Billing Code: 4410-58-P

DEPARTMENT OF JUSTICE

[CPCLO Order No. 002-2018]

Privacy Act of 1974; Systems of Records

AGENCY: United States Department of Justice, Office of Inspector General.

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 Office of Inspector General (OIG), a component within the United States Department of Justice (DOJ or Department), is publishing a new system of records notice titled "Data Analytics Program Records System," JUSTICE/OIG-006. OIG proposes to establish this system of records to assist with the performance of audits, investigations, and reviews, and to accommodate the requirements of the Digital Accountability and Transparency Act of 2014 (DATA Act).

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this notice is applicable upon publication, subject to a 30-day period in which to comment on the routine uses, described below. 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 by mail to the United States Department of Justice, Office of Privacy and Civil Liberties, ATTN: Privacy Analyst, National Place Building, 1331 Pennsylvania Avenue, NW, Suite 1000, Washington, DC 20530; by facsimile at 202-307-0693; or by email at

privacy.compliance@usdoj.gov. To ensure proper handling, please reference the above CPCLO Order No. on your correspondence.

FOR FURTHER INFORMATION CONTACT: William Blier, General Counsel, Office of the General Counsel, Office of the Inspector General, Department of Justice, 950 Pennsylvania Avenue, NW, Washington, DC 20530, (202) 514-3435.

SUPPLEMENTARY INFORMATION: Under the Inspector General Act of 1978, as amended, Inspectors General, including the DOJ Inspector General, are responsible for conducting, supervising, and coordinating audits and investigations relating to programs and operations of the Federal agency for which their office is established to recognize and mitigate fraud, waste, and abuse. This system of records facilitates OIG's performance of its statutory responsibility by implementing a data analytics (DA) program to assist with the performance of OIG audits, investigations, and reviews, and accommodate the requirements of the DATA Act, Pub. L. 113–101, 128 Stat. 1146.

The DA program will provide OIG: timely insights from the data already stored in DOJ databases that OIG has legal authorization to access and maintain; the ability to monitor and analyze data for patterns and correlations that signal wasteful, fraudulent, or abusive activities impacting Department performance and operations; the ability to find, acquire, extract, manipulate, analyze, connect, and visualize data; the capability to manage vast amounts of data; the ability to identify significant information that can improve decision quality; and the ability to mitigate risk of waste, fraud, and abuse. The DA program will also allow the OIG to obtain technology to develop risk indicators that can analyze large volumes of data and help focus OIG's efforts to combat waste, fraud, and abuse. OIG intends to use statistical and mathematical techniques to identify areas to

conduct audits and identify activities that may indicate whether an investigation is warranted. The information maintained within this system of records will be limited to only information that OIG has legal authorization to collect and maintain as part of its responsibility to conduct, supervise, and coordinate audits and investigations of Department programs and operations to recognize and mitigate fraud, waste, and abuse.

Pursuant to 5 U.S.C. 552a(b)(12), records maintained in this system of records may be disclosed to a consumer reporting agency without the prior written consent of the individual to whom the record pertains. Such disclosure will only be made in accordance 31 U.S.C. 3711(e). In accordance with 5 U.S.C. 552a(r), the Department has provided a report to OMB and Congress on this new system of records.

Dated: March 15, 2018.

_____

Katherine Harman-Stokes,
Deputy Director,
Office of Privacy and Civil Liberties,
United States Department of Justice.

JUSTICE/OIG-006

SYSTEM NAME AND NUMBER:

Data Analytics Program Records System, JUSTICE/OIG-006.

SECURITY CLASSIFICATION:

Classified and Controlled Unclassified Information.

SYSTEM LOCATION:

Access to these electronic records includes all Department locations that the Department's Office of Inspector General (OIG) operates or that support OIG operations, including but not limited to, 1425 New York Avenue, Washington, DC 20005. Some or all system information may also be duplicated at other locations where the Department has granted direct access to support OIG operations, system backup, emergency preparedness, and/or continuity of operations. To determine the location of particular Data Analytics Program Records System records, contact the system manager, whose contact information is listed in the "SYSTEM MANAGER(S)" paragraph, below.

SYSTEM MANAGER(S):

Director, Office of Data Analytics, Office of the Inspector General, Department of Justice, 1425 New York Avenue, NW, Suite 10008, Washington, DC 20530, telephone: 202-353-7493.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Inspector General Act of 1978, as amended, 5 U.S.C. App. 3; DATA Act, 31 U.S.C. 3521 *et seq.*; Inspector General Empowerment Act of 2016, Pub. L. 114-317, 130 Stat. 1595.

