Rules and Regulations

Federal Register
Vol. 75, No. 22
Wednesday, February 3, 2010

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS–2009–0055]

Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/U.S. Customs and Border Protection—006 Automated Targeting 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 Department of Homeland Security/U.S. Customs and Border Protection system of records entitled the, "Department of Homeland Security/U.S. Customs and Border Protection—006 Automated Targeting System of Records" from certain provisions of the Privacy Act. Specifically, the Department exempts portions of the Department of Homeland Security/U.S. Customs and Border Protection—006 Automated Targeting system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: *Effective Date:* This final rule is effective February 3, 2010.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Laurence E. Castelli (202–325–0280), Privacy Officer, U.S. Customs and Border Protection, Office of International Trade, Mint Annex, 799 Ninth Street, NW., Washington, DC 20001–4501. For privacy issues please contact: Mary Ellen Callahan (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) published a notice of proposed rulemaking in the **Federal Register**, 72 FR 43567, August 6, 2007, 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 the DHS/U.S. Customs and Border Protection (CBP)—006 Automated Targeting system. The DHS/CBP—006 Automated Targeting system of records notice was published concurrently in the **Federal Register,** 72 FR 43650, August 6, 2007, and comments were invited on both the notice of proposed rulemaking and system of records notice. Comments were received on both notice of proposed rulemaking and system of records notice.

Public Comments

DHS received thirteen comments on the notice of proposed rulemaking (NPRM) and three comments on the system of records notice (SORN). Of the total sixteen comments: (1) Five comments are duplicate submissions; (2) four comments were erroneously filed relating to a Transportation Security Administration (TSA) publication pertaining to Secure Flight; (3) one comment was erroneously filed relating to a U.S. Customs and Border Protection publication pertaining to the Border Crossing Information system; and (4) of the discrete six comments filed in connection with this system, two comments agreed with the DHS/CBP—006 Automated Targeting (ATS) system of records. The following is an analysis of the substantive related comments and questions submitted by the public.

General Comments

Comment: ATS continues to lack transparency.

Response: DHS disagrees. In recognition of the importance of providing the public with increased notice and transparency regarding CBP's screening efforts, DHS removed ATS from coverage under the legacy Treasury/CS.244 Treasury Enforcement Communication System (66 FR 52984, October 18, 2001), where it has been operational for nearly a decade, and created a separate SORN for ATS (72 FR 43650, August 6, 2007) that details with particularity the collection of information by the system and its use.

Comment: Mission creep is inevitable.

Response: ATS is designed to assist CBP in ensuring compliance not only with customs (Title 19) and immigration laws (Title 8) under its jurisdiction, but also with the numerous other U.S. laws that CBP enforces on behalf of many Federal agencies, such as: (1) The Agricultural Bioterrorism Protection Act of 2002 (7 U.S.C. 8401); (2) the Honeybee Act (7 U.S.C. 281–286); (3) the Export Administration Act of 1979 (15 U.S.C. 4605); (4) the Copyright Act (17 U.S.C. 101–120); (5) the Clean Air Act (42 U.S.C. 7521–7543); and (6) the Trading with the Enemy Act (50 U.S.C. App 1–§ 44). By necessity, ATS is designed to accommodate changes in both the law and the intelligence landscape. However, the use of ATS is governed by a number of policy and administrative checks and balances to ensure that ATS, and the PNR, are maintained specifically in the ATS module, referred to as that Automated Targeting System—Passenger (ATS–P), and used in a manner appropriate with the mission of DHS.

Comment: Computer algorithms cannot make accurate security judgments.

Response: ATS does not, by itself, form administrative decisions or institute law enforcement actions against travelers and cargo. Instead, ATS is a decision-support tool that assists CBP officers in identifying individuals who, and cargo which, warrant additional screening. Any legal actions are the result of a trained CBP officer's hands-on interaction and examination of a person or cargo and a consideration of additional evidence or information obtained from the traveler and other sources, or in the case of cargo, the entry documents and other available data.

Comment: ATS will result in the creation of 'security ratings' for citizens.

