9111-14

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS-2015-0075]

Privacy Act of 1974; Implementation of Exemptions; Department of Homeland Security, U.S. Customs and Border Protection – DHS/CBP-007 Border Crossing Information, System of Records

AGENCY: Department of Homeland Security, Privacy Office.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Department of Homeland Security is giving notice of proposed rulemaking pursuant to the Privacy Act of 1974 in connection with a current system of records titled "Department of Homeland Security/U.S. Customs and Border Protection-007 Border Crossing Information (BCI) System of Records." The exemptions for the system of records notice published May 28, 2013, continue to apply for the updated system of records for those categories of records listed in the previous System of Records Notice. This document proposes to exempt portions of certain new categories of records ingested from the Advance Passenger Information System (APIS) claimed for those records in that system pursuant to the United States Code.

DATES: Comments must be received on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number DHS-2015-0075 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: Karen L. Neuman, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

Instructions: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, please visit http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: John Connors, (202) 344-1610, Privacy Officer, U.S. Customs and Border Protection, Privacy and Diversity Office, 1300 Pennsylvania Avenue, N.W., Washington, DC 20229. For privacy questions, please contact: Karen L. Neuman, (202) 343-1717, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) is giving notice of a proposed rulemaking that DHS/CBP intends to update its regulations to exempt

portions of a system of records from certain provisions of the Privacy Act. Specifically, the Department proposes to exempt portions of the "DHS/CBP-007 Border Crossing Information System of Records" from one of more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. DHS reissued the current DHS/CBP-007 Border Crossing Information (BCI) System of Records in the Federal Register on May 11, 2015 (80 FR 26937), to provide notice to the public that DHS/CBP is updating the categories of records to include the capture of certain biometric information and Advance Passenger Information System (APIS) records at the border.

CBP's priority mission is to prevent terrorists and terrorist weapons from entering the country while facilitating legitimate travel and trade. To accomplish this mission, CBP maintains border crossing information about all individuals who enter, are admitted or paroled into, and (when available), exit from the United States regardless of method or conveyance. Border crossing information includes certain biographic and biometric information; photographs; certain mandatory or voluntary itinerary information provided by air, sea, bus, and rail carriers or any other forms of passenger transportation; and the time and location of the border crossing. Border crossing information resides on the TECS (not an acronym) information technology platform. DHS/CBP provided notice to the public about the update and expansion of the categories of records as part of DHS's ongoing effort to better reflect the categories of records in its collection of information. DHS/CBP published this updated system of records notice in the Federal Register on May 11, 2015 (80 FR 26937).

CBP is responsible for collecting and reviewing border crossing information from travelers entering and departing the United States as part of DHS/CBP's overall border security and enforcement missions. All individuals crossing the border are subject to CBP processing upon arrival in the United States. Each traveler entering the United States is required to establish his or her identity, nationality, and admissibility to the satisfaction of a CBP officer during the clearance process. To manage this process, CBP creates a record of an individual's admission or parole into the United States at a particular time and port of entry. CBP also collects information about U.S. citizens and certain aliens (in-scope travelers pursuant to 8 CFR 215.8, "requirements for biometric identifiers from aliens on departure from the United States") upon departure from the United States for law enforcement purposes and to document their border crossing.

DHS is statutorily mandated to create and integrate an automated entry and exit system that records the arrival and departure of aliens, verifies alien identities, and authenticates alien travel documents through the comparison of biometric identifiers (8 U.S.C. 1365(b)). Certain aliens may be required to provide biometrics (including digital fingerprint scans, palm prints, photographs, facial and iris images, or other biometric identifiers) upon arrival in or departure from the United States. The biometric data is stored on the Automated Biometric Identification System (IDENT) information technology platform. IDENT stores and processes biometric data (e.g., digital fingerprints, palm prints, photographs, and iris scans) and links biometrics with biographic information to establish and verify identities. The IDENT information

technology platform serves as the biometric repository for the Department, and also stores related biographic information.

Previously DHS established the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program to manage an automated entry and exit system. On March 16, 2013, US-VISIT's entry and exit operations (including deployment of a biometric exit system) were transferred to CBP through the Consolidated and Further Continuing Appropriations Act of 2013 (Pub. L. 113-6, H.R. 933). The Act also transferred US-VISIT's overstay analysis function to U.S. Immigration and Customs Enforcement (ICE) and US-VISIT's biometric identity management services to the Office of Biometric Identity Management (OBIM), within the DHS National Protection and Programs Directorate (NPPD). CBP assumed biometric entry and exit operations on April 1, 2013.

