Billing Code: Billing Code 4410-NW

DEPARTMENT OF JUSTICE

[CPCLO Order No. 012-2019]

Privacy Act of 1974; Systems 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 United States Department of Justice (DOJ or Department), proposes to develop a new system of records titled "DOJ Identity, Credential, and Access Service Records System," JUSTICE/DOJ-020. DOJ proposes to establish this system of records as a part of the Department's Enterprise Identity, Credential, and Access Management services, which will serve as a central and authoritative identity management data repository for DOJ identity information. JUSTICE/DOJ-020 combines user information from various data sources to provide a centralized and authoritative identity governance solution.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this system of records 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 AFTER DATE OF 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, Two Constitution Square, 145 N. Street NE, Suite 8W.300, 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: Nickolous Ward, DOJ Chief Information Security Officer, (202) 514-3101, 145 N. Street NE, Washington, DC 20530.

SUPPLEMENTARY INFORMATION:

In accordance with the Federal Information Security Modernization Act of 2014, DOJ is responsible for complying with policies and procedures issued by the OMB and implementing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of DOJ information and information systems. 44 U.S.C. 3554. OMB policy requires agencies to properly identify, credential, monitor, and manage subjects that access Federal resources, including information, information systems, facilities, and secured areas. *See* Office of Management and Budget M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management (May 21, 2019). DOJ's compliance with the Federal Identity, Credential, and Access Management (ICAM) policy is essential to meeting DOJ's information security and privacy risk management responsibilities.

JUSTICE/DOJ-020 will serve as DOJ's central and authoritative ICAM record repository for DOJ Identity Services, a program that allows DOJ management and information system staff to monitor and manage enterprise identities (e.g., DOJ employees, contractors, mission or business partners, devices, etc.) to DOJ information and information systems. DOJ will collect and maintain identity records in order to manage enterprise accounts across DOJ components and business units within DOJ. Such activities can include, but are not limited to, account request, creation, modification, removal, and annual account recertification across DOJ components and business units within DOJ.

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: November 1, 2019.

_____

_____

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

JUSTICE/DOJ-020

SYSTEM NAME AND NUMBER:

DOJ Identity, Credential, and Access Service Records System, JUSTICE/DOJ-020.

SECURITY CLASSIFICATION:

The system is unclassified.

SYSTEM LOCATION:

Records will be maintained electronically at one or more of the Department's data centers, including, but not limited to, one or more of the Department's Core Enterprise Facilities (CEF), including, but not limited to, the Department's CEF East, Clarksburg, WV 26306, or CEF West, Pocatello, ID 83201. Records within this system of records may be transferred to a Department-authorized cloud service provider within the Continental United States. Access to these electronic records may occur at any location at which the DOJ, Justice Management Division, Office of the Chief Information Officer, Cybersecurity Services Staff (DOJ CSS) operates or where DOJ CSS operations are supported, including the Two Constitution Square building, 145 N. Street NE, Washington, DC 20530. Some or all of the information in the system may be duplicated at other locations where the Department has granted direct access to support DOJ CSS operations, system backup, emergency preparedness, and/or continuity of operations. To determine the location of a particular record maintained in this system of records, contact the system manager, whose contact information is listed in the ''SYSTEM MANAGER(S)'' paragraph, below.

SYSTEM MANAGER(S):

DOJ Chief Information Security Officer, (202) 514-3101, 145 N. Street NE, Washington, DC 20530.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Federal Information Security Modernization Act of 2014, 44 U.S.C. 3551 *et seq.*; 44 U.S.C 3504; Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors (Aug. 2015); FIPS 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors (Aug. 2013); OMB Circular A-130, Managing Information as a Strategic Resource (July 2016); OMB Memorandum M-10-28, Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (July 6, 2010); OMB Memorandum M-14-03, Enhancing the Security of Federal Information and Information Systems (Nov. 18, 2013); OMB Memorandum M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management (May 21, 2019).

