Billing Code 4410-NW

DEPARTMENT OF JUSTICE

[CPCLO Order No. 001-2017]

Privacy Act of 1974; System of Records

AGENCY: United States Department of Justice.

ACTION: Notice of a New System of Records.

SUMMARY: Pursuant to the Privacy Act of 1974 and Office of Management and Budget (OMB) Circular No. A-108, notice is hereby given that the Department of Justice (Department or DOJ) proposes to add a new DOJ system of records titled, "DOJ Insider Threat Program Records (ITPR)," JUSTICE/DOJ-018. In the Federal Register of May 31, 2017, the Department is rescinding its notice of an FBI system of records notice titled "FBI Insider Threat Program Records," JUSTICE/FBI-023, published on September 19, 2016. This new DOJ-wide system of records will cover the records previously claimed under JUSTICE/FBI-023. This new system of records establishes certain Department-wide capabilities to detect, deter, and mitigate insider threats. Insiders are defined to include any person with authorized access to any United States Government resource to include personnel, facilities, information, equipment, networks, or systems. DOJ personnel assigned to the DOJ 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 DOJ 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. Elsewhere in this Federal Register, DOJ is concurrently issuing a Notice of Proposed Rulemaking to exempt JUSTICE/DOJ-018 from certain provisions of the Privacy Act, and withdrawing the notice of proposed rulemaking regarding for JUSTICE/FBI-023, issued in CPCLO Order No. 008-2016.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this notice is effective upon publication, subject to a 30-day period in which to comment on the routine uses, described below. Please submit any comments by [INSERT DATE 30 DAYS AFTER DATE OF 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, by facsimile at 202-307-0693, or email at *privacy.compliance@usdoj.gov*. To ensure proper handling, please reference the above CPCLO Order No. in your correspondence.

FOR FURTHER INFORMATION CONTACT: Laurence Reed, DOJ Insider Threat Program Manager, United States Department of Justice, Insider Threat Prevention and Detection Program, 145 N Street NE, Washington, DC, 20002, 202-357-0165, *itp@usdoj.gov*.

SUPPLEMENTARY INFORMATION: The DOJ has created a system of records, known as the DOJ Insider Threat Program Records (ITPR), to manage insider threat matters within the DOJ. 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, requires 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 DOJ 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). For an overview of the Privacy Act, see: *https://www.justice.gov/opcl/privacy-act-1974*.

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 resource, 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. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

The DOJ ITPR may include information lawfully obtained by the DOJ from any United States Government component, from other domestic or foreign government entities, or from private entities, which is necessary to identify, analyze, or resolve insider threat matters.

In accordance with the 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.

_____May 19, 2017_____
Date

_____
Peter A. Winn,
Acting Chief Privacy and Civil Liberties Officer,
United States Department of Justice.

JUSTICE/DOJ-001

SYSTEM NAME AND NUMBER:

DOJ Insider Threat Program Records (ITPR), JUSTICE/DOJ-001.

SYSTEM CLASSIFICATION:

This system includes both Classified and Unclassified information.

SYSTEM LOCATION:

Records may be maintained at all locations at which the Department of Justice (DOJ) operates or at which DOJ operations are supported, including: Robert F. Kennedy Main Justice Department Building, 950 Pennsylvania Avenue NW, Washington, DC 20530-0001; Federal Bureau of Investigation J. Edgar Hoover Building, 935 Pennsylvania Avenue NW, Washington, DC 20535-0001; Bureau of Alcohol, Tobacco, Firearms and Explosives, 99 New York Avenue NE, Washington DC 20226; and other DOJ components, field offices, information technology centers, and other locations as listed on the DOJ and DOJ components' Internet websites, including *https://www.justice.gov.* Some or all system information may also be duplicated at other locations where the DOJ has granted direct access for support of DOJ missions, for purposes of system backup, emergency preparedness, and/or continuity of operations.

SYSTEM MANAGER AND ADDRESS:

DOJ Insider Threat Program Manager, United States Department of Justice, Insider Threat Prevention and Detection Program, 145 N Street NE, Washington, DC, 20002, 202-357-0165, *itp@usdoj.gov*.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

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); 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) OF THE SYSTEM:

This system of records is used by DOJ employees and contractors to monitor, detect, deter, and/or mitigate DOJ insider threats. The DOJ has established the DOJ 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 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.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The categories of individuals covered by this system are DOJ insiders, defined as any person with authorized access to any DOJ resource to include personnel, facilities, information, equipment, networks or systems. Such persons include but are not limited to present and former DOJ employees, members of joint task forces under the purview of the DOJ, contractors, detailees, assignees, interns, visitors, and guests.

CATEGORIES OF RECORDS IN THE SYSTEM:

An insider threat is defined as the threat that any person with authorized access to any DOJ resource, to include personnel, facilities, information, equipment, networks or systems, will use his/her authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of DOJ resources or capabilities. *See* Presidential

Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* (Nov. 21, 2012). The Minimum Standards state that Agency heads shall direct Counterintelligence, Security, Information Assurance, Human Resources, and other relevant organizational components to securely provide insider threat program personnel regular, timely, and, if possible, electronic access to the information necessary to identify, analyze, and resolve insider threat matters. Such access and information includes, but is not limited to, the following:

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; and

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.

Records in the ITPR system consist of information necessary to identify, analyze, or resolve insider threat matters, including the information listed above or information derived from such information.