CBP has continued to develop mechanisms to collect biometric information from departing aliens since assuming responsibility for US-VISIT's entry and exit operations. During these operations, CBP officers may employ technology (e.g., wireless handheld devices or standalone kiosk) to collect biographic and biometric information from certain aliens determined to be in-scope pursuant to 8 CFR 215.8 "Requirements for biometric identifiers from aliens on departure from the United States" prior to exiting the United States. Biometrics are checked against the IDENT system's watchlist of known or suspected terrorists (KST), criminals, and immigration violators to help determine if a person is using an alias or attempting to use fraudulent identification. Biographic and biometric data is encrypted when it is collected and the data is transmitted in an

encrypted format to the IDENT system. The data is automatically deleted from the mobile device after the transmission is complete. The handheld mobile devices incorporate strict physical and procedural controls, such as Federal Information Processing Standard (FIPS)-compliant data encryption; residual information removal; and required authorization for users to sign-in using approved user account names and passwords.

Collection of additional biometric information from individuals crossing the border (such as information regarding scars, marks, tattoos, and palm prints) aids biometric sharing between the Department of Justice (DOJ) Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) and the IDENT system. The end result is enhanced access to (and in some cases acquisition of) IAFIS/NGI information by the IDENT system and its users. DHS, DOJ/FBI, and the Department of State (DOS)/Bureau of Consular Services entered into a Memorandum of Understanding (MOU) for Improved Information Sharing Services in 2008. The MOUs established the framework for sharing information in accordance with an agreed-upon technical solution for expanded IDENT/IAFIS/NGI interoperability, which provides access to additional data for a greater number of authorized users.

CBP collects border crossing information stored in this system of records through a number of sources, for example: (1) travel documents (e.g., a foreign passport) presented by an individual at a CBP port of entry when he or she provided no advance notice of the border crossing to CBP; (2) carriers that submit information in advance of travel through APIS; (3) information stored in the Global Enrollment System (GES) (see

DHS/CBP-002 Global Enrollment System (GES) SORN, 78 FR 3441, (January 16, 2013)) as part of a trusted or registered traveler program; (4) non-federal governmental authorities that issued valid travel documents approved by the Secretary of DHS (e.g., an Enhanced Driver's License (EDL)); (5) another federal agency that issued a valid travel document (e.g., data from a DOS visa, passport including passport card, or Border Crossing Card); or (6) the Canada Border Services Agency (CBSA) pursuant to the Beyond the Border Entry/Exit Program. When a traveler enters, is admitted to, paroled into, or departs from the United States, his or her biographical information, photograph (when available), and crossing details (time and location) is maintained in accordance with the DHS/CBP-007 Border Crossing Information SORN.

DHS/CBP updated the categories of records to provide notice that CBP is collecting biometrics such as digital fingerprints, photographs, and iris scans from certain non-U.S. citizens at the time of the border crossing or in support of their use of Global Entry or another trusted traveler program. In addition, CBP updated the categories of records in the SORN to provide notice that CBP plans to collect information regarding scars, marks, tattoos, and palm prints from individuals at the border to aid biometric interoperability between the IAFIS/NGI and the IDENT system. Finally, CBP updated the categories of records associated with APIS transmissions to better reflect the information collected and maintained in the DHS/CBP-007 BCI SORN.

Consistent with DHS's information sharing mission, information stored in the DHS/CBP-007 BCI SORN may be shared with other DHS components that have a need

to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions.

The exemptions for the system of records notice published May 28, 2013 (78 FR 31958) continue to apply for the updated system of records for those categories of records listed in the previous System of Records Notice. However, this document proposes to exempt portions of certain new categories of records ingested from APIS (see DHS/CBP-005 APIS SORN, 80 FR 13407 (March 13, 2015) claimed for those records in that system pursuant to 5 U.S.C. 552a(j)(2) and 5 U.S.C. 552a(k)(2). Furthermore, to the extent certain categories of records are ingested from other systems, the exemptions applicable to the source systems will remain in effect.

DHS is issuing this Notice of Proposed Rulemaking to exempt portions of DHS/CBP-007 Border Crossing Information System of Records from certain provisions of the Privacy Act.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which the Federal Government collects, maintains, uses, and disseminates individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. As a matter of policy, DHS extends

administrative Privacy Act protections to all individuals when systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

The Privacy Act allows government agencies to exempt certain records from the access and amendment provisions. If an agency claims an exemption, however, it must issue a Notice of Proposed Rulemaking to make clear to the public the reasons why a particular exemption is claimed.

