



DEPARTMENT OF JUSTICE

[CPCLO Order No. 006-2020]

Privacy Act of 1974; Systems of Records

AGENCY: Office of Justice Programs, United States Department of Justice.

ACTION: Notice of a New System of Records.

SUMMARY: Pursuant to the Privacy Act of 1974, Office of Management and Budget (OMB) Circular No. A-108, and 34 U.S.C. 10109(e), notice is hereby given that the Office of Justice Programs (OJP) proposes to develop a new system of records titled Justice Grants System (JustGrants) (JUSTICE/OJP-016) on behalf of itself, the Office of Community Oriented Policing Services (COPS), and the Office on Violence Against Women (OVW). OJP, COPS, and OVW are the three grant-making components of the United States Department of Justice (DOJ or Department). OJP, COPS, and OVW will use JustGrants to manage the planning, reviewing, awarding, modifying, monitoring, and closing out of DOJ grant awards and payment programs (such as the State Criminal Alien Assistance Program (SCAAP) and the Bullet Proof Vest Program (BVP)). JustGrants provides authorized internal users with the capability to effectively run queries on various data elements, review and score applications, generate award documents for successful applicants, approve awards, obligate award funds, and monitor the performance of award recipients. JustGrants also allows authorized internal users to maintain files on unsuccessful applicants and to update, modify, and maintain files for past and current award recipients. Finally, applicants for, and recipients of, federal grant funding from OJP, COPS, and OVW will be able to use JustGrants to manage the full lifecycle of the DOJ grants or payment programs with which they are involved, including applying for, accepting, modifying, monitoring, reporting on, and closing out of the grants or programs.

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 by mail to the United States Department of Justice, Office of Privacy and Civil Liberties, ATTN: Privacy Analyst, 145 N Street NE, Suite 8W.300, Washington, DC 20002; by facsimile at 202-307-0693; or by email at *privacy.compliance@usdoj.gov*. To ensure proper handling, please reference the above CPCLC Order No. on your correspondence.

FOR FURTHER INFORMATION CONTACT: Maria Swineford, Business Manager, Office of the Assistant Attorney General, Office of Justice Programs, 810 7th Street NW, Washington, DC 20531, *Maria.Swineford@usdoj.gov*, (202) 616-0109.

SUPPLEMENTARY INFORMATION:

JustGrants will replace and consolidate two systems of records, Grants Management Information System (GMS) [JUSTICE/OJP-004] and COPS's NexGen [JUSTICE/COPS-003], which are currently used by OJP, OVW, and COPS. JustGrants is designed to provide a uniform and flexible information platform that is simple to use, in order to promote continuous improvement in DOJ's grant and payment programs processes.

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 disclosures will only be made in accordance with 31 U.S.C. 3711(e).

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

Dated: December 9, 2020.

Peter Winn,

Acting Chief Privacy and Civil Liberties Officer,

United States Department of Justice.

JUSTICE/OJP-016

SYSTEM NAME AND NUMBER:

Justice Grants System (JustGrants), JUSTICE/OJP-016

SECURITY CLASSIFICATION:

The system is unclassified.

SYSTEM LOCATION:

Records in this system are maintained at the following locations: Office of Justice Programs (OJP); 810 7th Street NW, Washington, DC 20531; and with the following cloud service providers: Pega Cloud for Government, Pegasystems, Inc., 1 Rogers Street, Cambridge, MA 02142; Socrata Data Platform, 255 South King Street, Suite 1100, Seattle, WA 98104; Amazon Web Services (AWS) GovCloud, 13200 Woodland Park Road, Herndon, VA 20171; and AWS US East/West, 12900 Worldgate Drive, Herndon, VA 20170. The cloud computing service providers and their location may change from time to time, and this document may not reflect the most current information available. To confirm information about the current cloud computing service provider, please contact OJP through the

OJP service desk at email address *OJP.ITservicedesk@ojp.usdoj.gov*.

SYSTEM MANAGER(S):

Bryce Mitchell, Division Director, Enterprise Application Development Division, Office of the Chief Information Officer, Office of Justice Programs, 810 7th Street NW, Washington, DC 20531, *Bryce.Mitchell@usdoj.gov*, (202) 514-2412.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

28 U.S.C. 530C; 44 U.S.C. 3101; 31 U.S.C. 3512(b)-(c); 34 U.S.C. 10109(e); 34 U.S.C. 10442 and 34 U.S.C. 10444.

PURPOSE(S) OF THE SYSTEM:

JustGrants supports the grant making, grant management, performance reporting, and payment program processing of DOJ's three grant-making components, whose mission is to improve the nation's capacity to prevent and reduce crime, strengthen the criminal and juvenile justice systems, advance public safety through community policing, improve responses to violence against women, reduce crime and juvenile delinquency, support law enforcement officer safety and wellness, and serve the needs of crime victims.