RECORD SOURCE CATEGORIES:

Information may be provided by individuals covered by this system, the DOJ or other United States Government components, other domestic and foreign government entities, or obtained from private entities.

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), all or a portion of the records or information contained in this system of records may be disclosed as a routine use pursuant to 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. 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 DOJ.

B. 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.

C. 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.

D. To any person or entity if 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.

E. Violations of Law, Regulation, Rule, Order, or Contract. If any system record, alone, or in conjunction with other information, indicates a violation or potential violation of law (whether civil or criminal), regulation, rule, order, or contract, the pertinent record may be disclosed to the appropriate entity (whether federal, state, local, joint, tribal, foreign, or international) that is charged with the responsibility of investigating, prosecuting, implementing and/or enforcing such law, regulation, rule, order, or contract.

F. Complainants and Victims. 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 victims.

G. Courts or Adjudicative Bodies. To a court, grand jury, or administrative or adjudicative body, in matters in which (a) the DOJ or any DOJ employee in his or her official capacity, (b) any DOJ employee in his or her individual capacity where the Department of Justice has agreed to represent the employee, or (c) the United States, is or could be a party to the litigation, is likely to be affected by the litigation, or has an official interest in the litigation, and disclosure of system records has been determined by the DOJ to be arguably relevant, or by the adjudicator to be relevant, to the litigation. Similar disclosures may be made in the situations stated above related to assistance provided to the Federal Government by non-DOJ employees (see Routine Use J).

H. Parties. To an actual or potential party to litigation or his or her attorney or authorized representative for the purpose of negotiating or discussing such matters as settlement of the case or matter, plea bargaining, or informal discovery proceedings, in matters in which the DOJ has an official interest and in which the DOJ determines records in the system to be arguably relevant.

I. Appropriate Disclosures to the Public. 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 DOJ (e.g., to assist in locating fugitives; to provide notifications of arrests; to provide alerts, assessments, or similar information on potential threats to life, health, or property; or to keep the public appropriately informed of other law enforcement or DOJ matters or other matters of legitimate public interest) where disclosure could not reasonably be expected to constitute an unwarranted invasion of personal privacy. (The availability of information in pending criminal or civil cases will be governed by the provisions of 28 CFR 50.2.)

J. Non-DOJ Employees. To contractors, grantees, experts, consultants, students, or others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records.

K. To designated officers and employees of state, local (including the District of Columbia), 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.

L. 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.

M. The White House. 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 DOJ, 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 be disclosed also 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.

N. Former Employees. To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, local, tribal, or territorial government entity or professional licensing authority, in accordance with applicable DOJ regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the DOJ requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility. (Such disclosures will be effected under procedures established in 28 CFR 16.300– 301 and DOJ Order 2710.8C, including any future revisions.)

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

P. Members of Congress. To a Member of Congress or a person on his or her staff acting on the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

Q. National Archives and Records Administration (NARA) Records Management. To the National Archives and Records Administration (NARA) for

purposes of records management inspections and such other purposes conducted under the authority of 44 U.S.C. 2904 and 2906.

R. To appropriate agencies, entities, and persons when (1) DOJ suspects or has confirmed that there has been a breach of the system of records; (2) DOJ has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DOJ's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

S. To another Federal agency or Federal entity, when DOJ determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

T. To such agencies, entities, or 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.

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

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

W. As Mandated by Law. To such recipients and under such circumstances and procedures as are mandated by Federal statute, treaty, or other source of applicable law.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

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.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

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.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records in this system are maintained and destroyed in accordance with applicable schedules and procedures issued or approved by NARA.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records are maintained in secure, restricted areas and are accessed only by personnel who have a need for the records in the performance of their duties and have been authorized to access them. 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 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 DOJ's remote access policy, which requires encryption. All DOJ 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 DOJ 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, DOJ personnel also sign nondisclosure agreements which encompass, as appropriate, Classified and Unclassified information and remain in force even after DOJ employment. Employees who resign or retire are also cautioned about divulging information acquired in their DOJ capacity.

RECORD ACCESS PROCEDURES:

The Attorney General has exempted this system of records from the notification, access, amendment, 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 DOJ in its sole discretion.

A request for access to a record from this system of records must be submitted in writing and comply with 28 CFR part 16, and should be sent to the Office of Information Policy, 1425 New York Avenue NW, Suite 11050, Washington, DC 20530-0001. The envelope and letter should be clearly marked "Privacy Act Access Request." The request should include a general description of the records sought, and must include the requester's full name, current address, and date and place of birth. The request must be signed and dated and either notarized or submitted under penalty of perjury. While no specific form is required, requesters may obtain a form (Form DOJ-361) for use in certification of identity from the FOIA/Privacy Act Mail Referral Unit, Justice Management Division, United States Department of Justice, 950 Pennsylvania Avenue

NW, Washington, DC 20530–0001, or from the Department's Web site at *https://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/cert_ind.pdf*.

CONTESTING RECORD PROCEDURES:

The Attorney General has exempted this system of records from the notification, access, amendment, 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 DOJ in its sole discretion.

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.

NOTIFICATION PROCEDURES:

Same as the "**RECORD ACCESS PROCEDURES**," above.

EXEMPTIONS PROMULGATED 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 this 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 does 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 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).

HISTORY:

None.

[FR Doc. 2017-11445 Filed: 6/2/2017 8:45 am; Publication Date: 6/5/2017]