CENTER FOR DEMOCRACY & TECHNOLOGY
Keeping the Internet Open, Innovative and Free

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

August 25, 2008

Mr. Hugo Teufel, III
Chief Privacy Officer
Department of Homeland Security
Washington, D.C. 20528

Re: Comments on Border Crossing Information System of Records Notice 73 Fed. Reg. 43457 Docket No. DHS-2007-0040

Via: www.regulations.gov

Dear Mr. Teufel:

On July 25, 2008, the Department of Homeland Security (DHS) and U.S. Customs and Border Protection (CBP) printed a notice in the Federal Register (BCI SORN) announcing the establishment of a distinct system of records, a Border Crossing Information (BCI) database. 73 Fed. Reg. 43457. The Center for Democracy & Technology submits these brief comments to urge the Department of Homeland Security to limit the period for which border crossing information is held and to limit the "routine uses" to which that data can be put. We are also separately submitting comments on the companion Non-Federal Entity Data System (NEDS) system of records notice [73 Fed. Reg. 43462, Docket No. DHS-2007-0016] and those comments are attached here as an Appendix.[1]

The BCI SORN indicates that a record of the time, place and date of every entry into the United States, along with the name, date of birth, gender, photograph (where available), and country of citizenship of every person making an entry, including Americans returning to their own country, will be maintained in the BCI database. The

[1] The *Washington Post* recently reported on these two SORNs. *See* Ellen Nakashima, "Citizens' U.S. Border Crossings Tracked; Data From Checkpoints To Be Kept for 15 Years" (Aug. 20, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/08/19/AR2008081902811_pf.html.

database will also include a record, where appropriate, that the individual making the entry aroused the suspicion of border officials and was referred for secondary inspection. Where CBP is able to secure departure records, those, too will be maintained in the BCI database, and will include the date, time and place of the departure, and the biographical information set forth above that identifies the person making the departure. The BCI SORN indicates that the data, when it pertains to a citizen or lawful permanent resident of the United States, will be maintained for 15 years. Records pertaining to non-immigrants (primarily visitors and asylum seekers who are foreign nationals) will be maintained for 75 years.

* **Vast Scope of Data Collection.** For the first time, the United States government will maintain comprehensive records for 15 years of the date, time and place every American enters the country. Previously, as a practical matter, records could be maintained only of entries made by air, and later sea entries as well. However, approximately 75% of entries are made at the land borders.[2] Until recently, and for most of those entries made by a U.S. citizen, no record of entry was made: the citizen showed his or her driver's license as proof of identity, orally declared his or her U.S. citizenship, and was often allowed to enter the country on that basis. The advent of new, machine-readable and RFID-enabled passports, passport cards, and "Enhanced Drivers Licenses" ("EDLs) issued by states and other entities will make collection of land border entry information practical.[3]

* **Absence of a Specific Statutory Mandate Counsels Caution.** The BCI SORN cites as authority to establish the BCI database a series of statutes, none of which specifically authorizes the creation of the BCI database. Instead, the statutes establish regimes for issuing travel documents, screening air passengers and for other border enforcement activities. Congress never directed DHS to establish a database to track every American's entry into the U.S. The DHS assertion that the statutes provide legal authority is at best a broad interpretation of the authority that is specifically provided in these statutes. In view of the absence of a mandate from Congress to establish the database in question, DHS should be careful to ensure that it collects in the data base only the data necessary to its core mission, holds it only as long as is necessary, and uses it for carefully defined and specifically limited purposes. The current BCI SORN does not describe such a circumscribed model for the BCI database.

* **Assessing Admissibility and Threat, as Opposed To Tracking.** Some data must be collected at the border to determine whether the person seeking entry is admissible and whether the person poses a security threat. For example, terrorists are properly inadmissible to the United States; in order to determine whether a terrorist is

---

[2] The Government Accountability Office reported that for fiscal year 2005, 74% of border crossings occurred at land ports of entry. GAO-08-219, *Border Security: Despite Progress, Weakness in Traveler Inspections Exist at Our Nation's Ports of Entry,* (November 2007) at pp. 11-12. http://www.gao.gov/new.items/d08219.pdf.

[3] *See* Appendix for more information about EDLs and the treatment of data supporting them. Currently, CBP officials must sometimes manually input data for some entries at the land border. This is impractical for any substantial volume of entries.

seeking admission, it is necessary to collect some biographical information and compare it to watch list entries. Americans entering the U.S. expect that this information will be collected for this purpose. What many do not expect, though, is that personal information, including border crossing history, will be saved for 15 years and that it can be used down the road for any law enforcement or intelligence purpose that presents itself. There is no effort to retain only the data of people with respect to whom there is some level of suspicion – rather, the information about the date, time and place of every American's entry is stored. This makes the system more akin to a tracking mechanism than to an effort enforce entry requirements at the border, or for targeted law enforcement purposes for which border crossing data would be uniquely suited. We urge DHS to re-focus the BCI SORN on protecting the border rather than on tracking Americans who cross it.

