9110-9B

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS-2016-0025]

Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/ALL-030 Use of the Terrorist Screening Database System of Records

AGENCY: Privacy Office, Department of Homeland Security.

ACTION: Final Rule.

SUMMARY: The Department of Homeland Security (DHS) is issuing a final rule to amend its regulations to exempt portions of an existing system of records titled, "Department of Homeland Security/ALL-030 Use of the Terrorist Screening Database System of Records" from certain provisions of the Privacy Act. Specifically, the Department exempts portions of the "Department of Homeland Security/ALL-030 Use of the Terrorist Screening Database System of Records" from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: This final rule is effective [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER].

FOR FURTHER INFORMATION CONTACT: Karen L. Neuman, (202) 343-1717, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background:

The Department of Homeland Security (DHS) published a notice of proposed rulemaking in the Federal Register at 81 FR 3758, on January 22, 2016, 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. DHS issued the "Department of Homeland Security/ALL-030 Use of the Terrorist Screening Database System of Records" in the Federal Register at 81 FR 3811 on January 22, 2016, to provide notice to the public that DHS was adding two new consumers to the "DHS Watchlist Service." DHS also clarified an existing category of individuals, added two new categories of individuals, and clarified the categories of records maintained in this system. DHS invited comments on both the Notice of Proposed Rulemaking (NPRM) and System of Records Notice (SORN).

II. Public Comments:

DHS received three comments. Two comments were from private individuals who complemented DHS for this update. DHS received an identical comment from a public interest research center on the SORN and NPRM. The commenter raised concerns regarding the number of exemptions taken by DHS, particularly exemptions related to access and accounting for disclosures. Specifically, the commenter questioned the need to exempt records once an investigation was complete.

In response, DHS emphasizes that the Terrorist Screening Database (TSDB) belongs to the Department of Justice (DOJ)/Federal Bureau of Investigation (FBI). DHS does not change or alter these records. All records within the DHS/ALL-030 Use of the

Terrorist Screening Database System of Records are collected and disseminated by the DOJ/FBI and are covered by the DOJ/FBI-019, "Terrorist Screening Records Center System," 72 FR 77846 (Dec. 14, 2011). Because DHS does not make any changes to the records obtained from DOJ/FBI, the same exemptions outlined in the DOJ/FBI SORN, and reasons provided in its implementing regulations for use of such exemptions at 28 CFR 16.96, transfer and apply. For instance, disclosing this information to individuals who have been misidentified as known or suspected terrorists due to a close name similarity, and of which the investigation has been completed, could reveal the Government's investigative interest in a terrorist suspect for an ongoing investigation, because it could make known the name of the individual who actually is the subject of the Government's interest. Similarly, providing any type of notice to a misidentified known or suspected terrorist due to a close name similarity could alert the actual known or suspected terrorist of the Government's investigative interest in that individual. Further, amendment of these records would impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised. DHS is not taking any new exemptions as a result of the expansion to the categories of individuals in the TSDB. As noted in the NPRM, permitting access and amendment to watchlist records could disclose sensitive information that could be detrimental to national security. Release of the accounting of disclosures could reveal the details of watchlist matching measures, as well as capabilities and vulnerabilities of the watchlist matching process, the release of which could permit an individual to evade future detection and thereby impede efforts to ensure national security.

However, DHS does agree that some of the exemptions proposed in the NPRM are unnecessary. With the publication of this Final Rule, DHS is removing the exemption from subsections 5 U.S.C. 552a(e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because DHS has already established requirements, rules, or procedures with respect to individual access and will review each request for access on a case-by-case basis. Concurrent with this Final Rule, DHS is republishing the DHS/ALL-030 Use of the Terrorist Screening Database System of Records to reflect this change.

List of Subjects in 6 CFR Part 5

Freedom of information, Privacy.

For the reasons stated in the preamble, DHS amends 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 66 to read as follows:

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

* * * * *

66. The DHS/ALL-030 Use of the Terrorist Screening Database System of Records consists of electronic and paper records and will be used by DHS and its Components. The DHS/ALL-030 Use of the Terrorist Screening Database 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 thereunder; and national security and intelligence activities. The Terrorist Screening Database belongs to the Department of Justice (DOJ)/Federal Bureau of Investigation (FBI). DHS does not change or alter these records. All records within the DHS/ALL-030 Use of the Terrorist Screening Database System of Records are collected and disseminated by the DOJ/FBI and are covered by the DOJ/FBI-019, "Terrorist Screening Records Center System," 72 FR 77846 (Dec. 14, 2011). Because DHS does not make any changes to the records obtained from DOJ/FBI, the same exemptions outlined in the DOJ/FBI SORN, and reasons provided in its implementing regulations for use of such exemptions at 28 CFR 16.96, transfer and apply. 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)(5), (e)(8), and (g). When a record has been received from DOJ/FBI-019 Terrorist Screening Records System of Records and has been exempted in that source system, DHS will claim the same exemptions for those records that are claimed for that original primary system 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 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 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.

(g) 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.

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

* * * * *

Dated: March 22, 2016. .

Karen L. Neuman,
Chief Privacy Officer,
Department of Homeland Security.
[FR Doc. 2016-07896 Filed: 4/5/2016 8:45 am; Publication Date: 4/6/2016]