supplement to the complaint on August 8, 2007. The complaint, as supplemented, alleges violations of § 337 in the importation into the United States, the sale for importation, and the sale within the United States after importation of certain nitrile rubber gloves by reason of infringement of U.S. Patent No. Re. 35,616. The complaint further alleges that an industry in the United States exists as required by subsection (a)(2) of § 337.

The complainant requests that the Commission institute an investigation and, after the investigation, issue a permanent exclusion order and a permanent cease and desist order.

ADDRESSES: The complaint, except for any confidential information contained therein, is available for inspection during official business hours (8:45 a.m. to 5:15 p.m.) in the Office of the Secretary, U.S. International Trade Commission, 500 E Street, SW., Room 112, Washington, DC 20436, telephone 202–205–2000. Hearing impaired individuals are advised that information on this matter can be obtained by contacting the Commission's TDD terminal on 202–205–1810. Persons with mobility impairments who will need special assistance in gaining access to the Commission should contact the Office of the Secretary at 202–205–2000. General information concerning the Commission may also be obtained by accessing its internet server at *http://www.usitc.gov.* The public record for this investigation may be viewed on the Commission's electronic docket (EDIS) at *http://www.usitc.gov/secretary/edis.htm.*

FOR FURTHER INFORMATION CONTACT: Vu Q. Bui, Esq., Office of Unfair Import Investigations, U.S. International Trade Commission, telephone (202) 205–2582.

Authority: The authority for institution of this investigation is contained in section 337 of the Tariff Act of 1930, as amended, and in section 210.10 of the Commission's Rules of Practice and Procedure, 19 CFR 210.10 (2006).

Scope of Investigation: Having considered the complaint, the U.S. International Trade Commission, on August 15, 2007, ordered that—

(1) Pursuant to subsection (b) of section 337 of the Tariff Act of 1930, as amended, an investigation be instituted to determine whether there is a violation of subsection (a)(1)(B) of § 337 in the importation into the United States, the sale for importation, or the sale within the United States after importation of certain nitrile rubber gloves by reason of infringement of one or more of claims 1 and 17–19 of U.S. Patent No. Re. 35,616, and whether an industry in the United States exists as required by subsection (a)(2) of § 337;

(2) For the purpose of the investigation so instituted, the following are hereby named as parties upon which this notice of investigation shall be served:

(a) The complainant is—

Tillotson Corporation, d/b/a, Best Manufacturing Company, 579 Edison Street, Menlo, Georgia 30731.

(b) The respondents are the following entities alleged to be in violation of section 337, and are the parties upon which the complaint is to be served:

Cardinal Health, Inc., 7000 Cardinal Place, Dublin, Ohio 43017.

Cardinal Health 200, Inc., 1430 Waukegan Road (MP KB–1A), McGaw Park, Illinois 60085.

Cardinal Health Malaysia 211 Sdn. Bhd., Plot 87, Kampung Jawa 11900, Bayan Lepas, Malaysia.

Henry Schein, Inc., 135 Duryea Road, Melville, New York 11747.

HSI Gloves Inc., 135 Duryea Road, Melville, New York 11747.

Latexx Partners Berhad, Pt5054, Jalan Perusahaan 3, Kamunting, Industrial Estate, 34600 Kamunting, Perak, Darul Ridzuan, Malaysia.

Medtexx Partners Inc., 102 Engle St. FL2, Englewood, New Jersey 07631.

(c) The Commission investigative attorney, party to this investigation, is Vu Q. Bui, Esq., Office of Unfair Import Investigations, U.S. International Trade Commission, 500 E Street, SW., Suite 401, Washington, DC 20436; and

(3) For the investigation so instituted, the Honorable Charles E. Bullock is designated as the presiding administrative law judge.

(4) The Commission has determined to assign this investigation to Judge Bullock, who is the presiding administrative law judge in *Certain Nitrile Gloves*, Inv. No. 337–TA–608, in view of the overlapping subject matter in the two investigations. The presiding administrative law judge is authorized to consolidate Inv. No. 337–TA–608 and this investigation if he deems it appropriate.

Responses to the complaint and the notice of investigation must be submitted by the named respondents in accordance with section 210.13 of the Commission's Rules of Practice and Procedure, 19 CFR 210.13. Pursuant to 19 CFR 201.16(d) and 210.13(a), such responses will be considered by the Commission if received not later than 20 days after the date of service by the Commission of the complaint and the notice of investigation. Extensions of time for submitting responses to the complaint and the notice of investigation will not be granted unless good cause therefor is shown.

