

[Federal Register: January 18, 2007 (Volume 72, Number 11)]  
[Notices]  
[Page 2294-2298]  
From the Federal Register Online via GPO Access [wais.access.gpo.gov]  
[DOCID:fr18ja07-92]

=====

-----

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS 2006-0077]

Privacy Act; Redress and Response System of Records

AGENCY: Privacy Office, Office of the Secretary, Department of Homeland Security

ACTION: Notice of Privacy Act system of records.

-----

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) is giving notice that it proposes to add a new system of records to its inventory of record systems, the DHS Redress and Response Records System. This system maintains records for the DHS Traveler Redress Inquiry Program (TRIP), which is the traveler redress mechanism being established by DHS in connection with the Rice-Chertoff Initiative, as well as in accordance with other policy and law. As the manifestation of the one-stop redress for travelers objective stated in the Rice-Chertoff Initiative, DHS TRIP will facilitate the public's ability to provide appropriate information to DHS for redress requests when they believe they have been denied entry, refused boarding for transportation, or identified for additional screening by DHS components or programs at their operational locations, including airports, seaports, train stations and land borders that may have resulted in

[[Page 2295]]

the individual being delayed or inconvenienced. DHS TRIP will create a cohesive process to address these redress requests across DHS.

DATES: Written comments must be submitted on or before February 20, 2007.

ADDRESSES: You may submit comments, identified by Docket Number DHS-2006-0077 by one of the following methods:

Federal e-Rulemaking Portal:

<http://frwebgate.access.gpo.gov/cgi-bin/leaving.cgi?from=leavingFR.html&log=linklog&to=http://www.regulations.gov>.

Follow the instructions for submitting comments.

Facsimile: 202-572-8727 (not a toll-free number).

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

FOR FURTHER INFORMATION CONTACT: Please identify by Docket Number DHS-2006-0077 to request further information by one of the following methods:

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

Facsimile: 866-466-5370.

E-Mail: [privacy@dhs.gov](mailto:privacy@dhs.gov).

SUPPLEMENTARY INFORMATION: The Department of Homeland Security (DHS) is establishing a new system of records pursuant to the Privacy Act (5 U.S.C. 552a), entitled the Redress and Response Records System, DHS/ALL--005. The system serves as a DHS System of Records for the DHS Traveler Redress Inquiry Program (TRIP). On January 17, 2006, DHS Secretary Chertoff and Department of State Secretary Rice established the Rice-Chertoff Initiative. One objective of this initiative is to ``accelerate efforts to establish a government-wide traveler screening redress process to resolve questions if travelers are incorrectly selected for additional screening.'' DHS TRIP realizes this objective as the traveler redress program at DHS that will coordinate the redress processes for travelers among DHS components and other agencies and simplify the process for travelers.

For example, individuals who believe they have been denied entry, refused boarding for transportation, or identified for additional screening by DHS components or programs at their operational locations, including airports, seaports, train stations and land borders that may have resulted in the individual being denied access to transportation or entry into the United States or otherwise delayed or inconvenienced may submit information through DHS TRIP.

DHS TRIP collects and maintains information from the individual that DHS may use to make an appropriate determination to resolve, if possible, the underlying issue regarding the request for redress. The information collected will be used to determine which DHS component or other agency is most able to address the redress request.

DHS TRIP will serve as a mechanism to share redress-related information across DHS components, to facilitate efficient adjudication of redress requests, and to facilitate communication of redress results across DHS components. Once the information intake is complete, DHS TRIP will facilitate the transfer of or access to this information for the DHS components or other agencies redress process, which will address the redress request.

As part of addressing the redress request under DHS TRIP, each DHS component or other agency redress process may share information provided by individuals seeking redress with other DHS components or programs and other Federal agencies, such as the Department of State and the Department of Justice, including its Terrorist Screening Center, to work toward the possible resolution of the problem for the individual.