* **Excessive Data Retention Period.** The 15-year period for which border crossing data pertaining to Americans would be maintained is excessive.[4] It cannot be justified as necessary for determining whether the record subject is admissible or is dangerous or is the subject of an outstanding criminal warrant. Such screening activities can be conducted with much more limited retention periods. The law enforcement and counterterrorism purposes for which border crossing data would be collected and retained are not delineated in the BCI SORN. As a result, the 15-year period of retention is not sufficiently justified in the BCI SORN. DHS should assess the efficacy of retaining border crossing information for such a lengthy period of time. How often has 15-year old entry data been essential to a law enforcement investigation? Was the information reasonably available from other sources so that it could be provided on a more targeted basis? We are hopeful that such an assessment, based on past experience, would lead to a conclusion that a substantially shorter retention period is appropriate.

* **Overbroad "Routine Uses."** The Privacy Act permits a federal agency that collects information to share the information with other agencies for "routine uses" the agency identifies in the System of Records Notice. Routine use must be looked at in light of the retention period of the data: if data is to be retained for a short time, the breadth of the routine uses claimed is less problematic because the data will not be available for disclosure after the retention period has ended. However, the BCI SORN would establish a lengthy retention period. It also states very broad routine uses that DHS should reassess and narrow, focusing on uses related to assessing admissibility and risk at the border, and not on uses that tend toward establishing a tracking system. We urge DHS to reassess the routine uses claimed, eliminate those that can be eliminated and restrict the breadth of some of those that remain. Concerns and recommendations about specific routine uses, and about particularly sensitive border crossing data, follow.

* **Law Enforcement Routine Use Should Be Limited as In TECS and Should Exclude Data Mining.** The first routine use mentioned in the BCI SORN would permit

[4] A lengthy period of retention for data pertaining to non-immigrants may be justifiable based on the need to assess eligibility for immigration benefits years after an entry was made. CDT expresses no view as to whether the 75-year period for which border crossing data pertaining to non-immigrants is to be retained is excessive.

biographical and entry data to be shared with "Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting 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." In contrast, the corresponding routine use for the Treasury Enforcement Communications System ("TECS") system of records[5] – which, according to the BCI SORN, governed disclosure of border crossing information until the BCI SORN became effective today – permitted disclosure only when DHS became aware of an indication of a violation or potential violation of a civil or criminal law or regulation. The BCI SORN permits disclosure based on the *mere belief* that disclosure would assist with enforcement, rather than requiring an indication that there has been or potentially will be a violation. This much broader formulation is not warranted or explained by anything in the BCI SORN. The BCI SORN also permits disclosure for uses that are not "compatible with the purpose" for which the information was gathered, and this is inconsistent with the routine use requirements of the Privacy Act. We urge that the BCI SORN adopt the TECS formulation. In addition, the Privacy Impact Assessment governing this collection of information indicates that the entry data will not be used for one law enforcement purpose – pattern-based data mining.[6] At a minimum, and for this restriction to have teeth, data mining should be specifically excepted from the law enforcement routine uses authorized in the BCI SORN.

* **Hiring and Contracting Routine Use Should Be Limited.** The BCI SORN allows disclosure of biographical and entry data for use in hiring, firing, contracting, and security clearance decisions made by governmental entities. It even permits disclosure of border crossing information about Americans to foreign governments to assist them in making such decisions. Most such disclosures should be made only with the consent of the person to whom the information pertains, and consent could easily be obtained when the person applies for the job or bids on the contract. Non-consensual disclosure of border crossing information for these purposes should be more narrowly described in this routine use.

* **Disclosure of Border Crossing Information To the Media.** The SORN permits disclosure of biographical and entry information in the BCI database to the media and to the public "when there exists a legitimate public interest in the disclosure of the information," except where disclosure would constitute an unwarranted invasion of personal privacy. While there may be circumstances in which disclosure to the media and to the public of border crossing information about an individual would be appropriate, the expansive language in the BCI SORN does not describe them. The "legitimate public interest" test is virtually meaningless; it provides little guidance as to the circumstances in which border crossing information will be broadly disseminated.

* **Limiting Dissemination of Secondary Inspection Records.** The routine use limitations treat all data in the BCI database equally, regardless of the sensitivity of the

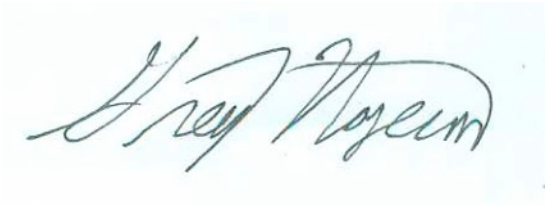
[5] 66 Fed. Reg. 52984, 53029 (October 18, 2001)

[6] *Privacy Impact Assessment for CBP Procedures for Processing Travel Documents at the Border* (July 2, 2008) http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_borderops.pdf, at p.12.

data. Secondary inspection data should be treated differently because it is more sensitive. A person is usually referred for secondary inspection when border officials believe the person is an inadmissible alien or is an American who has committed or may be committing a crime. Release of this information can cast a cloud on a person who has done nothing wrong. We urge DHS to carefully review the routine uses it has claimed for border crossing information with an eye toward further limiting disclosure of a person's secondary inspection status.

Thank you for the opportunity to submit these brief comments on the BCI SORN. Please feel free to contact me (gnojeim@cdt.org) if you have any questions about these comments.

Sincerely,



Gregory T. Nojeim
Senior Counsel and
Director, Project on Freedom, Security & Technology

Appendix Attached: CDT Comments of August 25, 2008 on Non-Federal Entity Data System SORN.