AILA National Office
Suite 300
1331 G Street, NW
Washington, DC 20005

Tel: 202.507.5600
Fax: 202.783.7853

www.aila.org

Jeanne A. Butterfield
*Executive Director*

Susan D. Quarles
*Deputy Director, Finance & Administration*

Crystal Williams
*Deputy Director, Programs*

August 25, 2008

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

***Re: Comments on the Department of Homeland Security ("DHS") Docket No. 2008-0024;"Privacy Act of 1974: Implementation of Exemptions; Border Crossing Information" ("BCI"), (73 Fed. Reg. 43374 (July 25, 2008)***

Dear Mr. Teufel:

The American Immigration Lawyers Association ("AILA") submits the following in response to the request for public comment by the DHS Privacy Office on the proposed rule ("Proposed Rule" or "Proposed Regulation") amending Chapter I of Title 6, Part 5 of the Code of Federal Regulations ("CFR") to add at the end of Appendix C to Part 5 regarding exemptions from the Privacy Act an exemption regarding BCI, 73 Fed. Reg., No. 144, pages 43374-43375 (July 25, 2008).

AILA is a voluntary bar association of more than 11,000 attorneys and law professors practicing, researching, and teaching in the field of immigration and nationality law. The organization has been in existence since 1946 and is affiliated with the American Bar Association. Our mission includes the advancement of the law pertaining to immigration and nationality and the facilitation of justice in the field. We appreciate the opportunity to comment on the proposed rule and believe that our members' collective expertise provides experience that makes us particularly well-qualified to offer views that we believe will benefit the public and the government. AILA members regularly advise and represent businesses, U.S. citizens, U.S. lawful permanent residents, and foreign nationals regarding the application and interpretation of U.S. immigration laws.

AILA is concerned with the proposed rule's exemption of BCI information from the Privacy Act for two main reasons. First, the rule mischaracterizes information in the BCI as purely law enforcement information. While some information may constitute law enforcement information, the rule broadly

paints all BCI data as law enforcement data and thus exempt from Privacy Act protection. Importantly, the characterization of BCI's information as solely law enforcement is in conflict with prior characterizations of the same data in connection with WHTI. Moreover, the proposed rule departs from the practice under BCI's predecessor SOR, BCIS, which did not characterize this information as law enforcement and thus, affords Privacy Act protection to this information. AILA recommends a more narrowly tailored case-by-case approach to designation of BCI information as law enforcement information exempt from the Privacy Act.

Second, exempting BCI information from the Privacy Act renders far more difficult, if not impossible, the ability of individuals to contest and fix errors that show up in the database. There are many examples of errors in the multiple databases that BCI relies on and connects to. Due to massive interconnectivity of databases, the potential for unresolved errors and the absence of adequate mechanisms for redress and correction impose extreme burdens on individuals.

The Proposed Rule is fundamentally misleading to the public regarding its impact. The BCI Privacy Act exemption notice should be republished to the public with a thorough and detailed description of its potential impact upon those who will have data entered into this system.

1. **The Rule mischaracterizes BCI information as law enforcement information.**

The proposed rule's exemption broadly mischaracterizes all admission or departure records as data gathered and maintained in connection with a principal criminal law enforcement function. The proposed rule does not recognize that this data is not collected principally for criminal law enforcement purposes.

The proposed rule does not exempt biographic or travel information submitted by, and collected from, a person's travel documents or submitted from a government computer system to support or to validate those travel documents. The traveler is only assured that data access will be available to confirm data already possessed by the traveler. AILA has strong concerns that all other data collected in BCI will be restricted from disclosure under the Privacy Act.

The implications of Privacy Act exemptions regarding the BCI are far-reaching and include data regarding U.S. citizens, domestic travel, visa applications filed with DOS, passport applications, immigration benefit applications filed with U.S. Citizenship and Immigration Services ("USCIS"), applications for admission to the U.S. through U.S. Customs and Border Protection ("CBP"), eligibility for trusted travel programs, and exposure to enforcement actions by U.S. Immigration and Customs Enforcement ("ICE") and other law enforcement entities.

