Billing Code: 4410-02-P

DEPARTMENT OF JUSTICE

[CPCLO Order No. 012-2012]

Privacy Act of 1974; System of Records

AGENCY: Federal Bureau of Investigation, United States Department of Justice.

ACTION: Notice of a New System of Records.

SUMMARY: Pursuant to the Privacy Act of 1974 (5 U.S.C. 552a), the United States Department of Justice (DOJ), Federal Bureau of Investigation (FBI), proposes to establish a new system of records entitled, the FBI Data Warehouse System, JUSTICE/FBI-022, to cover all FBI data warehouses that have been or are created to manage the information necessary to carry out FBI's national security and criminal justice missions. The FBI is also deleting its Data Integration and Visualization System, JUSTICE/FBI-021," last published at 75 FR 53262 (Aug. 31, 2010), and modified at 75 FR 66131 (Oct. 27, 2010) because this new system duplicates it.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), the public is given a 30-day period in which to comment. Therefore, please submit any comments by [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: The public, Office of Management and Budget (OMB) and Congress are invited to submit any comments to the Department of Justice, ATTN: Privacy Analyst, Office of Privacy and Civil Liberties, Department of Justice, National Place Building, 1331 Pennsylvania Avenue NW., Suite 1000, Washington, DC 20530-0001 or by facsimile at 202-307-0093.

FOR FURTHER INFORMATION CONTACT: Kristin Meinhardt, Assistant General Counsel, Privacy and Civil Liberties Unit, Office of the General Counsel, FBI, 935 Pennsylvania Avenue, NW., Washington, DC 20535-0001, telephone 202-324-3000.

SUPPLEMENTARY INFORMATION:

In an effort to carry out its national security and criminal law enforcement responsibilities, and to more robustly exchange with its partners, the FBI has created data warehouses to maintain information from its own investigative files (currently covered by and maintained in the Central Records System, Justice/FBI-002), public source information, and information lawfully ingested from other government agencies, such as the Departments of Defense, Energy, Homeland Security, State, and Treasury. Data sets ingested into a warehouse from other government agencies have been determined to be responsive to the FBI's missions and particular threats. This SORN will cover all FBI data warehouses, including the Data Mart maintained by the Foreign Terrorist Tracking Task Force (FTTTF), the Investigative Data Warehouse, and the Data Integration and Visualization System.

Data warehouses function as the point of receipt for incoming information and provide repositories where disparate data sets can be compared with each other and with FBI information to provide a more complete picture of potential national security threats or criminal activities. Maintaining the data in warehouses allows users to search across relevant government agency data sets and FBI case information at the same time rather than searching each data set individually. These data warehouses contain much of the same information; however, the FTTTF Data Mart is used primarily to address the FBI's national security mission, IDW facilitates analysis across the major FBI mission areas

(and makes searching selected FBI case information easier) and DIVS provides an enhanced and integrated view of FBI information. Queries of the warehouses can yield results in a matter of minutes, which facilitates analysis and provides information for further examination. Query results are used to set leads for investigations and, in appropriate cases, to prepare analytical products for information sharing.

The extraction of useful information from multiple data sets is the kind of work FBI analysts conduct on a daily basis; being able to do this across multiple data sets maintained in the warehouses increases the speed and efficiency of this work which, in turn, contributes to the FBI's ability more readily and effectively to carry out its national security and law enforcement missions.

Because this system contains law enforcement information, the Attorney General is proposing to exempt this system from certain provisions of the Privacy Act, as permitted by law. 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 has provided a report to OMB and the Congress on this new system of records.

June 19, 2012_____

Date: Nancy C. Libin
Chief Privacy and Civil Liberties Officer
United States Department of Justice

JUSTICE/FBI-022

SYSTEM NAME:

FBI Data Warehouse System.

SECURITY CLASSIFICATION:

Classified and/or unclassified information.

