this Routine Use altogether.

XII. Conclusion

The overbroad, vague, and in some cases illegal Routine Uses included in this SORN are troubling, as is the lack of compliance with existing OMB guidance. We offer these comments respectfully, but we underscore our conclusion that some of the Routine Uses are legally unacceptable and seemingly drafted without regard to applicable standards and judicial findings. We urge the Department to thoroughly reassess the Routine Uses discussed in these comments.

Thank you for the opportunity to offer comments.

Respectfully submitted,

Pam Dixon
World Privacy Forum

www.worldprivacyforum.org
760-436-2489