Response: Unlike the ATS components relating to cargo, ATS–P does not assign a "risk score" to travelers. Instead, travelers that ATS, and more specifically, ATS–P, identifies for possible further scrutiny are not selected because of any rating or objective physical characteristic or political, religious, racial, or ethnic affiliation. Travelers are so identified as the result of threshold targeting rules in

ATS, which are based on current intelligence or past case experience. Travelers may also be identified for further screening if their date of birth or identifier match an entry placed for subject query in DHS/CBP—011 TECS (73 FR 77778, December 19, 2008). A subject query is a query of records that pertains to persons, aircraft, businesses, or vehicles.

SORN Routine Use Comments

Comment: The Routine Uses categories are so broad as to be almost meaningless.

Response: CBP is a law enforcement agency that enforces over 400 statutes on behalf of more than 40 agencies in the Federal government. In addition, CBP and its predecessor agencies (the U.S. Customs Service and the Immigration and Naturalization Service), have signed Memoranda of Understandings (MOUs) or similar agreements with a wide variety of Federal, State and local agencies with border security and law enforcement interests and have similar arrangements with other nations, including customs mutual assistance agreements (CMAAs). The Routine Uses are established to facilitate the sharing of specific information in furtherance of these shared law enforcement missions. The Routine Uses set forth at great length in the ATS SORN also provide notice and transparency to the public as to the nature and extent of the sharing of ATS data while containing appropriate parameters to limit the sharing of discrete law enforcement purposes.

Comment: Routine Use C duplicates and weakens the statutory condition of disclosure in (b)(8) because it does not include notification to the individual required by statute.

Response: The statutory condition of disclosure set forth in section (b)(8) of the Privacy Act permits disclosure of a record "to a person pursuant to a showing of compelling circumstances affecting the health and safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual." As set forth in the ATS SORN (72 FR 43650, August 6, 2007), Routine Use C permits disclosure of ATS data to an organization or individual that is or could become the target of a particular terrorist activity or conspiracy. As such, Routine Use C does not weaken the statutory condition, which is most commonly utilized in compelling public health situations involving exposure to communicable or quarantinable diseases, but instead, illustrates circumstances appropriate to a disclosure for compelling safety reasons involving both organizations and individuals. With regard to the statutory provisions of section (b)(8) of the Privacy Act, in the instance of a potential pandemic outbreak resulting from exposure to a communicable or quarantinable disease during travel and the possible subsequent dispersal throughout a region or the nation, CBP's first responsibility is to inform the proper health agencies and professionals of this risk to facilitate a rapid response to protect the public health. Routine Use D also eliminates potential duplicative reporting requirements to U.S. authorities responsible for protecting public health and combating pandemics. As such, it reduces the economic burden on air carriers. It also promotes the privacy interest of travelers by minimizing the processing of their information by U.S. authorities.

Comment: Routine Use M, which provides access to the Federal government and unnamed third parties while keeping the data secret from the individual, is a strange use of Privacy Act exemptions.

Response: The language of Routine Use M was drafted by the Department of Justice (DOJ) in connection with the Identity Theft Task Force (*See* "Combating Identity Theft: A Strategic Plan" at *http://www.identitytheft.gov*) to address security breaches where disclosure under statutory condition (b)(1) is not applicable. In particular, this Routine Use is intended to cover situations where a breach has occurred and DHS may need to share information with agencies or entities conducting an investigation or to facilitate notifying the individuals whose information has been breached. The "unnamed third party" will be an entity under contract and subject to a non-disclosure agreement to provide services related to the security breach. The "unnamed third party" would only receive the minimum information necessary to perform contracted services such as determining the specific circumstances of the data breach and informing individuals of the breach, its extent, and remedies to be offered, as appropriate. Normally, the type of information to be shared is restricted to name and address, "contact information," and would not include information about the context of the records or non-identity related facts.

Legality of ATS System Comments

Comment: ATS is prohibited by the Privacy Act because it involves the collection and retention of records pertaining to activities protected by the First Amendment (*i.e.,* "right of assembly").

