9110-06

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS-2012-0020

Privacy Act of 1974: Implementation of Exemptions; Automated Targeting System

AGENCY: Privacy Office, DHS.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Department of Homeland Security is giving concurrent notice of a updated system of records pursuant to the Privacy Act of 1974 for the "Department of Homeland Security/ U.S. Customs and Border Protection - 006 - Automated Targeting System (ATS) System of Records" and this proposed rulemaking. The Department is publishing this Notice of Proposed Rulemaking to ensure that the exemptions previously published are clearly and appropriately applied to all records in the updated system of records.

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-2012-0020, by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 703-483-2999.

- Mail: Mary Ellen Callahan, 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 go to http://www.regulations.gov.

Instructions: All submissions received must include the agency name and docket number for this notice. 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 questions please contact: Laurence E. Castelli (202-325-0280), CBP Privacy Officer, Office of International Trade, U.S. Customs and Border Protection, Mint Annex, 799 Ninth Street, NW, Washington, D.C. 20229. For 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:

I. Background:

In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to update and expand an existing Department of Homeland Security

SORN titled, U.S. Customs and Border Protection, DHS/CBP-006 - Automated Targeting System (ATS) 72 FR 43650, August 6, 2007.

The SORN published elsewhere in the *Federal Register* is being updated and expanded to inform the public about changes to the Automated Targeting System (ATS) categories of individuals, categories of records, routine uses, access provisions, and sources of data. DHS/CBP is updating and expanding the categories of individuals, categories of records and sources of records stored in ATS because it has certain data that it must ingest for performance purposes. The Privacy Impact Assessment (PIA), which DHS will publish on its website (http://www.dhs.gov/privacy) concurrently with the publication of the SORN in the *Federal Register*, provides a full discussion of the functional capabilities of ATS and its modules. DHS and CBP have previously exempted portions of ATS from the access, amendment, and public accounting provisions of the Privacy Act because it is a law enforcement system. DHS and CBP, however, will consider each request for access to records maintained in ATS to determine whether or not information may be released. DHS and CBP further note that despite the exemption taken on this system of records they are providing access and amendment to passenger name records (PNR) collected by CBP pursuant to its statutory authority, 49 U.S.C. § 44909, as implemented by 19 CFR § 122.49d; Importer Security Filing (10+2 documentation) information; and any records that were ingested by ATS where the source system of records already provides access and/or amendment under the Privacy Act.

ATS provides the following basic functionalities to support the CBP officer in identifying individuals and cargo that need additional review across the different means or modes of travel to and from the United States:

- *Comparison:* ATS compares information on travelers and cargo coming into and going out of the country against law enforcement and intelligence databases to identify individuals and cargo requiring additional scrutiny. For example, ATS compares information on individuals (identified as passengers, travelers, crewmembers, or persons appearing on documents supporting the movement of cargo) trying to enter the country or trying to enter merchandise into the country against the Terrorist Screening Database (TSDB), which ATS ingests from the DHS Watchlist Service (WLS), and outstanding wants and warrants.
- *Rules:* ATS compares existing information on individuals and cargo entering and exiting the country with patterns identified as requiring additional scrutiny. The patterns are based on CBP officer experience, analysis of trends of suspicious activity, and raw intelligence corroborating those trends. For example, ATS might compare information on cargo entering the country against a set of scenario-based targeting rules that indicate a particular type of fish rarely is imported from a given country.
- *Federated Query:* ATS allows users to search data across many different databases and correlates it across the various systems to provide a person centric view of all data responsive to a query about the person's identity from the selected data bases.

In order to do the above, ATS pulls data from many different source systems. In some instances ATS is the official record for the information, while in other instances ATS ingests and maintains the information in order to improve the functionality of the system or provides a pointer to the information in the underlying system. Below is a summary:

- *Official Record:* ATS maintains the official record for Passenger Name Records (PNR) collected by CBP pursuant to its statutory authority, 49 U.S.C. § 44909, as implemented by 19 CFR § 122.49d; for Importer Security Filing (10+2 documentation) information, which provides advanced information about cargo and related persons and entities for risk assessment and targeting purposes; for results of Cargo Enforcement Exams; for the combination of license plate, Department of Motor Vehicle (DMV) registration data and biographical data associated with a border crossing; for law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source and/or classified information; and information obtained through memorandum of understanding or other arrangements because the information is relevant to the border security mission of the Department.
- *Ingestion of Data:* ATS maintains copies of key elements of certain CBP databases in order to minimize the processing time for searches on the operational systems and to act as a backup for certain operational systems, including, but not limited to: Automated Commercial Environment (ACE), Automated Commercial System (ACS), Automated Export System (AES),

Advance Passenger Information System (APIS), Border Crossing Information (BCI), Consular Electronic Application Center (CEAC), Enforcement Integrated Database (EID) [which includes the Enforcement Case Tracking System (ENFORCE)], Electronic System for Travel Authorization (ESTA), Global Enrollment System (GES), Non-Immigrant Information System (NIIS), historical National Security Entry-Exit Registration System (NSEERS), Seized Asset and Case Tracking System (SEACATS), U.S. Immigration and Customs Enforcement (ICE) Student Exchange and Visitor Information System (SEVIS), Social Security Administration (SSA) Master Death File, TECS, Terrorist Screening Database (TSDB) through the DHS Watchlist Service (WLS), and WebIDENT. If additional data is ingested and that additional data does not require amendment of the categories of individuals or categories of records in the SORN, the PIA for ATS will be updated to reflect that information. The updated PIA can be found at www.dhs.gov/privacy.