The simple BCI exemption proposal manages to reverse any attempt at transparency regarding exit/entry data by now characterizing such data as law-enforcement related.

2. **Exempting BCI information from the Privacy Act impedes an individual's ability to redress errors that are present in BCI and other integrated databases.**

The labyrinth of databases that BCI will rely on for making admissions decisions and propagating information in its fields is riddled with errors. Exempting BCI from coverage under the Privacy Act will

impede efforts to correct errors in the multiple databases that BCI accesses. Moreover, exempting BCI information from the Privacy Act will impede individuals and their attorneys from learning of the reasoning and factual basis for decisions made at the border.[1]

To fully understand the impact that the BCI proposed Privacy Act exemption it is important to consider it in the context of the increase in the interconnectivity of immigration and criminal databases, the difficulty of database correction, database errors, and the lack of transparency provided to those subject to database related hits. The evolution of US-VISIT provides an illustrative example of this impact. US-VISIT owes its creation to the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 ("IIRIRA"), which mandated the Attorney General to develop an automated system to record the arrival and departure of every foreign national from the U.S.

As noted in the February 2008 U.S. Government Accountability Office report entitled, "Homeland Security – Strategic Solution for US-VISIT Program Needs to Better Defined, Justified, and Coordinated," DHS planned to deliver US VISIT in four increments:

- Increment 1 – (air and sea entry)
- Increment 2 – (air, sea, and land entry)
- Increment 3 – (land entry)
- Increment 4 – (a more strategic solution).

The key systems supporting or connected to US VISIT are:

- IDENT, which collects and stores biometric data about foreign visitors, including information from the FBI; ICE concerning deported felons and sexual registrants; and DHS on previous criminal histories and previous IDENT entries.

- IAFIS, which is the FBI's automated 10-fingerprint matching system and is electronically connected to all 50 states, as well as some federal agencies.

- Arrival Departure Information System ("ADIS"), which stores noncitizen traveler arrival and departure data from air and sea carrier manifests and provides query and reporting functions. ADIS matches entry, immigration status updates, and departure data to provide immigration status, including whether the individual overstayed his/her authorized period of stay.

[1] Lack of access to the agency's factual basis and reasoning for adjudications made at the border raises concerns under the Administrative Procedures Act. Generally, the APA mandates that an agency must provide a reasoned decision and provide a factual basis for all adjudications. Decisions made by CBP officers regarding admissibility, which will be included in the BCI database, are adjudications under the APA and thus require a reasoned decision based on facts that are disclosed to an individual. Moreover, at a minimum, at the time of adjudication the APA mandates that an individual receive a reasoned decision based on facts of the case. The proposed rule's exemption of BCI information from the Privacy Act blocks an individual from obtaining a reasoned decision based on facts and thus raises concerns under the APA.

The APA mandates reasoned decisions based on facts of a case to ensure that agencies are held accountable for their decisions. The Proposed Rule cloaks information regarding adjudications at the border that is included in BCI, as criminal investigation data and thus shields the agency from having to substantiate its adjudications. The exemption in the proposed rule frustrates the APA and impedes individual's opportunity to address errors that may be made in adjudication or in input of data to the database.

- Student and Exchange Visitor Information System ("SEVIS"), which contains data on changes of status throughout a foreign student's or exchange visitor's stay in the US.

- Computer Linked Application Information Management System ("CLAIMS 3"), which includes adjudication results on foreign nationals who request immigration benefits such as change of status, extension of stay, or adjustment to permanent resident status.

- TECS which maintains lookout/watch list data, interfaces with other agencies' databases, and is currently used by inspectors at ports of entry to verify traveler information and update traveler data. TECS also includes the Interagency Border Inspection Service ("IBIS") biographic data service, which serves as a centralized, shared database of well over 10 million subject records. CBP officers also have access to the National Crime Information Center ("NCIC") database established by the Department of Justice as a service to all criminal justice agencies, as well as federal, state, and local users; as well as the National Law Enforcement Telecommunications System ("NLETS") which allows queries on state criminal history, vehicle registration, driver's license information, and administration messages. In addition, the Automated Targeting System ("ATS") – Passenger, used at all U.S. airports and seaports receiving all international flights and voyages is used by CBP. [2]

- Advance Passenger Information System (APIS), which captures arrival and departure manifest information provided by air and sea carriers.