Response: CBP has broad authority to conduct activities relating to the entry into, or exit from the United States, of persons or goods. *See* 19 U.S.C. 482, 1461, 1496, 1499, 1581–83; 8 U.S.C. 1225, 1357; 31 U.S.C. 5332. ATS is a decision-support tool used by CBP officers to execute this lawful border enforcement authority and does not violate the right of citizens to assemble.

Comment: ATS is in violation of the funding prohibitions in section 514 of the 2007 Department of Homeland Security Appropriations Act.

Response: As specified with particularity, Section 514 of the 2007 Homeland Security Appropriations Act, Public Law 109–295, and the funding restrictions set forth therein, pertain to the "Secure Flight program administered by the Transportation Security Administration or any other follow-on or successor passenger screening program." Inasmuch as ATS has been funded by Congress since the late 1990s, it is clearly not a "follow-on or successor" to Secure Flight." Secure Flight is intended to screen domestic passengers attempting to board aircraft; ATS–P is used in connection with individuals seeking admission to the U.S. at ports of entry. Unlike Secure Flight, Congress has not imposed any independent restriction on ATS–P for passenger screening and instead, has appropriated funding for ATS's Passenger Screening Program.

Privacy Act Exemption Comments

Comment: Exempting business confidential information, PNR data, received from commercial third parties from access is contrary to the Privacy Act.

Response: ATS does not exempt access to PNR data about the requestor, obtained from either the requestor or from a booking agent, broker, or another person submitting on behalf of the requestor. DHS will provide the first party requestor with the information in the form in which it was received from the respective carrier about the individual. ATS does exempt business confidential information pertaining to the carrier from access, but this information is not submitted by or on behalf of the requestor, nor does it pertain personally to the requestor. ATS provides access to the raw PNR data in the form that it was submitted, upon request by the individual to whom the data pertains.

Comment: The proposed exemptions violate the requirements of relevance, necessity, accuracy, timeliness and completeness under the Privacy Act.

Response: The Privacy Act requires that an agency "maintain in its records

only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or executive order of the President." 5 U.S.C. 552a (e)(1). CBP, in consideration of its law enforcement mission, claims an exemption from this requirement. The purpose of this Privacy Act exemption is to strike a balance between protecting information collected about persons, while permitting law enforcement agencies to effectively carry out their missions. Here, the information used by ATS and specifically ATS–P, including PNR, has a long history of supporting successful targeting and investigations and is not available from other sources to support the prescreening of travelers prior to arrival in and departure from the United States. ATS is a unique tool that adds to an officer's ability to identify travelers who, and cargo which, may pose a higher risk of violating U.S. law. Without ATS–P, DHS would be unable to identify many travelers whose suspicious behavior is revealed only after considering past case experience and available intelligence. PNR, for example, is often only relevant when considered in light of information obtained from other law enforcement or intelligence sources. In this way, ATS–P complements and does not duplicate other border enforcement tools, such as training to identify false documents and in questioning travelers.

Comment: The proposed Privacy Act (j)(2) exemption contravenes the intent of the statute because the three statutory requirements are not met. Even if DHS asserts that innocent citizens are considered to be criminal offenders, the information qualifying for exemption must consist only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release and parole and probation status.

Response: Exemption (j)(2) permits CBP to assert an exemption for ATS because CBP is a law enforcement agency and the information in ATS is compiled to identify suspected and known criminal offenders or alleged criminal offenders. CBP is charged with screening all persons crossing U.S. borders to ensure compliance with U.S. laws. ATS exists for, among other reasons, to assist DHS in identifying those persons who, and cargo which, may pose a higher risk for violating U.S. law, while not impeding the flow of legitimate travelers, cargo, and conveyances.

Comment: The proposed Privacy Act (k)(2) exemption is inappropriate unless DHS agrees to provide ATS records to travelers who have been denied the opportunity to fly because their names were on a "list."

Response: The access provisions in the current ATS SORN clarify that a requestor may obtain access to the PNR submitted on his or her behalf by his or her respective carrier. This means that an individual may gain access to his or her PNR data, upon request. CBP has long made this information available to U.S. and non-U.S. citizens and thus this represents only a clarification of the prior ATS SORN, not a change of policy. Lastly, this access permits the requestor to seek redress for the fact that their name may be on a "list."