In addition, DHS TRIP will maintain a case management system of traveler redress requests. This case management function will be utilized to track case progress, to provide metrics of redress operations, to identify areas in need of additional support, and to develop lessons learned regarding the overall DHS traveler redress process.

During the course of an adjudication of a redress request submitted through DHS TRIP, records or information, exempt from specific requirements of the Privacy Act, as defined by regulation, from another

system of records may become part of, merged with, or recompiled within this system. To the extent this occurs, DHS will claim the same exemptions as were claimed in the original system from which the recompiled records, material, or information were a part. Such exempt records or information are likely to include law enforcement or national security investigation records, intelligence-related records, law enforcement encounter records, or terrorist screening records. These could come from various DHS systems, such as the Treasury Enforcement Communications System (TECS) and the Transportation Security Information System (TSIS), or from other agency systems. DHS, after conferring with the appropriate component or agency, may waive applicable exemptions in appropriate circumstances and where it would not interfere with or adversely affect the law enforcement or national security purposes of the systems from which the information is recompiled or in which it is contained.

Information that is maintained in this System of Records may need to be shared under certain circumstances to adjudicate an individual's redress request. This ordinarily will occur when, in an effort to verify an individual's identification to adjudicate a redress request, the redress program exchanges information with another governmental entity involved in an operational or informational process associated with the individual's redress request. Likewise, information may be shared with other Federal agencies where those agencies have information that can be used to distinguish the identity of the individual seeking redress from that of another individual included on a watch list.

Additionally, limited information may be shared with non-governmental entities where necessary for the sole purpose of effectuating an individual's redress request. For example, if an individual has been cleared and distinguished from a known or suspected threat to aviation security, that individual's name and appropriate associated information can be shared with the airlines to prevent future delays and disruptions for that individual while traveling.

Other types of information sharing that may result from the routine uses outlined in this notice include: (1) Disclosure to individuals who are not DHS employees but have an agency relationship with DHS to accomplish DHS responsibilities; (2) sharing when there appears to be a specific violation or potential violation of law, or identified threat or potential threat to national or international security, such as criminal or terrorist activities, based on individual records in this system; (3) sharing with the National Archives and Records Administration for proper handling of government records; (4) sharing when relevant to litigation associated with the Federal government; and (5) sharing to protect the individual who is the subject of the record from the harm of identity theft in the case of a data breach affecting this system.

DHS plans on publishing a Privacy Impact Assessment for DHS TRIP detailing the use and implementation of this System of Records in order to describe in detail specifics, including access procedures.

The Privacy Act embodies fair information principles in a statutory framework governing the means by

[[Page 2296]]

which the U.S. Government collects, maintains, uses, and discloses 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 a name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Individuals may request their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR part 5.

The Privacy Act requires that each agency publish in the Federal Register a description of the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system in order to make agency recordkeeping practices transparent, to notify individuals about the use made of personally identifiable information, and to assist the individual to more easily find files within the agency.

In accordance with 5 U.S.C. 552a(r), a report on this system has been sent to Congress and the Office of Management and Budget.  
DOCKET NUMBER DHS-2006-0077

System name:

DHS/ALL-005.

DHS Redress and Response Records System.

System Classification:

Unclassified.

System location:

Records are maintained by the Department of Homeland Security at the DHS Data Center in Washington, DC and at a limited number of remote locations where DHS components or programs maintain secure facilities and conduct DHS's mission.

Categories of individuals covered by the system:

Categories of individuals covered by this notice consist of:

A. All individuals who submit information through the DHS Traveler Redress Inquiry Program (TRIP).

B. All individuals whose records have been referred to a DHS component or program redress process by other components, programs, or agencies in connection with DHS TRIP.

C. Attorneys or other persons representing individuals submitting such requests and appeals and individuals who are the subjects of such requests.