DHS is claiming exemptions from certain requirements of the Privacy Act for portions of DHS/CBP-007 Border Crossing Information System of Records. Specifically, certain records ingested from the DHS/CBP-005 Advance Passenger Information System (APIS) SORN into the DHS/CBP-007 Border Crossing Information System of Records will continue to be covered by the exemptions claimed for those records in that system pursuant to 5 U.S.C. 552a(j)(2) and 5 U.S.C. 552a(k)(2). Information in DHS/CBP-007 Border Crossing Information System of Records relates to official DHS national security and law enforcement activities. These exemptions are needed to protect information relating to DHS law enforcement investigations from disclosure to subjects of investigations and others who could interfere with investigatory and law enforcement activities. Specifically, the exemptions are required to preclude subjects of these activities from frustrating the investigative process; to avoid disclosure of investigative techniques; protect the identities and physical safety of confidential informants and of law enforcement personnel; ensure DHS's and other federal agencies' ability to obtain information from third parties and other sources; protect the privacy of third parties; and safeguard sensitive information. Disclosure of information to the subject of the inquiry

could also permit the subject to avoid detection or apprehension.

In appropriate circumstances, when compliance would not appear to interfere with or adversely affect the law enforcement purposes of this system and the overall law enforcement process, the applicable exemptions may be waived on a case by case basis.

DHS will not assert any exemption with respect to information maintained in the system that is collected from a person at the time of crossing and submitted by that person's air, sea, bus, or rail carriers, if that person, or his or her agent, seeks access or amendment of such information. The DHS/CBP-007 Border Crossing Information System of Records Notice was published in the Federal Register on May 11, 2015.

List of Subjects in 6 CFR Part 5

Freedom of Information, Privacy.

For the reasons stated in the preamble, DHS proposes to amend chapter I of title 6, Code of Federal Regulations, as follows:

PART 5—DISCLOSURE OF RECORDS AND INFORMATION

1. The authority citation for part 5 continues to read as follows:

Authority: Pub. L. 107-296, 116 Stat. 2135; (6 U.S.C. 101 et seq.); 5 U.S.C. 301. Subpart A also issued under 5 U.S.C. 552. Subpart B also issued under 5 U.S.C. 552a.

2. In appendix C to part 5, revise paragraph 46 to read as follows:

Appendix C to Part 5—DHS Systems of Records Exempt From the Privacy Act

* * * * *

46. The DHS/CBP-007 Border Crossing Information System of Records consists of electronic and paper records and will be used by DHS and its components. The

DHS/CBP-007 Border Crossing Information System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; law enforcement, border security and intelligence activities. The DHS/CBP-007 Border Crossing Information System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies. At the time of border crossing and during the process of determining admissibility, CBP collects two types of data for which it claims different exemptions.

(a) CBP will not assert any exemption to limit an individual from accessing or amending his or her record with respect to information maintained in the system that is collected from a person at the time of crossing and submitted by that person's air, sea, bus, or rail carriers.

The Privacy Act requires DHS to maintain an accounting of the disclosures made pursuant to all routine uses. Pursuant to 5 U.S.C. 552a(j)(2), CBP will not disclose the fact that a law enforcement or intelligence agency has sought particular records because it may affect ongoing law enforcement activities. The Secretary of Homeland Security has exempted this system from sections (c)(3), (e)(8), and (g) of the Privacy Act of 1974, as amended, as is necessary and appropriate to protect this information. Further, DHS will claim exemption from section (c)(3)

of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(k)(2) as is necessary and appropriate to protect this information. Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(i) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(ii) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(iii) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

(b) Additionally, this system contains records or information recompiled from or created from information contained in other systems of records that are exempt from certain provisions of the Privacy Act. For these records or information only, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (c)(4); (d)(1)-(4); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5) and (e)(8); (f); and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2), has exempted this system from the following provisions of the Privacy Act, 5 U.S.C. 552a(c)(3); (d)(1)-(4); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(i) From subsection (c)(3) and (c)(4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire

investigative process.

(ii) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(iii) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(iv) From subsection (e)(2) (Collection of Information from Individuals)

because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(v) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(vi) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, potential witnesses, and confidential informants.

(vii) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant,

timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(viii) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(ix) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

* * * * *

Dated: December 10, 2015.

Karen L. Neuman,
Chief Privacy Officer,
Department of Homeland Security.
[FR Doc. 2015-31898 Filed: 12/21/2015 8:45 am; Publication Date: 12/22/2015]