Authorized DOJ internal users will use the system to effectively run queries on various data elements, review and score applications, generate award documents for successful applicants, approve awards, obligate award funds, and monitor the performance of awards. DOJ users will also use the system to maintain files on unsuccessful applicants and update, modify, and maintain files on past and current award recipients. Applicants for, and recipients of, federal funding from DOJ's three grant-making components will use this system to manage the full grants or payment programs lifecycle, including applying for, accepting, modifying, monitoring, reporting on, and closing out of DOJ grant awards or programs.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Current and former applicants; recipients and sub-recipients of DOJ grants and payment programs; peer reviewers; DOJ personnel and contractors; DOJ consultants or fellows; and other individuals will be granted access to the system as permitted by the Privacy Act and pursuant to the routine uses in this notice.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system will maintain business contact information (e.g., email address, phone number, address of business) for applicants, recipients (including any sub-recipients at any tier), and DOJ personnel; performance information for grant recipients (including consultants or fellows); other personal information of applicants and recipients (e.g., date

of birth or age, education or employment information, military service information); government assigned identifiers of applicants and recipients (e.g., Originating Agency Identifier (ORI) numbers, Data Universal Number System (DUNS) numbers, System for Award Management (SAM) numbers, award or application numbers, tax identification numbers, vendor identification numbers, driver's license numbers, alien registration numbers, and passport numbers); applicant and financial information of applicants and recipients (e.g., salary data, financial accounts, credit card information, income, debts, taxpayer information); and system administrative/audit data relating to recipients and DOJ personnel (e.g., user ID, passwords, IP address, date/time of access). The system will maintain information regarding the grant programs for which applicants have applied and the final disposition of their applications (funded or denied funding). The system will maintain information on sub-awards and procurement contracts under the awards and sub-awards. The system will also maintain statistical information on the number of applicants that applied for programs each fiscal year; the number of applicants funded and denied funding for each fiscal year; the total number of awards made by DOJ for each fiscal year; the number of years the same award recipients received funding from the DOJ; and the dollar amounts of the awards and the associated duration of award obligations.

RECORD SOURCE CATEGORIES:

The JustGrants System is comprised of two subsystems: the Dynamic Case Management (DCM) and Data Management, Reporting, and Analytics (DMRA) systems. Information maintained in the JustGrants system of records will originate from a number of sources including, but not limited to: applicants, recipients, sub-recipients, COPS NexGen, OJP Grants Management System, the System for Award Management (SAM.GOV), GRANTS.GOV, DOJ's Unified Financial Management System (UFMS), DOJ's Identity,

Credential, and Access Service Records System (DOJ DIAMD)(JUSTICE/DOJ-020), and U.S. Department of Treasury's Automated Standard Application for Payments (ASAP).

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. Where a record, either alone or in conjunction with other information, may be relevant to investigating 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.

2. 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.

3. 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.

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

5. To the news media and the public, including but not limited to disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case or matter would constitute an unwarranted invasion of personal privacy. While disclosures under 28 CFR 50.2 are in connection with a civil or criminal proceeding, disclosures under this routine use may also pertain to administrative proceedings as well as investigations of federal employee misconduct prejudicial to the interests of members of the public.

6. 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.

7. To a former employee of the DOJ for 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.

8. 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.

9. 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.

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

11. To another Federal agency or Federal entity, when the 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.

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

13. 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 JustGrants are stored in electronic format in the OJP cloud platforms. Records are stored securely in accordance with applicable federal laws, regulations, Department directives, and guidance.

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 retrievable by global search features such as recipient or applicant organizational name; recipient or applicant authorized representative name; application number; award number; ORI number; DOJ employee or contract name; email addresses; physical addresses; user identification numbers; unique identification numbers; SAM Registration numbers; Unique Entity Identifiers; and financial accounting identification.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records in this system are retained and disposed of in accordance with the National Archives and Records Administration, General Records Schedule 1.2: “Grant and Cooperative Agreement Records” for records created by Federal agency program offices

responsible for managing grants and cooperative agreements such as program announcements, application files, case files and similar or related records, state plans, and final products or deliverables. Financial transaction records maintained in this system are retained and disposed of in accordance with General Records Schedule 1.1, Financial Management and Reporting Records.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

This 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 system leverages Cloud Service Providers that maintain an authority to operate in accordance with applicable laws, rules, and policies, including Federal Risk and Authorization Management Program (FedRAMP) requirements.

Backup information will be 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 users identification and authentication.

RECORD ACCESS PROCEDURES:

All requests for access to records must be in writing and should be addressed to the component that manages the relevant award:

For COPS Office Awards: COPS FOIA Officer, Office of Community Oriented Policing Services; 145 N Street NE; Washington, DC 20530

For OJP Awards: OJP FOIA Officer; Office of Justice Programs; Office of the General Counsel; 810 7th Street, NW; Rm. 5400; Washington, DC 20531

For OVW Awards: OVW FOIA Officer; Office on Violence Against Women; 145 N Street NE; Suite 10W.121; Washington, DC 20530

The envelope and letter should be clearly marked "Privacy Act Access Request." The request must describe the records sought in sufficient detail to enable DOJ 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 website at <https://www.justice.gov/oip/oip-request.html>.

More information regarding the DOJ'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.

More information regarding the DOJ’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. 2020-27696 Filed: 12/15/2020 8:45 am; Publication Date: 12/16/2020]