Failure of a respondent to file a timely response to each allegation in the complaint and in this notice may be deemed to constitute a waiver of the right to appear and contest the allegations of the complaint and this notice, and to authorize the administrative law judge and the Commission, without further notice to the respondent, to find the facts to be as alleged in the complaint and this notice and to enter an initial determination and a final determination containing such findings, and may result in the issuance of a limited exclusion order or cease and desist order or both directed against the respondents.

Issued: August 16, 2007.

By order of the Commission.

Marilyn R. Abbott,

Secretary.

[FR Doc. E7–16432 Filed 8–21–07; 8:45 am]

BILLING CODE 7020–02–P

DEPARTMENT OF JUSTICE

Federal Bureau of Investigation

[AAG/A Order No. 028–2007]

Privacy Act of 1974; System of Records

AGENCY: Federal Bureau of Investigation, DOJ.

ACTION: Notice to amend system of records.

SUMMARY: The Federal Bureau of Investigation proposes to amend its Terrorist Screening Records System, Justice/FBI–019, maintained by the Terrorist Screening Center, to make several changes to its existing notice. Public comments are invited.

DATES: The Privacy Act requires that the public be given 30 days in which to comment on any new or amended uses of information in a system of records. In addition, the Office of Management and Budget (OMB), which has oversight responsibilities under the Act, and the Congress must be given 40 days in which to review major changes to Privacy Act systems. Therefore, the public, OMB, and the Congress are invited to submit written comments on this revised Privacy Act system of records. Please submit any comments by October 1, 2007.

ADDRESSES: Address all comments to Kenneth P. Mortensen, Deputy Privacy and Civil Liberties Officer, U.S. Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530, facsimile number (202) 616–9627.

FOR FURTHER INFORMATION CONTACT: Kenneth P. Mortensen, (202) 514–3853.

SUPPLEMENTARY INFORMATION: On July 28, 2005, the Department of Justice, Federal Bureau of Investigation (FBI) published a new Privacy Act System of Records notice, the Terrorist Screening Records System (TSRS), Justice/FBI–019, to cover records maintained by the Terrorist Screening Center (TSC), the system owner. See 70 FR 43715. Records in the TSRS include the Terrorist Screening Database (TSDB), records in the Encounter Management Application (EMA) that document the operational support TSC provides to agencies that screen for terrorists (''screening agencies''), and records related to the TSC's internal quality assurance process to ensure the terrorist data is thorough, accurate and current. The TSC also maintains records related to the resolution of terrorist watchlist-related redress complaints.

The TSC now proposes modifications to the system to expand the scope of the system, and to increase the clarity of the notice. The following explains the proposed modifications:

General Changes

The previous system notice used the terms ''terrorist screening'' and ''terrorism screening'' interchangeably to describe the same process. This notice is being modified so that only the term ''terrorism screening'' is used, making it consistent with the language in Homeland Security Presidential Directive 6 (HSPD 6). This system notice also makes use of the term Terrorism Information as defined in section 1016 of the Intelligence Reform and Prevention Act of 2004 (Pub. L. 108–458).

System Location

The current system of records notice for Justice/FBI–019 states that the records are located at the TSC, Federal Bureau of Investigation, Washington, DC. The notice has been amended to reflect that records in Justice/FBI–019 may also be located in secondary locations for system back-up and continuity-of-operations purposes.

Categories of Individuals

The TSC is expanding the categories of individuals covered by this system to cover individuals who are authorized users of the underlying information systems described by this system of records, such as the TSDB and EMA, since audit logs documenting their use will be maintained in connection with the system.

Currently, only TSC personnel can perform queries directly against the TSDB, EMA, and other internal TSC databases. In the future, the TSC plans to operate a query function permitting authorized individuals from screening agencies or entities to access TSC systems directly from an external location and submit search queries. Collection and maintenance of information through audit logs about authorized users will allow the TSC to monitor who uses TSC information systems for what purpose, in order to ensure compliance with applicable laws and policy. Therefore, the TSC is modifying this system of records notice to account for this fact.

Additionally, the TSC is clarifying that this system of records covers all individuals whose names or identifying information is collected to perform a query against TSC information systems, such as TSDB, but who are not necessarily individuals whose information is generally maintained as terrorist information in the TSDB. For example, in certain instances, individuals' names are queried directly against the TSDB or EMA to see if there is a possible record match and, if there is not, their names may be retained in an audit trail that records the activity of authorized users of TSC information systems. The system notice is being modified to make clear that these individuals' information is also included in this system of records.

