

**Sec. 2 Penalties:**

On public lands, under section 303(a) of the Federal Land Policy and Management Act of 1976 (43 U.S.C. 1733(a)) and 43 CFR 8360.0-7 any person who violates any of these supplementary rules within the boundaries established in the rules may be tried before a United States Magistrate and fined no more than \$1,000 or imprisoned for no more than 12 months, or both. Such violations may also be subject to the enhanced fines provided for by 18 U.S.C. 3571.

On public lands fitting the criteria in the Sikes Act (16 U.S.C. 670), under section 303(a) of the Federal Land Policy and Management Act of 1976, 43 U.S.C. 1733(a) and 16 U.S.C. 670j(a)(2), any person who violates any of these supplementary rules on public lands within the boundaries established in the rules may be tried before a United States Magistrate and fined no more than \$500.00 or imprisoned for no more than six months, or both. Such violations may also be subject to the enhanced fines provided for by 18 U.S.C. 3571.

**Elaine M. Brong,**

*State Director, Oregon State Office, Bureau of Land Management.*

[FR Doc. 05-14941 Filed 7-27-05; 8:45 am]

**BILLING CODE 4310-33-P**

---

## DEPARTMENT OF JUSTICE

### Federal Bureau of Investigation

[AAG/A Order No. 005-2005]

#### Privacy Act of 1974; System of Records

**AGENCY:** Federal Bureau of Investigation, DOJ.

**ACTION:** Notice to establish system of records.

**SUMMARY:** The Federal Bureau of Investigation (FBI) proposes to add a system of records to its inventory of record systems subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended. The FBI is establishing a new system of records to cover records maintained by the Terrorist Screening Center (TSC). These records were previously covered by the FBI Central Records System (Justice/FBI-002), last published in full text on February 20, 1998 (63 FR 8671) and amended in part on March 29, 2001 (66 FR 17200). Public comments are invited.

**DATES:** This action will be effective on September 6, 2005, unless comments are received that would result in a contrary determination.

**ADDRESSES:** Address all comments to Mary E. Cahill, Management Analyst, Management and Planning Staff, Justice Management Division, Department of Justice, Washington, DC 20530 (Room 1400, National Place Building).

**FOR FURTHER INFORMATION CONTACT:** Mary E. Cahill, (202) 307-1823.

**SUPPLEMENTARY INFORMATION:** On September 16, 2003, President George W. Bush issued Homeland Security Presidential Directive-6 (HSPD-6), which directed the establishment of an organization that would consolidate the government's approach to terrorism screening and provide for the appropriate and lawful use of terrorist information in screening processes. As a result, the Director of Central Intelligence, Secretaries of State and Homeland Security, and the Attorney General signed a memorandum of understanding creating the TSC and placing it within the FBI, U.S. Department of Justice (DOJ). The Secretaries of the Treasury and Defense signed an addendum to the memorandum to join the partnership supporting the TSC. The TSC became operational on December 1, 2003 and is charged with consolidating and maintaining the U.S. government's terrorist watch list. In fulfilling its mission, the TSC collects and maintains records about individuals, described below, that are subject to the requirements of the Privacy Act. These records were previously covered by the FBI Central Records System (Justice/FBI-002) and upon the effective date of this notice they will be part of the Terrorist Screening Records System (TSRS), Justice/FBI-019.

Prior to HSPD-6, information about known or suspected terrorists was dispersed throughout the U.S. Government and no one agency was charged with consolidating it and making it available for use in terrorist screening. In March 2004, the TSC consolidated the government's terrorist watchlist information into a sensitive-but-unclassified database, known as the Terrorist Screening Database (TSDB), containing only identifying information about known or suspected terrorists. As required by HSPD-6, the TSDB contains "information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism." Information from the TSDB is now used to screen for terrorists in a variety of contexts, including during law enforcement encounters, the adjudication of applications for U.S. visas or other immigration and citizenship benefits, at U.S. land borders

and ports of entry, and for civil aviation security purposes. The TSDB is included in the new TSRS.