SYSTEM LOCATION:

Records may be maintained at all locations at which the Federal Bureau of Investigation (FBI) operates or at which FBI operations are supported, including: J. Edgar Hoover Bldg., 935 Pennsylvania Avenue, NW., Washington, DC 20535-0001; FBI Academy and FBI Laboratory, Quantico, VA 22135; FBI Criminal Justice Information Services (CJIS) Division, 1000 Custer Hollow Rd., Clarksburg, WV 26306; FBI Records Management Division, 170 Marcel Drive, Winchester, VA 22602-4843; and FBI field offices, legal attaches, information technology centers, and other components as listed on the FBI's Internet website, http://www.fbi.gov. Some or all system information may also be duplicated at other locations where the FBI has granted direct access for support of FBI missions, for purposes of system backup, emergency preparedness, and/or continuity of operations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The following categories of individuals are covered by this system: Individuals who are identified in data maintained in FBI files or obtained by the FBI by authority of law and agreement from other federal, state, local, tribal or foreign government agencies in furtherance of authorized information sharing purposes to carry out the FBI's mission to protect and defend the United States against terrorist and foreign intelligence threats

and to enforce U.S. criminal laws. These individuals consist of the following: subjects, suspects, victims, witnesses, complainants, informants, sources, bystanders, law enforcement personnel, intelligence personnel, other responders, administrative personnel, consultants, relatives, and associates who may be relevant to the investigation or intelligence operation; individuals who are identified in open source information or commercial databases, or who are associated, related, or have a nexus to the FBI's missions; individuals whose information is collected and maintained for information system user auditing and security purposes.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records may contain investigative and/or intelligence information that has been replicated and/or extracted from other FBI systems; obtained from open source or commercial databases; and lawfully collected by the FBI or other government agencies such as the Departments of Defense, Energy, Homeland Security, State, and Treasury. These records include, but are not limited to, biographical information (such as name, alias, race, sex, date of birth, place of birth, social security number, passport number, driver's license, or other unique identifier, addresses, telephone numbers, physical descriptions, and photographs); biometric information (such as fingerprints); financial information (such as bank account number); location; associates and affiliations; employment and business information; visa and immigration information; travel; and criminal and investigative history, and other data that may assist the FBI in fulfilling its national security and law enforcement responsibilities. Records may also contain information collected and compiled to maintain an audit trail of the activity of authorized users of the system, such as user name and ID.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

28 U.S.C. Chapter 33; 18 U.S.C. 2332(b); 28 CFR 0.85; the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act); the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA); the Implementing Recommendations of the 9/11 Commission Act of 2007; 42 U.S.C. 3771; the National Security Act of 1947, as amended; Section 603 of the Intelligence Authorization Act of 1990, the Attorney General's Guidelines for Domestic FBI Operations and numerous other statutes, executive orders, and presidential directives.

PURPOSE(S):

The purpose of the system is to facilitate the FBI's national security and law enforcement missions by establishing centralized data warehouses for the compilation, fusion, storage, and comprehensive analysis of pertinent information that will allow the FBI to develop investigative leads, operational intelligence products and strategic intelligence assessments on new or evolving national security and criminal threats.

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), records or information in this system may be disclosed as a routine use under 5 U.S.C. 552a(b)(3) as noted below.

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

(b.) Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law -- civil, criminal, or regulatory in nature – the relevant records may be referred to the appropriate federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity, that is charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law.

(c.) To a governmental entity lawfully engaged in collecting law enforcement, law enforcement intelligence, or national security intelligence information for such purposes when determined to be relevant by the FBI/DOJ.

(d.) To any person, organization, or governmental entity in order to notify them of a potential terrorist threat for the purpose of guarding against or responding to such threat.

(e.) To an agency of a foreign government or international agency or entity where the FBI determines that the information is relevant to the recipient's responsibilities, dissemination serves the best interests of the U.S. Government, and where the purpose in making the disclosure is compatible with the purpose for which the information was collected.

(f.) To any non-governmental entity, including commercial entities, or nonprofit organizations, that are joint participants with or provide support to the FBI and disclosure is consistent with FBI's law enforcement, national security, or intelligence missions.

(g.) To any entity or individual where there is reason to believe the recipient is or could become the target of a particular criminal activity, conspiracy, or other threat, to the extent the information is relevant to the protection of life, health, or property.

Information may similarly be disclosed to other recipients who have interests to which the threat may also be relevant, or who may be able to assist in protecting against or responding to the threat.

(h.) To persons or entities where there is a need for assistance in locating missing persons, and where there are reasonable grounds to conclude from available information that disclosure would further the best interests of the individual being sought.

(i.) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department 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's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

(j.) To contractors, grantees, experts, consultants, students, or others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Department of Justice, when necessary to accomplish an agency function related to this system of records.

