9110-9M

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS-2011-0100]

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, DHS.

ACTION: Final rule.

SUMMARY: The Department of Homeland Security is issuing a final rule to amend its regulations to exempt portions of a newly established 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.

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

FOR FURTHER INFORMATION CONTACT: For general questions and privacy issues please contact: Mary Ellen Callahan (703-235-0780), Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

Background

The Department of Homeland Security (DHS) published a notice of proposed rulemaking (NPRM) in the Federal Register, July 6, 2011, 76 FR 39315, proposing 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. The system of records is titled, "DHS/ALL – 030 Use of the Terrorist Screening Database System of Records." The DHS/ALL – 030 Use of the Terrorist Screening Database system of records notice (SORN) was published concurrently in the Federal Register, July 6, 2011, 76 FR 39408, and comments were invited on both the NPRM and SORN.

Public Comments

DHS received a total of two comments, one on the NPRM and one that addressed both the NPRM and the SORN.

Comments on the NPRM

DHS received two comments on the NPRM. One of the comments on the NPRM also included comments on the SORN. That comment will be addressed in its entirety under SORN below. The one comment exclusively on the NPRM was from a private individual. The individual raised a series of philosophical questions regarding the policy behind homeland security issues that were unrelated to this proposed rulemaking. The individual also mentioned several times that this is a "new database." This is not a new database. The system of records addressed by this NPRM and the accompanying SORN represents a mirror copy of the Department of Justice (DOJ)/Federal Bureau of

Investigation (FBI) – 019 Terrorist Screening Records System of Records (August 22, 2007, 72 FR 47073). The same rules outlined in the DOJ/FBI - 019 Terrorist Screening Records System of Records (August 22, 2007, 72 FR 47073) transfer and apply. The individual goes on to discuss the historical relevance of the Terrorist Screening Database and outlines the positives and negatives of the system. The individual also raises concerns about the security of the system. The DHS mirrored copy of the system will receive the same security and protection as it does at the FBI and Terrorist Screening Center (TSC). The individual also speculates that, as a matter of fiscal priority, the system could be subject to less funding over time based on priorities. The system will meet the same requirements at DHS as it does at FBI/TSC. The individual concludes the general comments by saying the benefits outweigh the risks. On Privacy Act exemptions, the individual states that the proposed rule was nicely drafted. The individual asks the question of who will make the determination on when an exemption will be applied. In response to that question, that determination will be made by DHS privacy or disclosure staff in consultation with counsel. If the exemption is applied and an appeal is necessary, individuals may appeal the decision. That process can be found at www.dhs.gov/foia. The individual expresses appreciation for the Department's decision to consider requests on a case-by-case basis when applying exemptions. The individual states that the system should be implemented and that it be a model for other agencies.

Comment on the SORN

DHS received one comment on the SORN from a public interest research center that was joined in filing its comments by seventeen other privacy, consumer rights, and civil rights organizations. The comment addressed both the NPRM and SORN jointly and

is addressed in this section. The authors start by stating that DHS should "suspend the proposal pending a full review of the privacy, security, and legal implications of the program, including compliance with the federal Privacy Act." The NPRM and SORN received internal coordination and clearance by program and compliance officials, including, but not limited to, the Office of General Counsel and the Chief Privacy Officer. The organizations further stated that "if the agency (DHS) proceeds with the Watch List System (WLS) program, the system must, at a minimum: 1) adhere to Congress's intent to maintain transparent and secure government recordkeeping systems; 2) provide individuals judicially enforceable rights of notice, access, and correction; 3) conform to a revised SORN and NPRM that includes requirements for the agency (DHS) to respect individuals' rights to control their information in possession of federal agencies, as the Privacy Act requires; and (4) premise its technological and security approach on decentralization." With respect to these points, the Department follows the complete privacy legal framework as well as additional privacy policy it has put in place. The organizations go on to state that the Department is intentionally circumventing a number of provisions under the Privacy Act as well as the intent of the Privacy Act. As noted above, the NPRM and SORN received internal coordination and clearance by program and compliance officials, including, but not limited to, the Office of General Counsel and the Chief Privacy Officer. This addresses the author's points covering "meaningful privacy protections Congress established in the Privacy Act." The fact that Privacy Act exemptions are taken within this system of records, and explained within the NPRM, does not mean that the act is illegal or outside of the intent of Congress. The exemptions are contemplated by the Privacy Act and the Department is implemented

them consistent with that statute. The Department maintains that, for a variety of national security and law enforcement purposes, the exemptions taken within the system of records, and outlined in the NRPM, are necessary and are unchanged. The organizations go on to refute the Privacy Act exemptions claimed and recommend changing the way the Department does business including the way it conducts investigations. The organizations recommend that the Department void the claimed exemptions. The Department maintains that, for national security and law enforcement purposes, the exemptions taken within the system of records, and outlined in the NRPM, are necessary and remain in place. The organizations also go on to cite concerns regarding privacy risks contemplated in previously published Privacy Impact Assessments (PIAs) where the Terrorist Screening Database (TSDB) is used. In response, the Department emphasizes that this is not a new database. This NPRM and SORN represent a mirror copy of the DOJ/FBI – 019 Terrorist Screening Records System of Records (August 22, 2007, 72 FR 47073). The same rules outlined in the FBI SORN transfer and apply. The Department has taken additional steps to further ensure privacy protections by conducting appropriate privacy analysis through a published PIA as well as SORN. Doing so provides additional transparency on the risks, mitigations, and privacy rules associated with maintaining a mirror copy of the TSDB.

After consideration of public comments and reviewing the NPRM, the Department determined it did not require exemptions to subsections (e)(12) or (h) of the Privacy Act. Thus, the Department has removed proposed paragraphs (i) and (k) from the Final Rule. No additional changes were made.

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: 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. Add at the end of Appendix C to Part 5, the following new paragraph "66":

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

* * * * *

66. The DHS/ALL – 030 Use of 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 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, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; national security and intelligence activities; and protection of the President of the U.S. or other individuals pursuant to Section 3056 and 3056A of Title 18. The DHS/ALL – 030 Use of Terrorist Screening Database 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. Pursuant to 5 U.S.C. 552a(j)(2), the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); (f); and (g)(1). Additionally, pursuant to 5 U.S.C. 552a(k)(1) and (k)(2), the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitation set forth in 5 U.S.C. 552a(c)(3); (d); (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:

(a) 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.

(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 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, 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 subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

Dated: November 23, 2011

Mary Ellen Callahan

Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2011-33428 Filed 12/28/2011 at 8:45 am; Publication Date: 12/29/2011]