BILLING CODE 4410-10

PROPOSED RULES

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary; Privacy Office

Docket Number 2007-0043

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

AGENCY: Privacy Office, Office of the Secretary, DHS.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Department of Homeland Security is amending its regulations to exempt certain records from particular provisions of the Privacy Act. Specifically, the Department proposes to exempt certain records of the Automated Targeting System from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. This notice is a republication of the Treasury Department exemption regulation (title 31, Code of Federal Regulations, part 1) which previously covered the Automated Targeting System as part of the Treasury Enforcement Communications System.

DATES: Written comments must be submitted on or before [insert date ___ (30) days after publication in the FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by DOCKET NUMBER DHS-2007-0043 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 1-866-466-5370.

- Mail: Hugo Teufel III, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Laurence E. Castelli (202-572-8790), Chief, Privacy Act Policy and Procedures Branch, Bureau of Customs and Border Protection, Office of International Trade, Mint Annex, 1300 Pennsylvania Ave., NW, Washington, DC 20229. For privacy issues please contact: Hugo Teufel III (703-235-0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

Background

The Department of Homeland Security (DHS), elsewhere in this edition of the Federal Register, published a Privacy Act system of records notice describing records in the Automated Targeting System (ATS). ATS performs screening of both inbound and outbound cargo, travelers, and conveyances. As part of this screening function and to facilitate DHS's border enforcement mission, ATS compares information received with CBP's law enforcement databases, the Federal Bureau of Investigation Terrorist Screening Center's the Terrorist Screening Database (TSDB), information on outstanding wants or warrants, information from other government agencies regarding high-risk parties, and risk-based rules developed by analysts using law enforcement data, intelligence, and past case experience. The modules also facilitate analysis of the screening results of these comparisons.

ATS originally was designed as a rules-based program to identify such cargo; it did not apply to travelers. Today, ATS includes the following separate components: ATS-N, for screening inbound or imported cargo; ATS-AT, for outbound or exported

cargo; ATS-L, for screening private passenger vehicles crossing at land border ports of entry using license plate data; ATS-I, for cooperating with international customs partners in shared cargo screening and supply chain security; ATS-TAP, for assisting tactical units in identifying anomalous trade activity and performing trend analysis; and ATS-P, for screening travelers and conveyances entering the United States in the air, sea, and rail environments.

ATS-Passenger (ATS-P), one of six modules contained within ATS, maintains Passenger Name Record (PNR) data (data provided to airlines and travel agents by or on behalf of air passengers seeking to book travel) that has been collected by CBP as part of its border enforcement mission. ATS-P's screening relies upon information from the following databases: Treasury Enforcement Communications System (TECS), Advanced Passenger Information System (APIS), Non Immigrant Information System (NIIS), Suspect and Violator Indices (SAVI), and the Visa databases (maintained by the Department of State) with the PNR information that it maintains.

With respect to ATS-P module exempt records are the risk assessment analyses and business confidential information received in the PNR from the air and vessel carriers. No exemption shall be asserted regarding PNR data about the requester, obtained from either the requester or by a booking agent, brokers, or another person on the requester's behalf. This information, upon request, may be provided to the requester in the form in which it was collected from the respective carrier, but may not include certain business confidential information of the air carrier that is also contained in the record, such as use and application of frequent flier miles, internal annotations to the air fare, etc. For other ATS modules the only information maintained in ATS is the risk assessment analyses and a pointer to the data from the source system of records.

This system, however, may contain records or information recompiled from or created from information contained in other systems of records, which are exempt from certain provisions of the Privacy Act. For these records or information only, in accordance with 5 U.S.C. 552a (j)(2), and (k)(2), DHS will claims the following exemptions for these records or information from subsections (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (5), and (8); (f), and (g) of the Privacy Act of 1974, as amended, as necessary and appropriate to protect such information. Moreover, DHS will add these exemptions to Appendix C to 6 CFR Part 5, DHS Systems of Records Exempt from the Privacy Act. Such exempt records or information are law enforcement or national security investigation records, law enforcement activity and encounter records, or terrorist screening records.

DHS needs these exemptions in order to protect information relating to 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 investigations from frustrating the investigative process; avoid disclosure of investigative techniques; protect the identities and physical safety of confidential informants and of law enforcement personnel; ensure DHS' and other federal agencies' ability to obtain information from third parties and other sources; protect the privacy of third parties; and safeguard sensitive information.