- *Pointer System:* ATS accesses and uses additional databases without ingesting the data, including, but not limited to: CBP Border Patrol Enforcement Tracking System (BPETS), Department of State Consular Consolidated Database (CCD), commercial data aggregators, CBP's Enterprise Geospatial Information Services (eGIS), DHS/USVISIT IDENT, National Law Enforcement Telecommunications System (Nlets), DOJ's National Crime Information Center (NCIC), the results of queries in the FBI's Interstate Identification Index (III), and the National Insurance Crime Bureau's

(NICB's) private database of stolen vehicles. If additional data is ingested and that additional data does not require amendment of the categories of individuals or categories of records in the SORN, the PIA for ATS will be updated to reflect that information. The updated PIA can be found at www.dhs.gov/privacy.

DHS/CBP has reorganized the ATS routine uses to provide greater uniformity across DHS systems. Consistent with DHS's information sharing mission, information stored in ATS may be shared with other DHS components, as well as appropriate Federal, State, local, tribal, foreign, or international government agencies. This sharing will only take place after DHS determines that the recipient has a need to know the information to carry out functions consistent with the routine uses set forth in the SORN.

DHS has exempted the system from the notification, access, amendment, and certain accounting provisions of the Privacy Act of 1974 because of the law enforcement nature of ATS. Despite the exemptions taken on this system of records, CBP and DHS are not exempting the following records from the access and amendment provisions of the Privacy Act: passenger name records (PNR) collected by CBP pursuant to its statutory authority, 49 U.S.C. § 44909, as implemented by 19 CFR § 122.49d; Importer Security Filing (10+2 documentation) information; and any records that were ingested by ATS where the source system of records already provides access and/or amendment under the Privacy Act. A traveler may obtain access to his or her PNR and request amendment as appropriate, but records concerning the targeting rules, the responses to rules, case events, law enforcement and/or intelligence data, reports, projects developed by CBP analysts that may include public source and/or classified information,

information obtained through memorandum of understanding or other arrangements because the information is relevant to the border security mission of the Department, or records exempted from access by the system from which ATS ingested or accessed the information, will not be accessible to the individual.

II. Privacy Act:

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which the U.S. Government collects, maintains, uses, and disseminates 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. As a matter of policy (*Privacy Policy Guidance Memorandum 2007-1*, most recently updated January 7, 2009), DHS extends administrative Privacy Act protections to all persons, regardless of citizenship, where systems of records maintains information on both U.S. citizens and lawful permanent residents, as well as visitors.

The Privacy Act allows government agencies to exempt systems of records from certain provisions of the Act. 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.

As such, DHS is continuing to claim exemptions from certain requirements of the Privacy Act for DHS/CBP-006 - Automated Targeting System (ATS) System of Records.

Some information in DHS/CBP-006 - Automated Targeting System (ATS) System of Records relates to official DHS national security, law enforcement, immigration, and intelligence activities. 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 avoid disclosure of activity techniques; to protect the identities and physical safety of confidential informants and law enforcement personnel; to ensure DHS' ability to obtain information from third parties and other sources; to protect the privacy of third parties; and to safeguard officially classified and/or controlled information. Disclosure of information to the subject of the inquiry could also permit the subject to avoid detection or apprehension.

The exemptions proposed here are standard law enforcement and national security exemptions exercised by a large number of federal law enforcement and intelligence agencies. In appropriate circumstances, where 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.

A notice of system of records for DHS/CBP-006 - Automated Targeting System (ATS) 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 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. Replace paragraph 45 at the end of Appendix C to Part 5, with the following:

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

* * * * *

45. The DHS/CBP-006 - Automated Targeting System (ATS) System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/CBP-006 - Automated Targeting System (ATS) 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. The DHS/CBP-006 - Automated Targeting System (ATS) 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 has exempted this system from certain provisions of the Privacy Act as follows:

- Pursuant to 5 U.S.C. § 552a (j)(2), the system is exempt from 5 U.S.C. § 552a (c)(3) and (c)(4), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g).

- Pursuant to 5 U.S.C. § 552a (j)(2), the system (except for passenger name records (PNR) collected by CBP pursuant to its statutory authority, 49 U.S.C. § 44909, as implemented by 19 CFR § 122.49d; Importer Security Filing (10+2 documentation) information; and any records that were ingested by ATS where the source system of records already provides access and/or amendment under the Privacy Act) is exempt from 5 U.S.C. § 552a (d)(1), (d)(2), (d)(3), and (d)(4).
- Pursuant to 5 U.S.C. § 552a (k)(1) and (k)(2), the system is exempt from 5 U.S.C. § 552a(c)(3); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f).
- Pursuant to 5 U.S.C. § 552a (k)(1) and (k)(2), the system (except for passenger name records (PNR) collected by CBP pursuant to its statutory authority, 49 U.S.C. § 44909, as implemented by 19 CFR § 122.49d; Importer Security Filing (10+2 documentation) information; and any records that were ingested by ATS where the source system of records already provides access and/or amendment under the Privacy Act) is exempt from (d)(1), (d)(2), (d)(3), and (d)(4).

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 classified and 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 Individuals) 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.

Mary Ellen Callahan

Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2012-12395 Filed 05/22/2012 at 8:45 am; Publication Date: 05/23/2012]