D. DHS personnel or contractors assigned to handle such requests or appeals.

Categories of records in the system:

DHS Redress and Response Records System may contain:

A. Individual's name; date of birth; contact information; phone number; e-mail address; address; flight or travel information; application information, including the date of request and a description of the circumstances that led to the request of the redress form; passport number; appropriate immigration documents; documents used to support application for entry; correspondence from individuals regarding their redress requests; records of contacts made by or on behalf of individuals; documents submitted to verify identity or otherwise support the request for redress; and any other document relevant and appropriate to the particular redress program.

B. For those requesting redress as representatives of affected

individuals, representative name, contact information, phone number, e-mail address, relationship to the affected individuals, and power of attorney.

C. The name of the DHS component, DHS program, or other Federal agency, which will be responsible for addressing the incoming redress request as well as supporting components or agencies.

D. Administrative and contact information concerning DHS employees, contractors, or other agency representatives associated with the processing and/or adjudication of requests submitted to the redress process.

E. Appropriate information to reflect the resolution of a particular redress request, information determined during adjudication of the case, and sensitive information relevant to the redress process for the individual.

Authority for maintenance of the system:

Privacy Act of 1974, 5 U.S.C. 552a, as amended; Intelligence Reform and Terrorism Prevention Act of 2004, section 4012, 49 U.S.C. 114(f); 19 U.S.C. 482, 1461, 1496, and 1581-1582; 8 U.S.C. 1357; Title VII of Public Law 104-208; 49 U.S.C. 44909; and others.

Purpose(s):

This system maintains records in support of DHS TRIP that: (1) Coordinates DHS traveler redress programs to create a more efficient, effective, and easier process for individuals who believe they have been denied entry, refused boarding for transportation, or identified for additional screening at DHS component or program operational locations, including airports, seaports, train stations and land borders that may result in the individual being delayed or inconvenienced; and (2) stores information submitted by and collected from the individual or an individual's representative and information recompiled from or created from information from other DHS components and program and other government agencies, in order to address the individual's redress request.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3):

A. To a Federal, State, territorial, tribal, local, international, or foreign government agency or entity for the purpose of consulting with that agency or entity: (1) To assist in making a determination regarding redress for an individual in connection with the operations of a DHS component or program; (2) for the purpose of verifying the identity of an individual seeking redress in connection with the operations of a DHS component or program; or (3) for the purpose of verifying the accuracy of information submitted by an individual who has requested such redress on behalf of another individual.

B. To a Federal agency or entity that furnished a record or information for the purpose of permitting that agency or entity to make a decision regarding access to or correction of the record or information or to a Federal agency or entity that has information relevant to the redress request for purposes of obtaining guidance,

additional information, or advice from such Federal agency or entity regarding the handling of this particular redress request.

C. To third parties lawfully authorized in connection with a Federal Government program, which is authorized by law, regulation, or rule, but only the information necessary and relevant to effectuate or to carry out a particular redress result for an individual and disclosure is appropriate to enable these third parties to carry out their responsibilities related to the Federal Government program, such as when the name and appropriate associated information about an individual who has been cleared and distinguished from a known or

[[Page 2297]]

suspected threat to aviation security, is shared with the airlines to prevent future delays and disruptions for that individual while traveling.

D. To contractors, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or otherwise have an agency relationship with DHS, when the disclosure is necessary and relevant to the operation of the DHS TRIP program or the redress process of a DHS component or program in compliance with the Privacy Act, 5 U.S.C. 552a, as amended, including 5 U.S.C. 552a(m), in the case of the operation of all or a portion of this system of records on behalf of DHS.

E. To an appropriate Federal, State, territorial, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and disclosure is appropriate to the proper performance of the official duties of the person receiving the disclosure.

F. To an appropriate Federal, State, territorial, tribal, local, international, or foreign government intelligence entity, counterterrorism agency, or other appropriate authority charged with investigating threats or potential threats to national or international security or assisting in counterterrorism efforts, where a record, either on its face or in conjunction with other information, identifies a threat or potential threat to national or international security, which includes terrorist activities, and disclosure is appropriate to the proper performance of the official duties of the person receiving the disclosure.