Other records in the TSRS include those that document the operational support TSC provides to agencies that screen for terrorists ("screening agencies") and its internal quality assurance process to ensure the terrorist data is thorough, accurate and current. On a 24-hour basis, the TSC assists state, local and federal agencies in determining if an individual they have encountered is a positive identity match to a known or suspected terrorist. TSC also facilitates an appropriate and coordinated law enforcement response or other appropriate response (e.g., medical and containment response to a biological hazard) to positive terrorist encounters. TSC uses information from other government databases, some of which are classified, to facilitate the identity match process and incorporates that information into TSC records as appropriate.

The TSC also maintains records related to the resolution of terrorist watchlist-related complaints or inquiries. The TSC plans to include a misidentified persons list, which is intended to help clear individuals who have been repeatedly misidentified as matches to the TSDB during screening. Misidentified persons are not in the TSDB, but simply bear a close enough similarity in their name or other identifier to someone who is in the TSDB, such that the screening process cannot readily differentiate them. The remedy for misidentified persons is therefore not removal from the TSDB, because they are not in fact in it, but a mechanism to permit the screening agency to readily identify them as persons who have been repeatedly confused with a known or suspected terrorist in the past. When operational, this list would be used by the TSC and each screening agency that uses the TSC, to help distinguish misidentified persons during the screening process. This would consolidate and improve the current redress processes for misidentified persons, which vary from agency to agency and usually only provide relief with respect to one agency's screening programs, but not those run by other agencies. The ultimate goal of a consolidated misidentified persons list would be to drastically reduce, and ultimately eliminate altogether, the delay and inconvenience that misidentified persons have experienced as a result of terrorist screening.

Because TSRS contains information about known or suspected terrorists that is derived from law enforcement and

intelligence sources, the Attorney General is proposing to exempt this system from certain portions of the Privacy Act, as permitted by law, to protect classified and sensitive information contained in this system and to prevent the compromise of ongoing counterterrorism investigations, sources and methods. As required by the Privacy Act, a proposed rule is being published concurrently with this notice to seek public comment on the proposal to exempt this system.

In accordance with 5 U.S.C. 552a(r), the Department of Justice has provided a report of this new system of records to the Office of Management and Budget and to Congress.

Dated: July 22, 2005.

**Paul R. Cortis,**

*Assistant Attorney General for Administration.*

#### **JUSTICE/FBI-019**

##### **SYSTEM NAME:**

Terrorist Screening Records System.

##### **SECURITY CLASSIFICATION:**

Classified, unclassified (law enforcement sensitive).

##### **SYSTEM LOCATION:**

Terrorist Screening Center, Federal Bureau of Investigation, Washington, DC.

##### **CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

- a. Individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism ("known or suspected terrorists");
- b. Individuals identified during a terrorist screening process as a possible identity match to a known or suspected terrorist;
- c. Individuals who are repeatedly misidentified as a possible identity match to a known or suspected terrorist ("misidentified persons"); and
- d. Individuals about whom a terrorist watchlist-related redress inquiry has been made.

##### **CATEGORIES OF RECORDS IN THE SYSTEM:**

- a. Identifying information, such as name, date of birth, place of birth, biometrics, passport and/or drivers license information, and other available identifying particulars used to compare the identity of an individual being screened with a known or suspected terrorist;
- b. Information about encounters with individuals covered by this system, such as date, location, screening agency, analysis, and results (positive or negative identity match), and, for

terrorist encounters only, other agencies notified and details of any law enforcement or other operational response;

c. For known or suspected terrorists, in addition to the categories of records listed above, references to and/or information from other government law enforcement and intelligence databases;

d. For misidentified persons, in addition to the categories of records listed above, additional identifying information that will be used during screening only for the purpose of distinguishing them from a known or suspected terrorist who has similar identifying characteristics (such as name, date of birth, etc.); and

e. For redress inquiries, in addition to the categories of records listed above, information provided by individuals or their representatives, information provided by the screening agency, and internal work papers and other documents related to researching and resolving the inquiry.

##### **AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

Homeland Security Presidential Directive-6, "Integration and Use of Screening Information to Protect Against Terrorism" (Sept. 16, 2003); E.O. 13356, "Strengthening the Sharing of Terrorism Information to Protect Americans" (Aug. 27, 2004); 28 U.S.C. 533.

