9110-9B P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS-2017-0040]

Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/ALL-041 External Biometric Records (EBR) System of Records.

AGENCY: Privacy Office, DHS.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Department of Homeland Security (DHS) is giving concurrent notice of a new system of records pursuant to the Privacy Act of 1974 for the "Department of Homeland Security/ALL-041 External Biometric Records (EBR) System of Records" and this proposed rulemaking. In this proposed rulemaking, the Department proposes to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

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-2017-0040, 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**:** Philip S. Kaplan, 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 DHS-2017-0040. 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, go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general and privacy questions please contact: Philip S. Kaplan, privacy@hq.dhs.gov, (202-343-1717), Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background:

In accordance with the Privacy Act of 1974, 5 U.S.C. sec. 552a, DHS proposes a Privacy Act exemption for a new DHS system of records titled, "DHS/ALL-041 External Biometric Records (EBR) System of Records."

DHS has developed this system of records to receive, maintain, and disseminate biometric and associated biographic information from non-DHS entities (not already covered by a component system of records notices (SORNs)), both foreign and domestic, for the following purposes pursuant to formal or informal information sharing agreements or arrangements ("external information"), or with the express approval of the entity from which the Department received biometric and associated biographic information: law enforcement; national security; immigration screening; border enforcement; intelligence; national defense; and background investigations relating to

national security positions, credentialing, and certain positions of public trust, consistent with applicable DHS authorities.

In 2007, DHS published the Automated Biometric Identification System (IDENT) SORN. Since then, the Department's Privacy Act framework has evolved as the Department has matured and the complexity of the IDENT system increased. DHS Component SORNs now govern the function and use of the biometrics records collected by each component. However, the Department still requires a SORN to cover biometrics received from non-DHS entities. Therefore, DHS is establishing DHS/ALL-041 External Biometric Records (EBR) System of Records, which governs the maintenance and use of biometrics and associated biographic information received from non-DHS entities that are not covered by an existing Component SORNs. In addition, a forthcoming technical SORN will cover the limited information created by the IDENT system. Eventually, both this EBR SORN and the planned technical SORN will replace the IDENT SORN. In the meantime, to avoid any gap in SORN coverage for biometrics and associated biographic information, the EBR and IDENT SORNs will co-exist. After the technical SORN is published, DHS will rescind the IDENT SORN by publishing a *notice of rescindment* in the *Federal Register*.

External information is collected by non-DHS entities, including the Department of Defense (DoD), the Department of Justice (DOJ), State and local law enforcement authorities, or foreign governments. External information shared with DHS includes biometric (including latent fingerprints) and associated biographic information that may be used by DHS for the following purposes: law enforcement; national security; immigration screening; border enforcement; intelligence; national defense; and

background investigations relating to national security positions, credentialing, and certain positions of public trust, consistent with applicable DHS authorities.

DHS also maintains this information to support its information sharing agreements and arrangements with foreign partners to: prevent travelers from assuming different identities to fraudulently gain admission or immigration benefits; identify individuals who seek to enter the United States for unauthorized purposes; identify those who have committed serious crimes or violated immigration law; and enable informed decisions on visas, admissibility, or other immigration benefits. Such sharing augments the law enforcement and border control efforts of both the United States and its partners. Additionally, DHS is using this information in concert with external partners to facilitate the screening of refugees in an effort to combat terrorist travel consistent with DHS's and Components' authorities.

Consistent with DHS's mission, information covered by DHS/ALL-041 External Biometric Records may be shared with 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. In addition, DHS may share information with appropriate Federal, State, local, tribal, territorial, foreign, or international government agencies from the providing external entity, consistent with any applicable laws, rules, regulations, and information sharing and access agreements. DHS may share biometric and associated biographic information, as permitted pursuant to an applicable Privacy Act authorized disclosure, including routine uses set forth in this system of records notice.

DHS is issuing this Notice of Proposed Rulemaking to exempt this 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 Federal Government agencies collect, maintain, use, and disseminate personally identifiable information. 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 the 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. Additionally, the Judicial Redress Act (JRA) provides a statutory right to covered persons to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

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 DHS/ALL-041 External Biometric Records (EBR) System of Records, under 5 U.S.C. sec. 552a(j)(2), (k)(2), and (k)(5). Information in DHS/ALL-041 External Biometric Records (EBR) System of Records relates to official DHS law enforcement, national

security, immigration screening, border enforcement, intelligence, national defense, and background investigations relating to national security positions, credentialing, and certain positions of public trust, consistent with applicable DHS authorities. These exemptions are needed to protect information relating to DHS activities from disclosure to subjects or others related to these activities. Specifically, the exemptions are required to preclude subjects of these activities from frustrating these processes; to protect the identities and physical safety of confidential informants and law enforcement personnel; to ensure DHS's ability to obtain information from third parties and other sources; to protect the privacy of third parties; and to safeguard classified 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.

A notice of system of records for DHS/ALL-041 External Biometric Records (EBR) System of Records is also published in this issue of the *Federal Register*.

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 is revised to read as follows:

Authority: 6 U.S.C. 101 et seq.; Pub. L. 107-296, 116 Stat. 2135; 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. Amend Appendix to Part 5 by adding paragraph 78 to read as follows:

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

* * * * *

78. The DHS/ALL-041 External Biometric Records (EBR) System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/ALL-041 External Biometric Records (EBR) System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; and national security and intelligence activities. The DHS/ALL-041 External Biometric Records (EBR) 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.

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); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5), and (e)(8); (f); and (g)(1) through (5). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2) and (k)(5), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3); (d); and (e)(1), (e)(4)(G), (e)(4)(H); and (f). When a record received from another system has been exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are

claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here.

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:

(a) From subsection (c)(3) and (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.

(b) From subsection (d) (Access and Amendment 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, to tamper with witnesses or evidence, 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.

(c) 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.

(d) 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.

(e) 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.

(f) From subsections (e)(4)(G) and (e)(4)(H), (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, and potential witnesses, and confidential informants.

(g) 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.

(h) 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.

(i) From subsections (g)(1) through (5) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

Philip S. Kaplan
Chief Privacy Officer,
Department of Homeland Security.
[FR Doc. 2018-08454 Filed: 4/23/2018 8:45 am; Publication Date: 4/24/2018]