G. To a Congressional office, for the record of an individual in response to an inquiry from that Congressional office made at the request of the individual to whom the record pertains.

H. To the National Archives and Records Administration or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

I. To the United States Department of Justice (DOJ) (including United States Attorney offices) or another Federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation: (1) The United States, or any department or agency thereof; (2) any employee of DHS in his or her official capacity; or (3) any employee of DHS in his or her individual capacity where DOJ has agreed

to represent said employee.

J. To appropriate agencies, entities, and persons when: (1) It is suspected or confirmed that the security or confidentiality of information in the System of Records has been compromised; (2) DHS has determined that, as a result of the suspected or confirmed compromise, there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) that rely upon the compromised information; and (3) the disclosure is made to such agencies, entities, and persons who are reasonably necessary to assist in connection with the DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Records are stored electronically at the DHS Data Center in a secure facility. In addition, the records may be stored on a local system, magnetic disc, tape, CD-ROM, and other digital media, and may also be retained in hard copy format in secure file folders at the location of the DHS component or program for which the redress process exists.

Retrievability:

Data are retrievable by the individual's name or other identifier, such as case number, as well as non-identifying information.

Safeguards:

Information in this system is safeguarded in accordance with applicable laws, rules, and policies, including the DHS Information Technology Security Program Handbook. The Redress and Response Records System security protocols will meet applicable NIST Security Standards, from Authentication to Certification and Accreditation. Records in the system will be maintained in a secure, password-protected electronic system that will utilize security hardware and software to include multiple firewalls, active intruder detection, and role-based access controls. Additional safeguards will vary by component and program. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include restricting access to authorized personnel who have a need-to-know, using locks, and password protection identification features. DHS file areas are locked after normal duty hours and the facilities are protected from the outside by security personnel.

Retention and disposal:

DHS TRIP handles both information collected directly from the individual and information collected from DHS components and other agencies. DHS is working on a retention schedule with its Senior Records Officer for information collected directly from the individual. It is anticipated that the retention period for these records will be up to seven years. To the extent information is collected from other

systems, data is retained in accordance with the record retention requirements of those systems.

System manager(s) and address:

The System Manager is the Program Manager, DHS TRIP, U.S. Department of Homeland Security, Washington, DC 20528.

Notification procedure:

Any individual who wants to know whether this system of records contains a record about him or her may contact the System Manager, noted above. An e-mail address and fax number will be provided to the individual after the submission of the redress request that may also be used.

Record access procedures:

Requests for access should be submitted to the System Manager when an individual seeks to access his or her information. Requesters will be required to provide adequate identification, such as a driver's license, employee identification card, or other identifying document. Additional identification procedures may be required in some instances in accordance with various adjudication procedures related to the redress processing by DHS components or other agencies.

Contesting record procedures:

Requests for correction or amendment must identify the information to be changed and the corrective action sought. Requests must be submitted to the System Manager as provided above.

Record source categories:

Any person, including citizens and representatives of Federal, State or local governments; businesses; and industries. Any Federal system with

[[Page 2298]]

records appropriate and relevant to the redress process.

Exemptions claimed for the system:

No exemption shall be asserted with respect to information submitted by and collected from the individual or the individual's representative in the course of any redress process associated with this 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), (k)(1), (k)(2), and (k)(5), DHS will also claim the original exemption 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. Such exempt



records or information may be law enforcement or national security investigation records, law enforcement activity and encounter records, or terrorist screening records.

These records could come from various DHS systems, such as the Treasury Enforcement Communications System (TECS) and the Transportation Security Information System (TSIS), or from third agency systems. DHS, 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 or national security purposes of the systems from which the information is recompiled or in which it is contained. As required under the Privacy Act, DHS will issue a rule to describe more fully the needs and requirements for taking such exemptions on such information.

Dated: January 12, 2007.  
Hugo Teufel III,  
Chief Privacy Officer.  
[FR Doc. 07-190 Filed 1-12-07; 8:45 am]

BILLING CODE 4410-10-P