##### **PURPOSE(S):**

- a. To implement the U.S. Government's National Strategy for Homeland Security and Homeland Security Presidential Directive-6, to identify potential terrorist threats, to uphold and enforce the law, and to ensure public safety.
- b. To consolidate the government's approach to terrorism screening and provide for the appropriate and lawful use of terrorist information in screening processes.
- c. To maintain current, accurate and thorough terrorist information in a consolidated terrorist screening database and determine which agencies' terrorist screening processes will use each entry in the database.
- d. To ensure that appropriate information possessed by state, local, territorial, and tribal governments, which is lawfully available to the Federal Government, is considered in determinations made by the TSC as to whether a person is a match to a known or suspected terrorist.
- e. To host mechanisms and make terrorist information available to support appropriate domestic, foreign, and private sector terrorist screening processes.

f. To provide continual operational support to assist in the identification of persons screened and to facilitate an appropriate and lawful response when a known or suspected terrorist is identified in an agency's screening process.

g. To provide appropriate government officials and agencies with information about encounters with known or suspected terrorists.

h. To assist persons repeatedly misidentified during a terrorist screening process and to assist agencies in responding to individual complaints about the screening process (redress).

##### **ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:**

The TSC may disclose relevant system records in accordance with any current and future blanket routine uses established for FBI record systems. See Blanket Routine Uses (BRU) Applicable to More Than One FBI Privacy Act System of Records, Justice/FBI-BRU, published on June 22, 2001 at 66 FR 33558 and amended on February 14, 2005 at 70 FR 7513. In addition, as routine uses specific to this system, the TSC may disclose relevant system records to the following persons or entities and under the circumstances or for the purposes described below, to the extent such disclosures are compatible with the purpose for which the information was collected. (Routine uses are not meant to be mutually exclusive and may overlap in some cases.)

A. To those Federal agencies that have agreed to provide support to TSC for purposes of ensuring the continuity of TSC operations.

B. To Federal, State, local, tribal, territorial, foreign, multinational or other public agencies or entities, to entities regulated by any such agency or entity, and to owners/operators of critical infrastructure and their agents, contractors or representatives, for the following purposes: (1) For use in and in support of terrorist screening authorized by the U.S. Government, (2) to provide appropriate notifications of a positive terrorist encounter or a threat related to the encounter, (3) to facilitate any appropriate law enforcement or other response (e.g., medical and containment response to a biological hazard) to a terrorist encounter or a threat related to the encounter, and (4) to assist persons repeatedly misidentified during a screening process.

C. To any individual, organization, or governmental entity in order to notify them of a serious terrorist threat for the

purpose of guarding against or responding to such a threat.

D. To Federal, State, local, tribal, territorial, foreign, or multinational agencies or entities, or other organizations that are engaged in, or are planning to engage in terrorist screening authorized by the U.S. Government, for the purpose of the development, testing, or modification of information technology systems used or intended to be used during or in support of the screening process; whenever possible, however, TSC will substitute de-identified data.

E. To Federal, State, local, tribal, territorial, foreign, or multinational agencies or entities to assist in coordination of terrorist threat awareness, assessment, analysis or response.

F. To any person or entity in either the public or private sector, domestic or foreign, where reasonably necessary to elicit information or cooperation from the recipient for use by the TSC in the performance of an authorized function, such as obtaining information from data sources as to the thoroughness, accuracy, currency, or reliability of the data provided so that the TSC may review the quality and integrity of its records for quality assurance or redress purposes, and may also assist persons repeatedly misidentified during a screening process.

G. To any federal, state, local, tribal, territorial, foreign or multinational agency, task force, or other entity or individual that receives information from the U.S. Government for terrorist screening purposes, in order to facilitate TSC's or the recipient's review, maintenance, and correction of TSC data for quality assurance or redress purposes, and to assist persons repeatedly misidentified during a screening process.

H. To any agency, organization or individual for the purposes of performing authorized audit or oversight operations of the DOJ, FBI, TSC, or any agency engaged in or providing information used for terrorist screening that is supported by the TSC, and meeting related reporting requirements.

I. To a former employee of the TSC (including those detailed or assigned to the TSC from another government agency) or a former contractor supporting the TSC for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with any applicable government regulations; or facilitating communications with a former employee/contractor that may be

necessary for personnel-related or other official purposes where the TSC requires information and/or consultation assistance from the former employee/contractor regarding a matter within that person's former area of responsibility.

J. To any criminal, civil, or regulatory law enforcement authority (whether federal, state, local, territorial, tribal, multinational or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.