Comment: The proposed exemptions of the system are so broad that CBP would be allowed to use ATS with little accountability.

Response: CBP has asserted Privacy Act exemptions (j)(2) and (k)(2) to protect information maintained in a law enforcement system. These exemptions and their justifications are routinely employed throughout the Federal Government to protect official information maintained in a law enforcement system. The Privacy Act provides authority to assert as many as seven exemptions for records maintained in a system. These exemptions must be asserted in accordance with the provisions of sections (j) and (k) for purposes consistent with the provisions of the Privacy Act. CBP has only asserted exemptions (j)(2) and (k)(2), with respect to ATS, because these two exemptions covered the types and uses of information maintained in ATS. With respect to accountability, DHS already receives significant and constructive oversight by Congress and the Inspector General with respect to many of its programs, including ATS. Individuals may also seek judicial review of most enforcement actions taken by CBP, including those which may stem from the results of an ATS analysis.

Contents of ATS and PNR Comments

Comment: ATS contains passenger information obtained during a secondary screening, such as the title of a book carried by a passenger that will be used to discriminate against travelers.

Response: Secondary screening results are not collected or maintained in ATS. Instead, information relating to secondary screening is collected and maintained in other CBP data systems, in particular, DHS/CBP—011 TECS.

Comment: Data concerning race, ethnicity, political affiliation and other personal matters can be contained in PNR and used in risk assessments, which may result in discrimination against travelers.

Response: One of the many reasons travelers may be selected for additional screening is as a result of threshold targeting rules in ATS, which are based on current intelligence or past case experience and not on physical characteristics, or political, religious, racial, ethnic or sexual affiliation. Moreover, CBP policy prohibits improper discrimination and violators are subject to penalties.

Comment: Much of the ATS data in PNRs is not provided by air passengers seeking to book travel but are commercial records created and maintained by travel companies for their own purposes. The aggregation and use of PNR data from airlines permits DHS to be the enforcer of a joint blacklist by all the airlines of anyone secretly tagged with derogatory PNR sent to DHS.

Response: DHS disagrees. The PNR data that is transmitted to CBP and collected through ATS is composed primarily of information that is provided to airlines and travel agents by or on behalf of air travelers seeking to book travel. The commercial information, such as frequent flier information and internal annotations to the air fare, are transmitted to CBP as part of the PNR collected by ATS, and is limited in amount and proprietary to the submitting company.

Retention Comments

Comment: Two comments noted that the 15-year retention period for ATS is too long.

Response: Terrorist suspects often have no prior criminal record and, at the time of travel, the U.S. Government may have no other derogatory background information about them. CBP uses PNR, including historical PNR, to attempt to identify such previously unknown terrorists before they enter the United States. Specifically, ATS–P is able to analyze PNR data to uncover links between known and previously unidentified terrorists or terrorist suspects, as well as suspicious or irregular travel patterns.

CBP believes that the 15 year retention period enhances privacy protections for travelers whose information is collected, while at the same time permitting it to effectively carry out its proper law enforcement mission. Specifically, the retention period for information maintained in ATS will not exceed fifteen years, after which time it will be deleted in accordance with an approved records disposition schedule except as noted below.

Additionally, the following further access restrictions pertain to the retention and use of PNR, which is contained only in ATS–P: ATS–P users will have general access to PNR for seven years, after which time the PNR data will be moved to dormant, non-operational status. PNR data in dormant status will be retained for eight years and may be accessed only with approval of a senior DHS official designated by the Secretary of Homeland Security and only in response to an identifiable case, threat, or risk. Notwithstanding the above, information that is maintained only in ATS that is linked to law enforcement lookout records, CBP matches to enforcement activities, investigations or cases, such as specific and credible threats and flights, individuals and routes of concern, or other defined sets of circumstances, will remain accessible for the life of the law enforcement matter.

Redress and Accuracy Material Comments

Comment: Two comments noted that the supporting databases used by ATS contained inaccurate information.