PURPOSE(S) OF THE SYSTEM:

The system will use data that the OIG has the legal authority to collect and maintain to perform advanced statistical and mathematical techniques. The goal of this work is to identify anomalies in the data that indicate fraudulent or inappropriate activity. The work can also improve audit quality by helping to identify specific areas for OIG attention. The product of this work can be used by the OIG to identify areas to conduct audits or activities that may indicate that an investigation is warranted.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The categories of individuals covered by the system include current and former DOJ employees; DOJ contractors; recipients of DOJ grants awards or funds, whether direct or indirect; parties to DOJ cooperative agreements; arrestees, fugitives, prisoners, and other individuals under custody of the United States Marshals Service (USMS); prisoner health care service providers under the USMS Managed Health Care Contract; and individuals currently or formerly under the custody of the Attorney General and/or the Director of the Federal Bureau of Prisons (BOP), including those individuals under custody for criminal and civil commitments.

CATEGORIES OF RECORDS IN THE SYSTEM:

In connection with its investigative duties to recognize and mitigate fraud, waste, and abuse relating to Department programs and operations, OIG already maintains records on the following categories of individuals that will be maintained in this system of records:

A. Individuals or entities who are or who have been the subject of investigations conducted by the OIG, including current and former employees of the DOJ; current and former consultants, contractors, and subcontractors with whom the Department and other

federal agencies have contracted and their employees; grantees to whom the Department has awarded grants and their employees; and such other individuals or entities whose association with the Department relates to alleged violation(s) of the Department's rules of conduct, the Civil Service merit system, and/or criminal or civil law, which may affect the integrity or physical facilities of the Department.

B. Individuals who are or have been witnesses, complainants, or informants in investigations conducted by the OIG.

C. Individuals or entities who have been identified as potential subjects of or parties to an OIG investigation.

D. Individuals currently or formerly under the custody of the Attorney General and/or BOP and/or USMS.

In connection with its broader oversight responsibilities relating to programs and operations of the Department to recognize and mitigate fraud, waste, and abuse, OIG will maintain the following categories of records:

A. All categories of records relevant to JUSTICE/DOJ-001 – Accounting Systems for the Department of Justice, 69 FR 31406, 71 FR 142, 75 FR 13575, 82 FR 24147.

B. All categories of records relevant to JUSTICE/OJP-004 – Grants Management Information System 53 FR 40526, 66 FR 8425, 82 FR 24147.

C. All categories of records relevant to JUSTICE/USM-005 – U.S. Marshals Service Prisoner Processing and Population Management-Prisoner Tracking System (PPM-PTS), 72 FR 33515, 519, 82 FR 24151, 163.

D. All categories of records relevant to JUSTICE/BOP-005 – Inmate Central Records System, 67 FR 31371, 77 FR 24982, 81 FR 22639, 82 FR 24147.

E. All categories of records relevant to JUSTICE/JMD-003 – Department of Justice Payroll System, 69 FR 107, 72 FR 51663, 82 FR 24151, 158.

F. Department data files required by the DATA Act, including but not limited to sampling of the spending data submitted in accordance with the DATA Act.

G. Department charge card data (for example, travel, purchase, fleet and integrated card transactions).

H. Federal contract actions whose estimated value is $3,000 or more, that may be $3,000 or more, and every modification to such contract actions regardless of dollar value.

I. Single Audit results (for example, results of a financial or compliance audit of recipients of Federal funds) and related Federal award information.

J. BOP medical claim adjudication data.

K. Department employee worker's compensation payment data.

RECORD SOURCE CATEGORIES:

The records within this system of records are sourced from the following: the subjects of investigations; individuals with whom the subjects of investigations are associated; current and former Department officers and employees; Federal, State, local, foreign, and territorial law enforcement and non-law enforcement agencies; private citizens; witnesses; informants; public source materials; medical product and service providers; medical claim processing companies; financial institutions managing Department credit card and payroll information; and the system managers, or individuals

acting on a system manager's behalf, for the DOJ systems of records that OIG has legal authorization to collect and maintain as part of its responsibility to conduct, supervise, and coordinate audits and investigations of Department programs and operations to recognize and mitigate fraud, waste, and abuse.

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 another Federal Office of the Inspector General or Federal, state, local, foreign, territorial, or tribal unit of government for the purposes of identifying fraud, waste, abuse, or improper payments related to Federal programs, employees, contractors, grantees, inmates, or beneficiaries. These activities will be conducted under the authorities in the Inspector General Act of 1978, as amended, and the DATA Act.

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

C. 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.

D. 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 investigation or case arising from the matters of which they complained and/or of which they were a victim.

E. To any person or entity that the OIG has reason to believe possesses information regarding a matter within the jurisdiction of the OIG, to the extent deemed to be necessary by the OIG in order to elicit such information or cooperation from the recipient for use in the performance of an authorized activity.

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

G. 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 in informal discovery proceedings.

H. To the news media and the public, including disclosures pursuant to 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. To contractors, grantees, experts, consultants, students, and 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.

J. To designated officers and employees of Federal, 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 does occupy 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 and necessary to the recipient agency's decision.

K. 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.

L. To a former employee of the Department for purposes of: responding to an official inquiry by a Federal, state, local, tribal, territorial, or foreign 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.