K. To a governmental entity lawfully engaged in collecting law enforcement, law enforcement intelligence, or national security intelligence information for law enforcement or intelligence purposes.

**DISCLOSURE TO CONSUMER REPORTING AGENCIES:**

None.

**POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:**

**STORAGE:**

Records in this system are stored in paper and/or electronic format. Electronic storage is on servers, CD-ROMs, DVD-ROMs, and magnetic tapes.

**RETRIEVABILITY:**

Records in this system are typically retrieved by individual name, date of birth, passport number, and other identifying data, including unique identifying numbers assigned by the TSC or other government agencies.

**SAFEGUARDS:**

All records are maintained in a secure government facility with access limited to only authorized personnel or authorized and escorted visitors. Physical security protections include guards and locked facilities requiring badges and passwords for access. Records are accessed only by authorized government personnel and contractors and are protected by appropriate physical and technological safeguards to prevent unauthorized access. All federal employees and contractors assigned to the TSC must hold an appropriate security clearance, sign a non-disclosure agreement, and undergo privacy and security training.

**RETENTION AND DISPOSAL:**

Records in this system will be retained and disposed of in accordance with a records schedule to be approved by the National Archives and Records Administration.

**SYSTEM MANAGER(S) AND ADDRESS:**

Director, Terrorist Screening Center, Federal Bureau of Investigation, FBI

Headquarters, 935 Pennsylvania Avenue, NW., Washington, DC 20535-0001.

**NOTIFICATION PROCEDURE:**

Because this system contains classified and law enforcement information related to the government's counterterrorism, law enforcement and intelligence programs, records in this system have been exempted from notification, access, and amendment to the extent permitted by subsections (j) and (k) of the Privacy Act. Requests for notification should be addressed to the FBI at the address and according to the requirements set forth below under the heading "Record Access Procedures."

**RECORD ACCESS PROCEDURES:**

Because this system contains classified and law enforcement information related to the government's counterterrorism, law enforcement and intelligence programs, records in this system have been exempted from notification, access, and amendment to the extent permitted by subsections (j) and (k) of the Privacy Act. A request for access to a non-exempt record shall be made in writing with the envelope and the letter clearly marked "Privacy Act Request." Include in the request your full name and complete address. The requester must sign the request; and, to verify it, the signature must be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. You may submit any other identifying data you wish to furnish to assist in making a proper search of the system. Requests for access to information must be addressed to the Record Information Dissemination Section, Federal Bureau of Investigation, 935 Pennsylvania Avenue, NW., Washington, DC 20535-0001.

**CONTESTING RECORD PROCEDURES:**

Because this system contains classified and law enforcement information related to the government's counterterrorism, law enforcement and intelligence programs, records in this system are exempt from notification, access, and amendment to the extent permitted by subsections (j) and (k) of the Privacy Act. Requests for amendment should be addressed to the FBI at the address and according to the requirements set forth above under the heading "Record Access Procedures."

If, however, individuals are experiencing repeated delays or difficulties during a government screening process and believe that this might be related to terrorist watch list information, they may contact the

Federal agency that is conducting the screening process in question ("screening agency"). The screening agency is in the best position to determine if a particular problem relates to a terrorist watch list entry or is due to some other cause, such as a criminal history, an immigration violation or random screening. Some individuals also experience repeated delays during screening because their names and/or other identifying data, such as dates of birth, are similar to those of known or suspected terrorists. These individuals, referred to as "misidentified persons," often believe that they themselves are on a terrorist watch list, when in fact they only bear a similarity in name or other identifier to an individual on the list. Most screening agencies have or are developing procedures to expedite the clearance of misidentified persons during screening.

By contacting the screening agency with a complaint, individuals will be able to take advantage of the procedures available to help misidentified persons and others experiencing screening problems. Check the agency's requirements for submitting complaints but, at a minimum, individuals should describe in as much detail as possible the problem they are having, including dates and locations of screening, and provide sufficient information to identify themselves, such as full name, citizenship status, and date and place of birth. The TSC assists the screening agency in resolving any screening complaints that may relate to terrorist watch list information, but does not receive or respond to individual complaints directly. However, if TSC receives any such complaints, TSC will forward them to the appropriate screening agency.