The TSC is adding a new category to cover individuals who accompany or travel with a person when that person is an actual match to a known or suspected terrorist identity in the TSDB and when the TSC or screening agency or entity identifies that person as such during a terrorism screening process. The TSC collects this information in the course of encounters with known or suspected terrorists. For example, an encounter can include times when an individual was in the car along with a person matching an identity in the TSDB during a traffic stop by state or local law enforcement officers. TSC maintains this information about such individuals in EMA and not in the TSDB, and shares it as appropriate with other agencies for law enforcement and intelligence purposes consistent with the routine uses of this system of records.

Categories of Records

The TSC is adding new categories of records to cover audit logs for TSC systems, and archived records and record histories for the TSDB and other TSC systems.

As discussed above, audit log records allow the TSC to monitor who uses TSC systems for what purpose in order to ensure compliance with applicable laws and policy. A TSDB record history is a log of any previous changes to the current version of a TSDB record.

Archived TSDB records are TSDB records that pertain to individuals who are no longer eligible for inclusion in the TSDB, because those individuals no longer meet the criteria for inclusion in the TSDB as a known or suspected terrorist. The TSC retains these records in an archive that is logically separate from other TSDB data and may be accessed only by a limited number of TSC personnel who have undergone specialized training on the sensitivity of these records and the permissible reasons for access.

Pursuant to TSC policy, archived TSDB records may only be accessed for the following purposes: (1) Redress, (2) litigation, (3) quality assurance (e.g., to determine if a record correction is required to an existing record in a TSC or other agency system), (4) to respond to requests from oversight bodies and auditors, and to perform internal audits, (5) to evaluate TSC performance and data in the event of another terrorist attack or attempted attack, and to support any related investigation, and (6) when access is otherwise required by law (e.g., Freedom of Information Act (FOIA) request). Archived TSDB records are not used or made available for any watchlisting purposes. The search function for the TSDB archive requires that prior to accessing the TSDB archive authorized TSC personnel must identify an approved purpose with information supporting the need for access. This information is maintained in a detailed audit log, which is routinely reviewed by TSC compliance personnel.

Additionally, the TSC is modifying other descriptions of categories of records to clarify the types of information held in the TSC systems.

The TSC is adding language to clarify that records of encounters may include information about individuals who accompany or travel with a person when that person is an actual match to a known or suspected terrorist identity in the TSDB and the TSC or screening agency or entity identifies that person as such during a terrorism screening process.

The TSC is also modifying Item (a) To add ''photograph'' as a specific type of identifying data that may be contained in the TSRS. While a photograph may be considered a biometric, which is already listed in Item (a), TSC is listing photographs as a separate item to ensure clarity.

The TSC is modifying Item (b) By changing the term ''agency'' to ''entity'' to reflect that entities other than a

federal government agency may engage in terrorism screening. Item (b) is also being modified by removing the language ''terrorist encounters'' and replacing it with ''encounters with known or suspected terrorists,'' which is a more precise characterization, because Item (a) in the Categories of Individuals defines the phrase ''known or suspected terrorists.''

The TSC is also modifying Item (c) to make clear that TSRS may also include references to or information from other relevant databases that contain terrorism information, in the event such databases are not considered law enforcement or intelligence databases.

Authority for Maintenance of the System

The TSC is adding the following legal authorities: the National Security Act of 1947, as amended; the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108–458, 18 Stat. 3638 (December 17, 2004); and Executive Order 13388, ''Further Strengthening the Sharing of Terrorism Information to Protect Americans,'' (October 25, 2005). TSC is removing the reference to Executive Order 13356, which has been superseded by Executive Order 13388.

Also, the TSC is adding language to provide notice that in the event that the TSC's continuity-of-operations plans are invoked, the agency that assumes TSC operational functions will have the authority to administer the Terrorist Screening Records System as necessary to carry out those functions and will act consistent with the obligations required by the Privacy Act of 1974 in the maintenance of TSRS as a Privacy Act System of Records.

Purpose Statement

Consistent with the changes discussed above regarding auditing of TSC data systems, the TSC is expanding the purpose of the system of records to clarify that one purpose is to conduct appropriate oversight of the proper use of TSC data systems.

The language in Item (e) Is being modified to add the quoted language below to more accurately reflect TSC's mission, as set forth in HSPD 6, to provide support for private sector screening processes ''that have a substantial bearing on homeland security.''