- Consular Consolidated Database ("CCD"), which is maintained by the DOS and includes information on visa applicants.

- Image Storage and Retrieval System ("ISRS"), which stores USCIS biometrics data, including the photo and fingerprints of individuals who have been issued a document by USCIS.

- USCIS Enterprise Service Bus ("ESB"), which provides network connectivity in support of the USCIS "Inter-Country Adoption" program.

- The Global Enrollment System ("GES"), which supports CBP programs for expedited processing of pre-approved, international, and low-risk travelers who voluntarily exchange information in return for expedited transit at U.S. borders (e.g. Nexus and Sentri).

- The U.S. Coast Guard's ("USCG") Mona Pass Proof-of-Concept, which tests the feasibility of deploying mobile biometrics identification capability to a Coast Guard cutter in the Mona Passage.[3]

[2] Information Security – Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US-VISIT Program, GAO-07-870 at p. 9.
[3] *Id. at 9-10.*

US VISIT has been criticized by the GAO for its inadequate controls placing data at an increased risk of unauthorized disclosure, use, modification, or destruction, possibly without detection.[4] The GAO has also noted that:

> These risks are not confined to US VISIT information. The CBP mainframe and network resources that support US VISIT also support other programs and systems. As a result, the vulnerabilities identified in this report could expose the information and information systems of the other programs to the same increased risks.[5]

Without a truly centralized point within DHS to address any data error potentially accessed through the BCI, the traveling public will be continually facing multiple hurdles to remove erroneous data.[6]

Thus, based on the integrated nature of the US-VISIT supporting or interconnected databases, it is simple to anticipate that the veil of exemption will be used frequently and often erroneously to shield data from review behind the auspices of a law enforcement "hit" or "investigative interest" claim. Such shielding does not improve security when the database's accuracy is not properly protected from tampering and its content is already documented as being frequently erroneous. BCI's content should be reviewed as a part of the database information accessed through US-VISIT supporting databases, not in a vacuum.

From an airport traveler perspective, the GAO noted in a May 2007 report that:

> It is important that CBP completes reports that fully describe the agency's use and protection of personal data during the international passenger prescreening process to ensure that it is complying with all applicable privacy laws. CBP's current disclosures do not fully inform the public about all of its systems for prescreening aviation passenger information nor do they explain how CBP combines data in the prescreening process, as required by law. As a result, passengers are not assured that their privacy is protected during the international passenger prescreening process. [7]

In an October 2006 report, the Electronic Privacy Information Center noted that in 2005, the director of the Transportation Security Administration's redress office revealed that more than 30,000 people who are not terrorists asked the TSA to remove their names from lists since September 11, 2001. In addition, according to the DHS PIA for the Automated Targeting System ("ATS") published on November 12, 2006, DHS stated that there is no procedure to correct the risk assessment and associated rules stored in ATS.[8] Thus, the only way a traveler may know of a problem in the ATS would be if he or she is subjected to additional scrutiny or is detained, or arrested, or refused admission. Of course,

---

[4] *See supra at 25-26.*
[5] *Id.* at 25.
[6] More detailed information regarding USCIS foreign national security checks is included in the DHS Office of Inspector General ("OIG") report entitled, "A Review of U.S. Citizenship and Immigration Services' Alien Security Checks" dated November of 2005, which outlined the various IBIS and FBI related checks implicated in the USCIS system of review.
[7] Aviation Security – *Efforts to Strengthen International Passenger Prescreening are Under Way, but Planning and Implementation Issues Remain, GAO 07-346 at p. 25.*
[8] DHS Privacy Impact Assessment, *Automated Targeting System,* Nov. 12, 2006 at p. 19.

now under the Electronic System for Travel Authorization ("ESTA") program, the Visa Waiver Program participant could be notified via a denial of registration prior to the date of travel. [9]

**3. This rule should be evaluated by the OMB.**

DHS notes that this rule is not a "significant regulatory action" under Executive Order 12866 and notes that the rule has not been reviewed by the Office of Management and Budget ("OMB") based on DHS's pronouncement. This rule should be evaluated by the OMB. DHS claims that this rulemaking will not constitute a barrier to international trade. The exemption from the privacy act requested for the BCI by this proposed rule could indeed implicate thousands of cross border and international travelers, including U.S. citizens and legal permanent residents, due to the identified privacy protections for CBP-related data discussed in this comment and the high percentage of errors contained in US-VISIT related databases.

