Billing Code: 4410-18

DEPARTMENT OF JUSTICE

[CPCLO Order No. 004-2018]

Privacy Act of 1974; Systems of Records

AGENCY: United States Department of Justice, Office of Justice Programs, National Institute 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 Office of Justice Programs (hereinafter OJP), a component within the United States Department of Justice (DOJ or Department), proposes to develop a new system of records titled National Missing and Unidentified Persons System, JUSTICE/OJP—015. The OJP proposes to establish this system of records to improve the quantity and quality of—and appropriate access to—data on missing persons, unidentified decedents, and unclaimed decedents, in a centralized repository.

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. 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 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, or by facsimile at 202-307-0693, or email at

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

FOR FURTHER INFORMATION CONTACT: Charles Heurich, Senior Physical Scientist, National Institute of Justice, Office of Justice Programs, 810 7th Street, NW, Washington, DC 20531, Charles.Heurich@usdoj.gov, 202-616-9264.

SUPPLEMENTARY INFORMATION: The National Institute of Justice's National Missing and Unidentified Persons System (NamUs) houses records and information in a centralized system regarding cases of missing persons, unidentified persons (decedents), and unclaimed persons (decedents), and makes certain information available, based on access privileges, to the general public, law enforcement professionals, coroners, and medical examiners to help solve such cases. 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 16, 2018.

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

SYSTEM NAME AND NUMBER:

National Missing and Unidentified Persons System (NamUs), JUSTICE/OJP—015

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

Office of Justice Programs, 810 7th Street, NW, Washington, DC 20531

SYSTEM MANAGER(S):

Point of Contact: Charles Heurich, Charles.Heurich@usdoj.gov, National Institute of Justice, Office of Investigative and Forensic Sciences, 810 7th Street, NW, Washington, DC 20531

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Title I of the Omnibus Crime Control and Safe Streets Act of 1968 (sections 201 and 202); Homeland Security Act of 2002 (section 232); and 28 U.S.C. 530C.

PURPOSE(S) OF THE SYSTEM:

The National Missing and Unidentified Persons System (NamUs) houses records and information regarding cases of missing persons, unidentified decedents, and unclaimed decedents, and makes appropriate information available to the general public and law enforcement professionals to help solve such cases.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Missing persons and registered users of the system, including registered law enforcement personnel, coroners, medical examiners, and members of the public, and although not covered by the Privacy Act, unidentified decedents and unclaimed decedents (named but no next of kin).

CATEGORIES OF RECORDS IN THE SYSTEM:

Missing person case information, unidentified decedent case information, unclaimed decedent case information, and administrative data for registered users. Case information that is available to the general public may include, but is not limited to, case numbers, name, demographic information (such as age, gender, race/ethnicity, height, and weight), last known location, date of last contact, physical description, clothing and accessories, vehicle and transportation information, investigating agency information, and photographs. Professional users have access to additional case information that may include, but is not limited to, date of birth, place of birth, Social Security number (SSN) (for missing persons cases only), DNA availability (specifically whether a DNA sample exists and was submitted to a laboratory, and if so, which laboratory and whether the lab results are available —neither DNA profiles nor DNA testing results are housed within the NamUs system), fingerprint records, dental records, and family contact information. Administrative data for registered users includes, but is not limited to, name, address, email address, telephone number, work title (for professional users only) and agency name (for professional users only).

RECORD SOURCE CATEGORIES:

Professional users and members of the public provide information for the system:

- Professional Users: Law Enforcement, Medical Examiners/Forensic Pathologists, Coroners, Medicolegal Investigators, DNA Specialists, Fingerprint Examiners, Forensic Odontologists, Forensic Anthropologists, Regional System Administrators (OJP grantees), NamUs Staff (i.e. staff that do not have the ability to grant access to other users or have final approval

over edits or changes), and National Center for Missing and Exploited Children (NCMEC) Liaisons.

- Public Users: members of public including family members of missing persons, victim advocates, media representatives, and other members of the public who have registered as users in the NamUs application.

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:

1. To any criminal, civil, or regulatory law enforcement or medicolegal authority (whether federal, state, local, territorial, tribal, foreign, or international), where the information is relevant to the recipient entity's law enforcement or medicolegal responsibilities.
2. To a governmental entity lawfully engaged in collecting law enforcement, law enforcement intelligence, medicolegal, or national security intelligence information for such purposes when determined to be relevant by the DOJ.
3. 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.

4. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.
5. 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.
6. To the news media and members of the general public, 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.
7. 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.
8. 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 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.

9. 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.
10. To former employees 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 Department regulations; or facilitating communications with former employees 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.
11. 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.
12. 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.
13. 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.
14. 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.

15. 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.
16. To any agency, organization, or individual for the purposes of performing authorized audit and oversight operations of the DOJ and meeting related reporting requirements.
17. 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 in this system are stored in electronic form for use in a computer environment.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Information in this system may be retrieved by personal identifier, including but not limited to, an individual's name, case number, physical description, and other unique case information metadata, such as scars, marks, and tattoos.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

The records will be maintained in a secure manner within the NamUs information technology system until disposition. The retention period for the NamUs system is pending; until the National Archives and Records Administration approves the retention and disposal schedule, records will be treated as permanent.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Internet connections are protected by multiple firewalls. Information technology security personnel conduct periodic vulnerability scans using DOJ-approved software to ensure security compliance and security logs are enabled for all DOJ computers that access the system to assist in troubleshooting and forensic analysis during incident investigations. For access to sensitive information that is not published for public access, users of the system can only gain access to the data based on their access privileges and by a valid user identification and password. Access to the data in the system is further limited by the user's assigned role within the system. All communications between users and the system are protected by secure communication protocol that provides confidentiality and integrity of the transmitted data. The system leverages Federal Risk and Authorization Management Program (FedRAMP) compliant cloud service infrastructure with security controls including physical safeguards appropriate for a

system categorized as "moderate" under applicable Federal Information Security Modernization Act of 2014 (FISMA)-related information technology standards.

RECORD ACCESS PROCEDURES:

All requests for access to records must be in writing and should be addressed to the Government Information Specialist, Office of Justice Programs, Department of Justice, Room 5400, 810 7th Street, NW, Washington, DC 20531 or FOIAOJP@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, 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 Web site at *http://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" section, 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.

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" section, above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

[FR Doc. 2018-05971 Filed: 3/27/2018 8:45 am; Publication Date: 3/28/2018]