(k.) To the news media or members of the general public in furtherance of a legitimate law enforcement or public safety function as determined by the Department of Justice and, where applicable, consistent with 28 CFR § 50.2. unless it is determined that

release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(l.) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

(m.) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings.

(n.) To such recipients and under such circumstances and procedures as are mandated by federal statute or treaty.

(o.) To a Member of Congress or staff acting upon the Member’s behalf when the Member or staff requests the information on behalf of, and the request of, the individual who is the subject of the record.

(p.) To any agency, organization, or individual for the purposes of performing authorized audit or oversight operations of the Department and meeting related reporting requirements.

(q.) To the National Archives and Records Administration (NARA) for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

(r.) To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing

authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

(s.) To the White House (the President, Vice President, their staffs, and other entities of the Executive Office of the President (EOP)), and, during Presidential transitions, the President-elect and Vice President-elect and their designees for appointment, employment, security, and access purposes compatible with the purposes for which the records were collected by the FBI, e.g., disclosure of information to assist the White House in making a determination whether an individual should be: (1) granted, denied, or permitted to continue in employment on the White House Staff; (2) given a Presidential appointment or Presidential recognition; (3) provided access, or continued access, to classified or sensitive information; or (4) permitted access, or continued access, to personnel or facilities of the White House/EOP complex. System records may also be disclosed to the White House and, during Presidential transitions, to the President-elect and Vice-President-elect and their designees, for Executive Branch coordination of activities that relate to or have an effect upon the carrying out of the constitutional, statutory, or other official or ceremonial duties of the President, President-elect, Vice-President or Vice-President-elect. System records or information may also be disclosed during a Presidential campaign to a major-party Presidential candidate, including the candidate's designees, to the extent the disclosure is reasonably related to a clearance request submitted by the candidate for the candidate's transition team members pursuant

to Section 7601 of the Intelligence Reform and Terrorism Prevention Act of 2004, as amended.

(t.) To complainants and/or victims to the extent deemed necessary by the DOJ to provide such persons with information and explanations concerning the progress and/or results of the investigations or cases arising from the matters of which they complained and/or of which they were a victim.

(u.) To appropriate officials and employees of a federal agency or entity that requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the assignment, detail, or deployment of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit.

(v) To federal, state, local, tribal, territorial, foreign, or international licensing agencies or associations, when the Department determines the information is relevant to the suitability or eligibility of an individual for a license or permit.

(w) To designated officers and employees of state, local, territorial, or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prisoners or detainees, to the extent that the information is relevant to the recipient agency's decision.

(x) To such agencies, entities, and persons as the DOJ deems appropriate and relevant to ensure the continuity of government functions in the event of any actual or

potential disruption of normal government operations. This use encompasses all manner of such situations in which government operations may be disrupted, including: military, terrorist, cyber, or other attacks, natural or manmade disasters, and other national or local emergencies; inclement weather and other acts of nature; infrastructure/utility outages; failures, renovations, or maintenance of buildings or building systems; problems arising from planning, testing or other development efforts; and other operational interruptions. This also includes all related pre-event planning, preparation, backup/redundancy, training and exercises, and post-event operations, mitigation, and recovery.

(y.) To any person or entity, if deemed by the DOJ to be necessary to elicit information or cooperation from the recipient for use by the DOJ in the performance of an authorized law enforcement, national security, or intelligence function.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

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

STORAGE:

Computerized records are stored electronically on hard disk, removable storage devices or other digital media. Some information may be retained in hard copy format and stored in individual file folders and file cabinets with controlled access, and/or other appropriate GSA-approved security containers.

RETRIEVABILITY:

Information is retrieved by name or other identifying information. Some methods of retrieval will not identify an individual but only a set of circumstances that

may lead to the identification of an individual.