According to the Data Management Improvement Act ("DMIA") Task Force, Second Annual Report to Congress 2003, in fiscal year 2002, there were approximately 448 million inspections conducted by CBP, with about 358 million attributed to land border crossings.[10] In the February 2005 DHS OIG report regarding the implementation of US VISIT at land borders, 33.7 percent of land border admissions related to U.S. citizens and 20.9 percent were U.S. legal permanent residents.[11] On June 1, 2009, U.S. citizens will be required to submit a U.S. passport, U.S. passport card, or other WHTI-compliant document to enter the U.S., and at the same time, will be subject to review under the large scale databases supported or connected with US-VISIT. Denials of participation in frequent traveler programs by DHS under the "zero tolerance" policy already cost the traveling public significant delays and inconvenience, without a corresponding benefit from security perspective. It is critical that the economic impact of decreased accuracy of border crossing information be reviewed. The inability to enter the U.S. for legitimate travel has real costs to the ability of business to be conducted.

DHS also alleges that there are no current or new information collection requirements associated with the proposed rule under the Paperwork Reduction Act. Yet, based on the connection of the BCI records with US-VISIT and with WHTI, BCI Privacy Act exemptions have the potential to implicate millions of additional applicants for admission to the U.S. In a vacuum, BCI may not impose additional requirements as to recording admissions to the U.S., but when placed in context with WHTI and the tracking capabilities of US VISIT, most certainly more information will be generated tied to any application for admission to the U.S. due to the interconnected labyrinth of databases created which impact the BCI. Thus, OMB should be consulted due to such impact on the public.

## Conclusion

The potential impact of the proposed Privacy Act exemption for the BCI could be devastating to the traveling public due to the public's inability to correct erroneous records protected by the cloak of a

---

[9] *See* http://www.cbp.gov/xp/cgov/travel/id_visa/esta/esta_faq.xml.

[10] Department of Homeland Security, DMIA Task Force, *Data Management Improvement Act (DMIA) Task Force Second Annual Report to Congress* (December 2003).

[11] DHS Office of Inspector General, *Implementation of United States Visitor and Immigrant Status Indicator Technology Program at Land Border Ports of Entry*, OIG-05-01 (February, 2004) *available at: http://www.globalsecurity.org/security/library/report/2005/OIG_05-11_Feb05.pdf*

"law enforcement" claim. Further, the proposed exemption improperly distorts all entry and exit related information as law enforcement related.

The precursor to the new BCI was the BCIS. BCIS was recognized as not being compiled for law enforcement purposes and hence was not exempted from the Privacy Act.[12] Enhancing the scope of the BCI to incorporate new databases, systems of records, or other information does not change the reason for the compilation of the data. The requested exemption should not be approved, and the BCI should be accorded the same treatment from a privacy perspective as its predecessor, the BCIS.

In addition, due to the continued enhancement of the interconnectivity of the data supporting and connecting with US-VISIT, it is imperative that the public be provided a centralized redress point for the correction of errors and other forms of redress. As it stands, an error in one of the systems can impact a U.S. citizen potentially during any request for entry to the U.S., or for that matter, any participation in the numerous frequent traveler programs promoted by the DHS for facilitation of travel. The interests of justice and due process are ill-served when correction of inaccurate records is not possible due to privacy exemptions. The current system of TRIP redress provided by CBP is inadequate and will be further diminished by increasing the protections of CBP records from review in the guise of a law enforcement protected claim.

Respectfully submitted,

AMERICAN IMMIGRATION LAWYERS ASSOCIATION

[12] DHS Privacy Impact Assessment, *Western Hemisphere Travel Initiative*, (August 11, 2006). *Available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_whti.pdf.*