Billing Code 4410-02-P

DEPARTMENT OF JUSTICE

CPCLO Order No. 007-2016

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, and Office of Management and Budget (OMB) Circular No. A-130, the Federal Bureau of Investigation (FBI), a component of the United States Department of Justice (Department or DOJ), proposes to establish a new system of records titled, "FBI Insider Threat Program Records (ITPR)," JUSTICE/FBI-023, to establish certain capabilities to detect, deter, and mitigate threats by FBI personnel including, but not limited to, employees, Joint Task Force Members, contractors, detailees, assignees, and interns, with authorized access to FBI facilities, information systems, or Classified information. FBI personnel assigned to the FBI Insider Threat Prevention and Detection Program (ITPDP) will use the system to facilitate management of insider threat inquiries and activities associated with inquiries and referrals; identify potential threats to FBI resources and information assets; track referrals of potential insider threats to internal and external partners; and provide statistical reports and meet other insider threat reporting requirements. The FBI is concurrently issuing a Notice of Proposed Rulemaking to exempt this system of records

from certain provisions of the Privacy Act elsewhere in this Federal Register. For an overview of the Privacy Act, see: *https://www.justice.gov/opcl/privacy-act-1974*.

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, OMB, and Congress are invited to submit any comments to the U.S. Department of Justice, ATTN: Privacy Analyst, Office of Privacy and Civil Liberties, National Place Building, 1331 Pennsylvania Avenue NW., Suite 1000, Washington, DC 20530-0001, or by facsimile at 202-307-0693. To ensure proper handling, please reference the above CPCLO Order No. on your correspondence.

FOR FURTHER INFORMATION CONTACT: Richard R. Brown, Federal Bureau of Investigation, Assistant General Counsel, Privacy and Civil Liberties Unit, Office of the General Counsel, J. Edgar Hoover Building, 935 Pennsylvania Avenue NW., Washington, DC 20535-0001, telephone (202) 324-3000.

SUPPLEMENTARY INFORMATION: The FBI has created a system of records, known as the FBI Insider Threat Program Records (ITPR), to manage insider threat matters within the FBI. Presidential Executive Order (E.O.) 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, issued October 7, 2011, required Federal agencies to establish an insider threat detection and prevention program to ensure the security of Classified networks and the responsible sharing and safeguarding of Classified information consistent with appropriate protections for privacy and civil liberties. This system of records has been established to enable the FBI to implement the

requirements of E.O. 13587, to meet operating capability requirements as defined by the *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* (Nov. 21, 2012), and to fulfill responsibilities under DOJ Order 0901, *Insider Threat* (Feb. 12, 2014).

The Presidential Memorandum – *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* (Nov. 21, 2012) states that an insider threat is the threat that any person with authorized access to any United States Government resources, to include personnel, facilities, information, equipment, networks or systems, will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities. The FBI ITPR may include information lawfully obtained by the FBI from any FBI, DOJ, or United States Government component, from other domestic or foreign government entities, or obtained from private entities, which is necessary to identify, analyze, or resolve insider threat matters. All FBI employees are cleared for access to handle Classified information.

In accordance with Privacy Act requirements of 5 U.S.C. 552a(r), the Department of Justice has provided a report to OMB and to Congress on this new system of records.

_____ _____

September 2, 2016

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
Department of Justice

JUSTICE/FBI-023

SYSTEM NAME:

FBI Insider Threat Program Records (ITPR).

SYSTEM CLASSIFICATION:

This system includes both Classified and 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 22602-4843; and FBI field offices, legal attaches, information technology centers, and other components as listed on the FBI's Internet Website, *https://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 categories of individuals covered by this system are persons with authorized access to FBI facilities, information systems, or Classified information, including but not limited to present and former FBI employees, Joint Task Force Members, contractors, detailees, assignees, and interns.

CATEGORIES OF RECORDS IN THE SYSTEM:

An insider threat is defined as the threat that any person with authorized access to any FBI resource, to include personnel, facilities, information, equipment, networks, or systems may use his/her authorized access, wittingly or unwittingly, to do harm to the security of the United States, including damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of FBI resources or capabilities. *See* Presidential Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* (Nov. 21, 2012). Records in the ITPR system consist of information necessary to identify, analyze, or resolve insider threat matters. Such records and information may include or be derived from, but are not limited to:

A. All relevant counterintelligence and security databases and files, including personnel security files, polygraph examination reports, facility access records, security violation files, travel records, foreign contact reports, and financial disclosure filings.

B. All relevant Unclassified and Classified network information generated by Information Assurance elements, including, but not limited to, personnel usernames and aliases, levels of network access, audit data, unauthorized use of removable media, print logs, and other data needed for clarification or resolution of an insider threat concern.