The language in Item (f) is being modified to remove the word ''agency's'' and insert the word ''authorized'' preceding the term ''screening process'' to more accurately describe the type of screening TSC may perform. The word ''agency'' was removed because not all terrorism screening is necessarily performed by a federal government agency. The word ''authorized'' was added because all terrorism screening processes using TSC data must be authorized by the TSC pursuant to the standard articulated in HSPD 6.

The language in Item (g) Is being changed to add the word ''organizations'' to the list of entities and individuals that may receive information about encounters with known or suspected terrorists. This change is intended to better reflect the ongoing efforts by the federal government to increase sharing of intelligence, law enforcement and terrorism information with the State and local governments, fusion centers, and critical infrastructure owners and operators, consistent with the privacy protections required by the Privacy Act and as articulated in this notice.

The language in Item (h) is being changed by removing the word ''repeatedly'' from the phrase ''to assist persons repeatedly misidentified during a terrorism screening process.'' This change is intended to clarify that an individual does not have to be misidentified more than once for the TSC to act to provide assistance through a redress process or other means. Conforming changes are being made to the notice to remove the word ''repeatedly'' from Routine Uses B, F, and G, and the categories of individuals (Item (d)).

Routine Uses

Routine Use B listed for Justice/FBI–019 permits disclosure of information to various entities in order to, among other things ''provide appropriate notifications of a positive terrorist encounter or a threat related to the encounter.'' The TSC is modifying this language to clarify that the TSC may notify an entity of not only a positive match to the terrorist watchlist, but also a negative or inconclusive match. Also, the TSC is modifying this Routine Use to include ''private sector entities with a substantial bearing on homeland security'' as described in HSPD–6 as potential recipients of information. Finally, the TSC is modifying the language in purpose (2) of this Routine Use to make clear that a positive encounter means an encounter with an individual who is identified in the TSDB, and to clarify purpose (3) of this Routine Use by adding the modifiers ''known or suspected'' to the terms ''terrorist'' and ''threat related to the encounter.''

Routine Use D permits disclosure of information for the development, testing, or modification of information technology systems used or intended to be used during or in support of the screening process, but indicates TSC will use de-identified data whenever possible. The TSC is modifying the language of this Routine Use to clarify that ''de-identified data'' means data that cannot be used to derive an individual's identity and to note that de-identified data will be used to the extent practicable and possible.

Routine Use E permits disclosure of information to various agencies or entities to assist in the coordination of terrorist threat awareness, assessment, analysis, or response. The TSC is modifying this language to include private sector entities in the list of entities that may receive information from TSRS for these purposes. This change is intended to better reflect the ongoing efforts by the federal government to increase sharing of intelligence, law enforcement, terrorism and threat information with State fusion centers and the private sector, such as critical infrastructure and key resource owners and operators, consistent with the privacy protections required by the Privacy Act.

Routine Use H permits disclosure of information in support of authorized audit or oversight operations of the DOJ, including FBI and TSC, or any agency engaged in or providing information used for terrorism screening supported by the TSC. The TSC is modifying this Routine Use to include authorized security operations as a permissible purpose for sharing information, thereby allowing the TSC to disclose information to the investigating entity in the context of a security-related investigation or inquiry, such as a personnel investigation or inquiry into a breach of data security. Additionally, the TSC is expanding the scope of this Routine Use by adding language that would allow disclosure if the subject of the security, audit, or oversight operation was not a Federal agency but an organization or individual that was engaged in or providing information used for terrorism screening that is supported by the TSC. These changes will allow the TSC to disclose information to support any oversight efforts into TSC-related activities.

Routine Use K permits disclosure of information to a governmental entity lawfully engaged in collecting law enforcement, law enforcement intelligence, or national security intelligence information for law enforcement or intelligence purposes. TSC is modifying this Routine Use by changing ''national security intelligence information'' to ''national security information'' and ''national intelligence,'' which are terms defined

by Executive Order 12958, as amended, and the Intelligence Reform and Terrorism Prevention Act amendments to the National Security Act of 1947, respectively. Also, the TSC is specifying counterterrorism as one of the purposes for which information may be disclosed under this Routine Use, which is consistent with TSC's counterterrorism mission.

The Department of Justice previously published a notice modifying all of the Department's systems of records, including TSRS, to include a routine use to permit the disclosure of information to appropriate persons and entities for purposes of response and remedial efforts in the event that there has been a breach of the data contained in the Department's systems of records. See 72 FR 3410 (Jan. 25, 2007). The TSC is adding new Routine Use L to this notice to reflect this change.