Additionally, DHS needs these exemptions in order to protect information relating to law enforcement investigations from disclosure to subjects of such investigations and others who could interfere with investigatory activities. Specifically, the exemptions are required to: withhold information to the extent it identifies witnesses promised confidentiality as a condition of providing information during the course of the law

enforcement investigation; prevent subjects of such investigations from frustrating the investigative process; avoid disclosure of investigative techniques; protect the privacy of third parties; ensure DHS's and other federal agencies' ability to obtain information from third parties and other sources; and safeguard sensitive information.

The exemptions proposed here are standard law enforcement exemptions exercised by a large number of federal law enforcement agencies.

Nonetheless, DHS will examine each separate request on a case-by-case basis, and, after conferring with the appropriate component or agency, may waive applicable exemptions in appropriate circumstances and where it would not appear to interfere with or adversely affect the law enforcement purposes of the systems from which the information is recompiled or in which it is contained.

REGULATORY REQUIREMENTS

A. Regulatory Impact Analyses

Changes to Federal regulations must undergo several analyses. In conducting these analyses, DHS has determined:

1. Executive Order 12866 Assessment

This rule is not a significant regulatory action under Executive Order 12866, "Regulatory Planning and Review" (as amended). Accordingly, this rule has not been reviewed by the Office of Management and Budget (OMB). Nevertheless, DHS has reviewed this rulemaking, and concluded that there will not be any significant economic impact.

2. Regulatory Flexibility Act Assessment

Pursuant to section 605 of the Regulatory Flexibility Act (RFA), 5 U.S.C. 605(b), as amended by the Small Business Regulatory Enforcement and Fairness Act of 1996

(SBREFA), DHS certifies that this rule will not have a significant impact on a substantial number of small entities. The rule would impose no duties or obligations on small entities. Further, the exemptions to the Privacy Act apply to individuals, and individuals are not covered entities under the RFA.

3. International Trade Impact Assessment

This rulemaking will not constitute a barrier to international trade. The exemptions relate to criminal investigations and agency documentation and, therefore, do not create any new costs or barriers to trade.

4. Unfunded Mandates Assessment

Title II of the Unfunded Mandates Reform Act of 1995 (UMRA), (Pub. L. 104-4, 109 Stat. 48), requires Federal agencies to assess the effects of certain regulatory actions on State, local, and tribal governments, and the private sector. This rulemaking will not impose an unfunded mandate on State, local, or tribal governments, or on the private sector.

B. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501 et seq.) requires that DHS consider the impact of paperwork and other information collection burdens imposed on the public and, under the provisions of PRA section 3507(d), obtain approval from the Office of Management and Budget (OMB) for each collection of information it conducts, sponsors, or requires through regulations. DHS has determined that there are no current or new information collection requirements associated with this rule.

C. Executive Order 13132, Federalism

This action will not have a substantial direct effect on the States, on the relationship between the national Government and the States, or on the distribution of

power and responsibilities among the various levels of government, and therefore will not have federalism implications.

D. Environmental Analysis

DHS has reviewed this action for purposes of the National Environmental Policy Act of 1969 (NEPA) (42 U.S.C. 4321-4347) and has determined that this action will not have a significant effect on the human environment.

E. Energy Impact

The energy impact of this action has been assessed in accordance with the Energy Policy and Conservation Act (EPCA) Public Law 94-163, as amended (42 U.S.C. 6362). This rulemaking is not a major regulatory action under the provisions of the EPCA.

List of Subjects in 6 CFR Part 5

Sensitive information, Privacy, Freedom of information.

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.

2. At the end of Appendix C to Part 5, add the following new paragraph:

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

* * * * *

3. **DHS/CBP-006**, Automated Targeting System. Certain records or information in the following system of records are exempt from 5 U.S.C. 552a(c)(3) and (4); (d)(1),

(2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (e)(5), and (8); (f), and (g). With respect to the ATS-P module, exempt records are the risk assessment analyses and business confidential information received in the PNR from the air and vessel carriers. No exemption shall be asserted regarding PNR data about the requester, obtained from either the requester or by a booking agent, brokers, or another person on the requester's behalf. This information, upon request, may be provided to the requester in the form in which it was collected from the respective carrier, but may not include certain business confidential information of the air carrier that is also contained in the record. , such as use and application of frequent flier miles, internal annotations to the air fare, etc. For other ATS modules the only information maintained in ATS is the risk assessment analyses and a pointer to the data from the source system of records.