#### RECORD SOURCE CATEGORIES:

Information in this system is obtained from individuals covered by the system, public sources, agencies conducting terrorist screening, law enforcement and intelligence agency record systems, government databases, and foreign governments.

#### EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d)(1), (2), (3) and (4), (e)(1), (2), (3), (5) and (8), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j) and (k). These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j) and (k). Rules have been promulgated in accordance with the

requirements of 5 U.S.C. 553(b), (c) and (e).

[FR Doc. 05-14849 Filed 7-27-05; 8:45 am]

BILLING CODE 4410-02-P

## DEPARTMENT OF JUSTICE

### Parole Commission

#### Sunshine Act; Record of Vote of Meeting Closure (Public Law 94-409) (5 U.S.C. 552b)

I, Edward F. Reilly, Jr., Chairman of the United States Parole Commission, was present at a meeting of said Commission, which started at approximately 3 p.m. on Monday, July 18, 2005, at the U.S. Parole Commission, 5550 Friendship Boulevard, 4th Floor, Chevy Chase, Maryland 20815. The purpose of the meeting was to discuss the procedure to be followed for review of one case upon request of the Attorney General as provided in 18 U.S.C. 4215(c).

Public announcement further describing the subject matter of the meeting and certifications of General Counsel that this meeting may be closed by vote of the Commissioners present were submitted to the Commissioners prior to the conduct of any other business. Upon motion duly made, seconded, and carried, the following Commissioners voted that the meeting be closed: Edward F. Reilly, Jr., Cranston J. Mitchell, Deborah A. Spagnoli, Isaac Fulwood, Jr., and Patricia Cushwa.

*In witness whereof*, I make this official record of the vote taken to close this meeting and authorize this record to be made available to the public.

Dated: July 19, 2005.

**Edward F. Reilly, Jr.**,

*Chairman, U.S. Parole Commission.*

[FR Doc. 05-15004 Filed 7-26-05; 8:45 am]

BILLING CODE 4410-01-M

## DEPARTMENT OF LABOR

### Employment Standards Administration

#### Proposed Collection; Comment Request

**ACTION:** Notice.

**SUMMARY:** The Department of Labor, as part of its continuing effort to reduce paperwork and respondent burden, conducts a preclearance consultation program to provide the general public and Federal agencies with an opportunity to comment on proposed and/or continuing collections of

information in accordance with the Paperwork Reduction Act of 1995 (PRA95) [44 U.S.C. 3506(c)(2)(A)]. This program helps to ensure that requested data can be provided in the desired format, reporting burden (time and financial resources) is minimized, collection instruments are clearly understood, and the impact of collection requirements on respondents can be properly assessed. Currently, the Employment Standards Administration is soliciting comments concerning the proposed collection: Notice of Controversion of Right to Compensation (LS-207). A copy of the proposed information collection request can be obtained by contacting the office listed below in the addresses section of this Notice.

**DATES:** Written comments must be submitted to the office listed in the addresses section below on or before September 26, 2005.

**ADDRESSES:** Ms. Hazel M. Bell, U.S. Department of Labor, 200 Constitution Ave., NW., Room S-3201, Washington, DC 20210, telephone (202) 693-0418, fax (202) 693-1451, e-mail [bell.hazel@dol.gov](mailto:bell.hazel@dol.gov). Please use only one method of transmission for comments (mail, fax, or e-mail).

#### SUPPLEMENTARY INFORMATION:

I. *Background:* The Division of Longshore and Harbor Workers' Compensation administers the Longshore and Harbor Worker's Compensation Act. This Act provides benefits to workers injured in maritime employment on the navigable waters of the United States or in an adjoining area customarily used by an employer in loading, unloading, repairing or building a vessel. In addition, several acts extend Longshore Act coverage to certain other employees. Pursuant to sections 914(d) of the Act, and 20 CFR 702.251, if an employer controverts the right to compensation he/she shall file with the district director in the affected compensation district on or before the fourteenth day after he/she has knowledge of the alleged injury or death, a notice, in accordance with a form prescribed by the Secretary, stating that the right to compensation is controverted. Form LS-207 is used for this purpose. Form LS-207 is used by insurance carriers and self-insured employers to controvert claims under the Longshore Act and extensions. The information is used by OWCP district offices to determine the basis for not paying benefits in a case. This information collection is currently approved for use through March 31, 2006.