Retention and Disposal

Although TSC is a multi-agency organization, the FBI administers TSC. Recently, the FBI obtained approval from the National Archives and Records Administration for its request for records disposition authority for records created and maintained by the TSC. The TSC is modifying this language to provide information on the approved retention periods for TSC records described in Justice/FBI–019. For records maintained in the Terrorist Screening Database (TSDB), active records are maintained for 99 years and inactive (archived) records are maintained for 50 years. Encounter Management Application (EMA) records, which document positive, negative, and inconclusive screening encounters with individuals in the TSDB, are maintained for 99 years. TSC maintains EMA records on negative encounters, i.e., a person who is initially identified as a possible match to a TSDB identity but ultimately determined not to be a match, in order to expedite future screening of those individuals and to support the redress process. Records of redress inquiries and quality assurance matters are maintained for at least six years. Audit logs are maintained for 25 years and records of user audits are maintained for ten years.

Contesting Record Procedures

The TSC is adding language to this section to refer individuals to the TSC's public Web site for additional information on the redress process and the procedures for filing a complaint related to terrorism screening.

Record Source Categories

The TSC is modifying this section to include ''private sector entities engaged in terrorism screening'' as a record source category. This change is being made to reflect that the TSC may receive information for screening from the private sector in support of the TSC's mission, as set forth in HSPD 6, to support ''private sector screening processes that have a substantial bearing on homeland security.''

Public Comments Invited

Public comments are invited on all aspects of the revised system notice, including the retention periods for records and the new categories of individuals and records. See **ADDRESSES** section above for information on how to submit comments.

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

Dated: August 14, 2007.

Lee J. Lofthus,

Assistant Attorney General for Administration.

JUSTICE/FBI–019

SYSTEM NAME:

Terrorist Screening Records System (TSRS).

SECURITY CLASSIFICATION:

Classified, unclassified (law enforcement sensitive).

SYSTEM LOCATION:

Records described in this notice are maintained at the Terrorist Screening Center, Federal Bureau of Investigation, Washington, D.C., and at facilities operated by other government entities for terrorism screening, system back-up, and continuity of operations purposes.

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 who are the subject of queries against TSC information systems;

c. Individuals identified during a terrorism screening process as a possible identity match to a known or suspected terrorist and other individuals who accompany or travel with such individuals;

d. Individuals who are misidentified as a possible identity match to a known or suspected terrorist (''misidentified persons'');

e. Individuals about whom a terrorist watchlist-related redress inquiry has been made; and

f. Individuals whose information is collected and maintained for information system user auditing and security purposes, such as individuals who are authorized users of TSC information systems.

CATEGORIES OF RECORDS IN THE SYSTEM:

a. Identifying information, such as name, date of birth, place of birth, biometrics, photographs, 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, including audit records containing this information;

b. Information about encounters with individuals covered by this system, such as date, location, screening entity, analysis, associated individuals, and results (positive or negative identity match), and, for encounters with known or suspected terrorists only, other entities notified and details of any law enforcement, intelligence, 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, or other relevant databases that may contain terrorism information;

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 and date of birth);

e. For redress matters, 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 matter;

f. Information collected and compiled to maintain an audit trail of the activity of authorized users of TSC information systems, such as user name/ID, date/time, search query and results data, user activity information (e.g., record retrieval, modification, or deletion data), and record numbers; and,

g. Archived records and record histories from the Terrorist Screening Database, Encounter Management Application, and other TSC data systems that are part of the TSRS.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Homeland Security Presidential Directive-6, ''Integration and Use of Screening Information to Protect Against Terrorism'' (Sept. 16, 2003); Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans,'' (October 25, 2005); the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108–458; the National Security Act of 1947, as amended; and 28 U.S.C. 533. In the event that the TSC's continuity-of-operations plans are invoked, the agency that assumes TSC operational functions will have the authority to administer the Terrorist Screening Records System as necessary to carry out those functions.

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 terrorism 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 terrorism information available to support appropriate domestic, and foreign terrorism screening processes, and private-sector screening processes that have a substantial bearing on homeland security.

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 authorized screening process.

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

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

i. To oversee the proper use, maintenance, and security of TSC data systems and TSC personnel.