These exemptions also apply to the extent that information in this system of records is recompiled or is created from information contained in other systems of records subject to such exemptions pursuant to 5 U.S.C. 552a(j)(2),and (k)(2). After conferring with the appropriate component or agency, DHS may waive applicable exemptions in appropriate circumstances and where it would not appear to interfere with or adversely affect the law enforcement purposes of the systems from which the information is recompiled or in which it is contained.

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) (Accounting for Disclosure) because making available to a record subject the accounting of disclosures from records concerning him or her would specifically reveal any investigative interest in the individual. Revealing this information could reasonably be expected to compromise ongoing efforts to investigate a known or

suspected terrorist by notifying the record subject that he or she is under investigation. This information could also permit the record subject to take measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid or impede the investigation.

(b) From subsection (c)(4) (Accounting for Disclosure, notice of dispute) because certain records in this system are exempt from the access and amendment provisions of subsection (d), this requirement to inform any person or other agency about any correction or notation of dispute that the agency made with regard to those records, should not apply.

(c) From subsections (d)(1), (2), (3), and (4) (Access to Records) because these provisions concern individual access to and amendment of certain records contained in this system, including law enforcement, counterterrorism, and investigatory records. Compliance with these provisions could alert the subject of an investigation to the fact and nature of the investigation, and/or the investigative interest of intelligence or law enforcement agencies; compromise sensitive information related to law enforcement, including matters bearing on national security; interfere with the overall law enforcement process by leading to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; could identify a confidential source; reveal a sensitive investigative or intelligence technique; or constitute a potential danger to the health or safety of law enforcement personnel, confidential informants, and witnesses. Amendment of these records would interfere with ongoing counterterrorism or law enforcement investigations and analysis activities and impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised.

(d) From subsection (e)(1) (Relevancy and Necessity of Information) because it is not always possible for DHS or other agencies to know in advance what information is relevant and necessary for it to complete screening of cargo, conveyances, and passengers. Information relating to known or suspected terrorists is not always collected in a manner that permits immediate verification or determination of relevancy to a DHS purpose. For example, during the early stages of an investigation, it may not be possible to determine the immediate relevancy of information that is collected—only upon later evaluation or association with further information, obtained subsequently, may it be possible to establish particular relevance to a law enforcement program. Lastly, this exemption is required because DHS and other agencies may not always know what information about an encounter with a known or suspected terrorist will be relevant to law enforcement for the purpose of conducting an operational response.

(e) From subsection (e)(2) (Collection of Information from Individuals) because application of this provision could present a serious impediment to counterterrorism or law enforcement efforts in that it would put the subject of an investigation, study or analysis on notice of that fact, thereby permitting the subject to engage in conduct designed to frustrate or impede that activity. The nature of counterterrorism, and law enforcement investigations is such that vital information about an individual frequently can be obtained only from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely solely upon information furnished by the individual concerning his own activities.

(f) From subsection (e)(3) (Notice to Subjects), to the extent that this subsection is interpreted to require DHS to provide notice to an individual if DHS or another agency receives or collects information about that individual during an investigation or from a

third party. Should the subsection be so interpreted, exemption from this provision is necessary to avoid impeding counterterrorism or law enforcement efforts by putting the subject of an investigation, study or analysis on notice of that fact, thereby permitting the subject to engage in conduct intended to frustrate or impede that activity.

(g) From subsections (e)(4)(G), (H) and (I) (Agency Requirements) because portions of this system are exempt from the access and amendment provisions of subsection (d).

(h) From subsection (e)(5) (Collection of Information) because many of the records in this system coming from other system of records are derived from other domestic and foreign agency record systems and therefore it is not possible for DHS to vouch for their compliance with this provision; however, the DHS has implemented internal quality assurance procedures to ensure that data used in its screening processes is as complete, accurate, and current as possible. In addition, in the collection of information for law enforcement and counterterrorism purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by (e)(5) would limit the ability of those agencies' trained investigators and intelligence analysts to exercise their judgment in conducting investigations and impede the development of intelligence necessary for effective law enforcement and counterterrorism efforts.

(i) From subsection (e)(8) (Notice on Individuals) because to require individual notice of disclosure of information due to compulsory legal process would pose an impossible administrative burden on DHS and other agencies and could alert the subjects

of counterterrorism or law enforcement investigations to the fact of those investigations when not previously known.

(j) From subsection (f) (Agency Rules) because portions of this system are exempt from the access and amendment provisions of subsection (d). Access to, and amendment of, system records that are not exempt or for which exemption is waived may be obtained under procedures described in the related SORN or Subpart B of this Part.

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

Dated:

_____

Hugo Teufel III,

Chief Privacy Officer.