M. To federal, state, local, territorial, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

N. 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 at the request of, the individual who is the subject of the record.

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

P. To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Department (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 the Department efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

Q. To another Federal agency or Federal entity, when the Department 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.

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

S. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are stored in an electronic form in a framework of computer systems that allows distributed processing of data sets across clusters of computers. Records are stored securely in accordance with applicable executive orders, statutes, and agency implementing recommendations. Electronic records are stored in databases and/or on hard disks, removable storage devices, or other electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records in this system of records can be retrieved by name or other identifiers, including but not limited to: the surnames of subjects, witnesses, and/or complainants of an OIG complaint or investigation; social security account number; address; telephone number; OIG-assigned case numbers; taxpayer identification number; health care provider; assigned number given to an individual in custody with USMS; inmate register number; alien registration number; assigned DOJ charge card information; geo-code location (for example, physical addresses converted into geographic coordinates on a map); organizational name; employee payroll identifier; and Data Universal Numbering System (DUNS number).

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records in this system are retained and disposed of in accordance with the schedule approved by the Archivist of the United States, Job Number N1-060-09-025.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Both electronic and paper records are safeguarded in accordance with appropriate laws, rules, and policies, including Department and OIG policies. The records are protected by physical security methods and dissemination/access controls. Direct access is controlled and limited to approved personnel with an official need for access to perform their duties. Paper files are stored: (1) in a secure room with controlled access; (2) in locked file cabinets; and/or (3) in other appropriate GSA approved security containers. Protection of information technology systems is provided by physical, technical, and administrative safeguards. Records are located in a building with restricted access and are kept in a locked room with controlled access or are safeguarded with approved encryption technology. The use of multifactor authentication is required to access electronic systems. Information may be transmitted to routine users on a need to know basis in a secure manner and to others upon verification of their authorization to access the information and their need to know.

Security personnel conduct periodic vulnerability scans using DOJ-approved software to ensure security compliance and security logs are enabled for all computers to assist in troubleshooting and forensic analysis during incident investigations. Users of individual computers can only gain access to the data by a valid user identification authorization and authentication method.

RECORD ACCESS PROCEDURES:

All requests for access to records must be in writing and should be addressed to the System Manager listed above. The envelope and letter should be clearly marked "Privacy Act Access Request." Alternatively, requests can be emailed to *oigfoia@usdoj.gov*. The request must describe the records sought in sufficient detail to enable Department personnel to locate them with a reasonable amount of effort. The request must 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 either notarized or submitted under penalty of perjury. Some information may be exempt from the access provisions as described in the "EXEMPTIONS PROMULGATED FOR THE SYSTEM" paragraph, below. An individual who is the subject of a record in this system of records may access those records that are not exempt from access. A determination whether a record may be accessed will be made at the time a request is received.

Although no specific form is required, you may obtain forms for this purpose from the FOIA/Privacy Act Mail Referral Unit, United States Department of Justice, 950 Pennsylvania Avenue NW, Washington, DC 20530, or on the Department of Justice website at *https://www.justice.gov/oip/oip-request.html*.

More information regarding the Department's procedures for accessing records in accordance with the Privacy Act can be found at 28 CFR part 16 subpart D, "Protection of Privacy and Access to Individual Records Under the Privacy Act of 1974."

CONTESTING RECORD PROCEDURES:

Individuals seeking to contest or amend records maintained in this system of records must direct their requests to the address indicated in the "RECORD ACCESS

PROCEDURES" paragraph, above. All requests to contest or amend records must be in writing and the envelope and letter should be clearly marked "Privacy Act Amendment Request." All requests must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record. Some information may be exempt from the amendment provisions as described in the "EXEMPTIONS PROMULGATED FOR THE SYSTEM" paragraph, below. An individual who is the subject of a record in this system of records may contest or amend those records that are not exempt. A determination of whether a record is exempt from the amendment provisions will be made after a request is received.

More information regarding the Department's procedures for amending or contesting records in accordance with the Privacy Act can be found at 28 CFR 16.46, "Requests for Amendment or Correction of Records."

NOTIFICATION PROCEDURES:

Individuals may be notified if a record in this system of records pertains to them when the individuals request information utilizing the same procedures as those identified in the "RECORD ACCESS PROCEDURES" paragraph, above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

The Attorney General plans to exempt this system from subsections (c)(3) and (4); (d); (e)(1), (2), (3), (5) and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). In addition, the system has been exempted from subsections (c)(3), (d), and (e)(1) of the Privacy Act, pursuant to 5 U.S.C. 552a(k)(1) and (k)(2). The exemptions will be applied only to the extent that the information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and/or (k)(2). Rules are in the process

of being promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c), and (e), and will be published in the Federal Register.

HISTORY:

None.

[FR Doc. 2018-05656 Filed: 3/27/2018 8:45 am; Publication Date: 3/28/2018]