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, the records or information in this system may be disclosed as a routine use, under 5 U.S.C. 552a(b)(3), in accordance with 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 or private sector entities with a substantial bearing on homeland security and their agents, contractors or representatives, for the following purposes: (1) For use in and in support of terrorism screening authorized by the U.S. Government, (2) to provide appropriate notifications of the results of terrorism screening using information from the Terrorist Screening Database or a threat related to a positive encounter with an individual identified in the Terrorist Screening Database, (3) to facilitate any appropriate law enforcement or other response (e.g., medical and containment response to a biological hazard) to a known or suspected terrorist or a threat related to the encounter, and (4) to assist persons misidentified during a screening process.

C. To any person, 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 terrorism 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 practicable, however, TSC, to the extent possible, will substitute anonymized or de-identified data, such that the identity of the individual cannot be derived from the data.

E. To federal, state, local, tribal, territorial, foreign, multinational agencies or entities, or private sector 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 misidentified during a screening process.

G. To any federal, state, local, tribal, territorial, foreign or multinational agency, task force, or other entity or person that receives information from the U.S. Government for terrorism 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 misidentified during a screening process.

H. To any agency, organization or person for the purposes of (1) performing authorized security, audit, or oversight operations of the DOJ, FBI, TSC, or any agency, organization, or person engaged in or providing information used for terrorism screening that is supported by the TSC, and (2) meeting related reporting requirements.

I. To a former employee of the TSC 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, national security information, national intelligence, or terrorism information for law enforcement, intelligence, or counterterrorism purposes.

L. To appropriate agencies, entities, and persons when (1) the Department of Justice suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department of Justice 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 the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department of Justice's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

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 the records schedule approved by the National Archives and Records Administration. For records maintained in the Terrorist Screening Database, active records are maintained for 99 years and inactive (archived) records are maintained for 50 years. Records of possible encounters with individuals on the Terrorist Screening Database are maintained for 99 years. Records of redress inquiries and quality assurance matters are maintained for at least six years. Audit logs are maintained for 25 years and records of user audits are maintained for ten years.

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 intelligence 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 intelligence 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 intelligence 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 (5 U.S.C. 552a). 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.

Additional information about the redress process and how to file a complaint with a screening agency is available on TSC's Web site at *http://www.fbi.gov/terrorinfo/counterrorism/redress.htm.*

RECORD SOURCE CATEGORIES

Information in this system is obtained from individuals covered by the system, public sources, agencies and private sector entities conducting terrorism 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. E7–16487 Filed 8–21–07; 8:45 am]

BILLING CODE 4410–02–P

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: Application for Continuation of Death Benefit for Student (LS–266). 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 October 22, 2007.

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*. Please use only one method of transmission for comments (mail, fax, or E-mail).

SUPPLEMENTARY INFORMATION:

I. Background

The Office of Workers' Compensation Programs (OWCP) administers the Longshore and Harbor Workers' Compensation Act. The Act provides for continuation of death benefits for a child or certain other surviving dependents after the age of 18 (to age 23) if the dependent qualifies as a student as defined in Section 2 (18) of the Act. Regulation 20 CFR 702.121 addresses the use of forms for the reporting of required information. The LS–266 is submitted by the parent or guardian of the dependent for whom continuation of benefits is sought. The statements contained on the form must be verified by an official of the educational institution. The information is used by the Department of Labor to determine whether a continuation of the benefits is justified. This information collection is currently approved for use through December 31, 2007.

II. Review Focus

The Department of Labor is particularly interested in comments which:

- Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;
- Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;
- Enhance the quality, utility and clarity of the information to be collected; and
- Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submissions of responses.

III. Current Actions

The Department of Labor seeks the approval of the extension of this information collection in order to ensure that eligible dependents may continue to receive benefits to which they are entitled.

Type of Review: Extension.

Agency: Employment Standards Administration.

Title: Application for Continuation of Death Benefits for Student.

OMB Number: 1215–0073.

Agency Number: LS–266.

Affected Public: Individuals or households; Business or other for-profit.

Total Respondents: 43.

Total Annual responses: 43.

Time per Response: 30 minutes.

Estimated Total Burden Hours: 22.

Frequency: On occasion.

Total Burden Cost (capital/startup): $0.

Total Burden Cost (operating/maintenance): $0.

Comments submitted in response to this notice will be summarized and/or included in the request for Office of Management and Budget approval of the information collection request; they will also become a matter of public record.

Dated: August 16, 2007.

Hazel M. Bell,

Acting Chief, Branch of Management Review and Internal Control, Division of Financial Management, Office of Management, Administration and Planning, Employment Standards Administration.

[FR Doc. E7–16533 Filed 8–21–07; 8:45 am]

BILLING CODE 4510–CF–P