SAFEGUARDS:

Records are maintained in secure, restricted areas and are accessed only by authorized personnel. Physical security protections include guarded and locked facilities requiring badges and passwords for access and other physical and technological safeguards (such as role-based access and strong passwords) to prevent unauthorized access. All visitors must be accompanied by authorized staff personnel at all times. Highly classified or sensitive privacy information is electronically transmitted on secure lines and in encrypted form to prevent interception and interpretation. Users accessing system components through mobile or portable computers or electronic devices such as laptop computers, multi-purpose cell phones, and personal digital assistants (PDAs) must comply with the FBI's remote access policy, which requires encryption. All FBI employees receive a complete background investigation prior to being hired. Other persons with authorized access to system records receive comparable vetting. All personnel are required to undergo privacy and annual information security training, and are cautioned about divulging confidential information or any information contained in FBI files. Failure to abide by this provision violates DOJ regulations and may violate certain civil and criminal statutes providing for penalties of fine or imprisonment or both. As a condition of employment, FBI personnel also sign nondisclosure agreements which encompass both classified and unclassified information and remain in force even after FBI employment. Employees who resign or retire are also cautioned about divulging information acquired in their FBI jobs.

RETENTION AND DISPOSAL:

Records in this system are maintained and disposed of in accordance with appropriate authority of the National Archives and Records Administration.

SYSTEM MANAGER AND ADDRESS:

Director, Federal Bureau of Investigation, 935 Pennsylvania Avenue, NW., Washington, DC 20535-0001.

NOTIFICATION PROCEDURE:

Same as "RECORD ACCESS PROCEDURES," below.

RECORD ACCESS PROCEDURES:

The Attorney General has exempted this system of records from the notification, access, and contest procedures of the Privacy Act. These exemptions apply only to the extent that the information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j) and/or (k). Where compliance would not appear to interfere with or adversely affect the purposes of the system, or the overall law enforcement/intelligence process, the applicable exemption (in whole or in part) may be waived by the FBI in its sole discretion.

All requests for access should follow the guidance provided on the FBI's website at http://foia.fbi.gov/requesting_records.html. Individuals may mail, fax, or email a request, clearly marked "Privacy Act Request," to the Federal Bureau of Investigation, Attn: FOI/PA Request, Record/Information Dissemination Section, 170 Marcel Drive, Winchester, VA 22602-4843; Fax: 540-868-4995/6/7; Email: (scanned copy) foiparequest@ic.fbi.gov. The request should include a general description of the records sought and must include either a completed Department of Justice Certification of

Identity Form, DOJ-361, which can be located at the above link, or a letter that has been notarized which includes: the requester's full name, current and complete address, and place and date of birth or be submitted under penalty of perjury of law pursuant to 28 USC 1746. In the initial request the requester may also include any other identifying data that the requester may wish to furnish to assist the FBI in making a reasonable search. The request should include a return address for use by the FBI in responding; requesters are also encouraged to include a telephone number to facilitate FBI contacts related to processing the request. A determination of whether a record may be accessed will be made after a request is received.

CONTESTING RECORD PROCEDURES:

Individuals desiring to contest or amend information maintained in the system should direct their requests according to the Record Access Procedures listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. The envelope and letter should be clearly marked "Privacy Act Amendment Request" and comply with 28 CFR 16.46 (Request for Amendment or Correction of Records). Some information may be exempt from contesting record procedures as described in the section entitled "Exemptions Claimed for the System." An individual who is the subject of a record in this system may amend those records that are not exempt. A determination whether a record may be amended will be made at the time a request is received.

RECORD SOURCE CATEGORIES:

Information provided by Federal, state, local, tribal, territorial, and foreign law enforcement agencies; agencies of the U.S. foreign intelligence community and military

community; open sources, such as broadcast and print media, publicly-available and commercial data bases; and individuals, corporations, and organizations.

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), (4)(G), (H) and (I), (5) and (8); (f); and (g) of the Privacy Act. The exemptions will be applied only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a (j) and/or (k). Rules are being promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and are published in today's Federal Register. In addition, the DOJ will continue in effect and assert all exemptions claimed under 5 U.S.C. 552a(j) or (k) (or other applicable authority) by an originating agency from which the DOJ obtains records, where one or more reasons underlying an original exemption remain valid. Where compliance with an exempted provision could not appear to interfere with or adversely affect interests of the United States or other system stakeholders, the DOJ in its sole discretion may waive an exemption in whole or in part; exercise of this discretionary waiver prerogative in a particular matter shall not create any entitlement to or expectation of waiver in that matter or any other matter. As a condition of discretionary waiver, the DOJ in its sole discretion may impose any restrictions deemed advisable by the DOJ (including, but not limited to, restrictions on the location, manner, or scope of notice, access or amendment).

[FR Doc. 2012-16823 Filed 07/09/2012 at 8:45 am; Publication Date: 07/10/2012]