Response: ATS is a decision-support tool that provides a risk analysis by comparing information contained in various databases. With the exception of PNR, ATS does not actively maintain the information from those databases; the information is merely analyzed by ATS. Therefore, when an individual is seeking redress for information other than PNR, which is maintained in ATS–P, such redress may be accomplished by referring to the databases that maintain that information. With regard to the information that is actively collected by ATS PNR data, an individual may utilize the comprehensive DHS Traveler Redress Inquiry Program (DHS TRIP) that was created to receive all traveler related comments, complaints and redress requests affecting its component agencies. Through DHS TRIP, a traveler can seek correction of erroneous information stored in ATS, as well as other databases. Although not required to do so under the provisions of the Privacy Act, which are applicable only to U.S. citizens and legal permanent residents, DHS policy extends the opportunity to access and correct data to foreign nationals as well.

Comment: No meaningful redress is provided because an individual does not know if incorrect information is kept in ATS.

Response: DHS disagrees. As noted earlier ATS provides a requestor with access to PNR that was submitted by or on behalf of the requestor. Should the requestor discover that the PNR record or records are inaccurate, then the requestor may seek redress to inform DHS of the inaccuracy and correct it.

Comment: No meaningful redress process is provided because source systems are also exempt from the protections of the Privacy Act.

Response: DHS disagrees. For example, ATS provides access to raw PNR data provided by or on behalf of the requestor. Similarly, the DHS/CBP—005 Advance Passenger Information System (73 FR 68435, November 18, 2008, 73 FR 68435) also provides access to information submitted by or on behalf of a requestor. DHS TRIP provides a means for persons to seek redress regarding information in CBP maintained databases as well as permits CBP to coordinate with other appropriate entities which may have information on a traveler. The results of screening in ATS are a decision-support tool that must still be reviewed by a CBP analyst before further action, such as a referral to secondary inspection, may occur.

Upon careful review of the submitted public comments, having taken into consideration public comments resulting from this NPRM and SORN, as well as the Department's position on these public comments, DHS has determined that for the reasons stated, it is important that the exemptions remain in place. DHS will implement the rulemaking as proposed.

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. Add at the end of Appendix C to Part 5, Exemption of Record Systems under the Privacy Act, the following new paragraph "45":

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

* * * * *

45. The DHS/CBP—006 Automated Targeting system of records 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, the DHS/CBP—006 Automated Targeting system of records compares information received with CBP's law enforcement databases, the Federal Bureau of Investigation Terrorist Screening Center's 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. This supports the several and varied missions and functions of DHS, including but not limited to: The enforcement of civil and criminal laws (including the immigration law); investigations, inquiries; national security and intelligence activities in support of the DHS mission to identify and prevent acts of terrorism against the United States. The information 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. Certain records or information in DHS/CBP—006 Automated Targeting system of records are exempt from the Privacy Act. With respect to the ATS–P module, exempt records are the targeting rule sets, risk assessment analyses, and business confidential information contained in the PNR that relates to the air and vessel carriers. No exemption shall be asserted regarding PNR data about the requester, provided by either the requester or 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 DHS/CBP—006 Automated Targeting system of records modules the only information maintained in the system is the targeting rule sets, risk assessment analyses, and a pointer to the data from the source system of records. 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 (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (e)(5), and (8); (f); and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, 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 (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (e)(5), and (8); (f); and (g) pursuant to 5 U.S.C. 552a(k)(2). 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. 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) and (4) (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 criminal or terrorist, or other person of interest, 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. 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 criminals or terrorists or other persons of interest, 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 criminal or terrorist or other person of interest 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 other 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 other 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 systems 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: January 21, 2010.

Mary Ellen Callahan

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2010–2201 Filed 2–2–10; 8:45 am]

BILLING CODE 9110–06–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS–2009–0052]

Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/U.S. Customs and Border Protection—007 Border Crossing Information 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 Department of Homeland Security/U.S. Customs and Border Protection system of records entitled the, "Department of Homeland Security/U.S. Customs and Border Protection—007 Border Crossing Information System of Records." Specifically, the Department exempts portions of the Department of Homeland Security/U.S. Customs and Border