PURPOSE(S) OF THE SYSTEM:

DOJ establishes this system of records to support the information and information systems serving as the central and authoritative identity management data repository for DOJ enterprise identities. This system of records will allow management and IT staff to monitor and manage user access to DOJ information systems across departments and business units within DOJ. Such activities include, but are not limited to, account requests, creation, modification, removal, and annual account recertification.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

All DOJ employees and contractors, DOJ information system users, and

individuals granted access to DOJ information.

CATEGORIES OF RECORDS IN THE SYSTEM:

User identity information, such as name and associated identities; user identification information (e.g., username); home and/or work address(es); personal and/or work email address(es); personal and/or work telephone numbers; duty city, county, state, and/or station information; Social Security Number; sponsorship information; employee identification information; employment and enrollment information; assigned government furnished equipment information (mobile device identifiers); and biometric identifiers (e.g., fingerprints and high-resolution photographs).

Identity investigation and adjudication information.

Assigned card information, such as associated identity information; card activated date; card delivered date; credential and certificate information; card reissue request and replacement information; card replacement status; card reprint request status; card suspended and termination dates; and user account flags.

Training information, including but not limited to, date training is required to be completed, date training was assigned, and date training was completed.

Access management information, such as information system roles held by an identity.

RECORD SOURCE CATEGORIES:

Information will feed into this system of records from a number of source systems: USAccess (including records in GSA/GOVT-7, Personal Identity Verification Identity Management System (PIV IDMS), last published in full at 71 FR 56983 (Sept. 28, 2006)); National Finance Center (NFC); Justice Security Tracking and Adjudication

Record System (JSTARS) (including records in JUSTICE/DOJ-006, Personnel Investigation and Security Clearance Records for the Department of Justice, last published in full at 67 FR 59864 (Sept. 24, 2002)); and LearnDOJ.

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) 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 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.

(C) To any person or entity that the DOJ has reason to believe possesses information regarding a matter within the jurisdiction of the DOJ, to the extent deemed to be necessary by the DOJ in order to elicit such information or cooperation from the

recipient for use in the performance of an authorized activity.

(D) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when DOJ 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.

(E) 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.

(F) 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.

(G) 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.

(H) 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 and necessary to the recipient agency's decision.

(I) 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.

(J) 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.

(K) 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.

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

(M) 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.

(N) 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's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

(O) 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.

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

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

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

All records in this system of records are maintained electronically and are in compliance 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 can be retrieved through the system portal or through a connecting system via a connector or application program interface (API). The records are searchable using First Name, Last Name, Email Address, Social Security Number, Birth Date, Components, Process Status, and Person ID.

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, General Records Schedule 3.2, for records created and maintained by Federal agencies related to protecting the security of information technology systems and data, and responding to computer security incident.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

The system meets all DOJ requirements for authorization to operate per DOJ Order 0904, Cybersecurity Program. Specifically, information in this system is maintained in accordance with applicable laws, rules, and policies on protecting individual privacy. The servers storing electronic data and the backup tapes stored onsite are located in locked rooms with access limited to authorized agency personnel. Backup tapes stored offsite are maintained in accordance with a government contract that requires adherence to applicable laws, rules, and policies. Internet connections are protected by multiple firewalls. 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 forensics analysis during incident investigations. Users of individual computers can only gain access to the data by a valid

user identification and authentication.

RECORD ACCESS PROCEDURES:

All requests for access to records must be in writing and should be mailed to the Justice Management Division, ATTN: FOIA Contact, Robert F. Kennedy Department of Justice Building, Room 1111, 950 Pennsylvania Avenue NW, Washington, DC 20530, sent by facsimile to (202) 616–6695, or emailed to *JMDFOIA@usdoj.gov*. The envelope and letter should be clearly marked "Privacy Act Access Request." 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.

Although no specific form is required, requesters may obtain sample request forms 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: *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, with the envelope and letter 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.

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:

None.

HISTORY:

None.

[FR Doc. 2019-24246 Filed: 11/6/2019 8:45 am; Publication Date: 11/7/2019]