C. All relevant Human Resources databases and files including, but not limited to: personnel files, payroll and voucher files, outside work and activities requests, disciplinary files, and personal contact records, as may be necessary for resolving or clarifying insider threat matters.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Executive Order (E.O.) 12968, *Access to Classified Information*, issued August 2, 1995, 60 FR 40245 (Aug. 7, 1995), as amended by E.O. 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, issued June 30, 2008, 73 FR 38103 (July 2, 2008); E.O. 13526, *Classified National Security Information*, issued December 29, 2009, 75 FR 707 (Jan. 5, 2010); and E.O. 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, issued October 7, 2011, 76 FR 63811 (Oct. 13, 2011); and Presidential Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* (Nov. 21, 2012). DOJ Order 901, *Insider Threat* (Feb. 12, 2014), also directs the head of each Department Component to implement DOJ policy and minimum standards issued pursuant to this policy and in coordination with the DOJ ITPDP and "[p]romulgate additional Component guidance, if needed, to reflect unique mission requirements consistent with meeting the minimum standards and guidance issued pursuant to this policy."

PURPOSE(S):

To monitor, detect, deter, and/or mitigate FBI insider threats. The FBI has established the FBI ITPDP and this system of records in order to implement the requirements of E.O. 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information* (Oct. 7, 2011), and the *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* (Nov. 21, 2012). These authorities require agencies

with access to Classified information to establish certain capabilities for detecting, deterring, and/or mitigating insider threats, including: accessing, gathering, integrating, assessing, and sharing information and data derived from offices across the organization for a centralized analysis, reporting, and response; monitoring user activity on Classified computer networks controlled by the federal government; evaluating personnel security information; and establishing procedures for insider threat response actions, such as inquiries, to clarify or resolve insider threat matters.

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), relevant information contained in this system of records may be disclosed as a routine use, under 5 U.S.C. 552a(b)(3), in accordance with the 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 at 66 FR 33558 (June 22, 2001), and amended at 70 FR 7513 (Feb. 14, 2005), and 72 FR 3410 (Jan. 25, 2007). In addition, relevant information contained in this system of records may be disclosed as a routine use, under 5 U.S.C. 552a(b)(3), under the circumstances or for the purposes described below, to the extent such disclosures are compatible with the purposes for which the information was collected:

A. Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law – criminal, civil, 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 charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.

B. 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.

C. 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.

D. 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.

E. 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 to the extent the information is relevant to the protection of life, health, or property.

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

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

H. 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 FBI 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.

I. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the FBI 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.

J. 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.

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

L. 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.

M. To any agency, organization, or individual for the purposes of performing authorized audit or oversight operations of the FBI and meeting related reporting requirements.

N. 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.

O. To a former employee of the FBI for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable FBI or Department of Justice 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.

P. 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.

Q. To complainants and/or victims to the extent necessary 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.

R. 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.

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

T. 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.

U. To such agencies, entities, and persons as is necessary 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.

V. To any person or entity, if necessary to elicit information or cooperation from the recipient for use by the FBI 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:

Records in this system are stored on paper and/or in electronic form. Electronic records are stored in enterprise information technology platforms and networks, databases and/or on hard disks, removable storage devices or other electronic media. Paper records may be stored in individual file folders and file cabinets with controlled access, or other appropriate GSA-approved security containers. Classified information is stored in accordance with applicable legal, administrative, and other requirements.

RETRIEVABILITY:

Information in this system may be retrieved by an individual's name, user ID, email address, Social Security number, unique employee identifier, as well as by use of key word search terms, including the names of persons with whom covered individuals have interacted or to whom they have been linked.

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 capacity.

RETENTION AND DISPOSAL:

Records in this system are maintained and destroyed in accordance with applicable schedules and procedures issued or approved by 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) 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 *https://www.fbi.gov/services/records-management/foipa*. Individuals may mail, fax or email a request, clearly marked "Privacy Act Access 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. 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. Some information may be exempt from contesting record procedures as described in the **EXEMPTIONS CLAIMED FOR THE SYSTEM** paragraph. 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 may be provided by individuals covered by this system, the FBI, DOJ and United States Government components, other domestic and foreign government entities, or obtained from private entities.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Attorney General has exempted this system of records from subsection (c)(3) and (4); (d)(1), (2), (3) and (4); (e)(1), (2), and (3); (e)(4) (G), (H) and (I); (e)(5) and (8); (f) and (g) of the Privacy Act. These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j) or (k). Rules are being promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c), and (e) and have been published in today's Federal Register. In addition, the DOJ will continue in effect and claim 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 claim remain valid. Where compliance with an exempted provision could not appear to interfere with or adversely affect interests of the United States or other stakeholders, the DOJ in its sole discretion may waive an exemption in whole or in part; exercise of the discretionary waiver prerogative in a particular matter shall not create any entitlement to or expectations 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. 2016-22410 Filed: 9/16/2016 8:45 am; Publication Date: 9/19/2016]