

United States Department of Justice (DOJ)

Office of Justice Programs (OJP)



Privacy Impact Assessment for the U.S. Department of Justice Grants System (JustGrants)

Issued by:
Maureen Henneberg
Deputy Assistant Attorney General
Senior Component Official for Privacy
Office of Justice Programs

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: [February 23, 2021]

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

The Office of Justice Programs (OJP), a component within the United States Department of Justice (DOJ or Department), proposes to develop a new information system known as the Justice Grants System (JustGrants). OJP, the Office of Community Oriented Policing Services (COPS Office), and the Office on Violence Against Women (OVW) will use JustGrants for grant management. JustGrants will replace both OJP and OVW's Grants Management System (GMS), and the COPS Office's grants management system, NexGen.

The Department's use of JustGrants will enable continuous improvement to DOJ's grant and payment program processes, in order to keep pace with technological advancement. OJP, the COPS Office, and OVW internal users will use JustGrants to manage grant and payment program planning, conduct application review, manage awards, modify, monitor, and close out DOJ grant applications, awards, and/or payment programs, such as the State Criminal Alien Assistance Program and the Bullet Proof Vest Program. Members of the public will also leverage JustGrants to apply for grants and payment programs.

Section 2: Purpose and Use of the Information Technology

2.1 *Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.*

JustGrants supports the grant making, grant management, performance reporting, and payment program processes of DOJ's three grant-making components to effectively promote their missions: 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.¹ JustGrants will enable continuous improvement in the administration of these components' grant and payment programs in a more unified and streamlined manner.

OJP, the COPS Office, and OVW will use JustGrants to collect, maintain, and disseminate the information required to manage DOJ's grant and payment programs. For instance, Department users will use the system to maintain and run queries on various data elements, to maintain, review, and score applications, and to generate and maintain award documents for successful applicants, approve awards, obligate award funds, and monitor the performance of federal awards. Department users will also maintain files in JustGrants for unsuccessful applicants and update, modify, and maintain files in the system for past and current award recipients.

¹ OJP's Office of Audit, Assessment, and Management (OAAM) is responsible for establishing and maintaining a modern, automated system for managing all information relating to the grants made under grant programs administered by OJP and the COPS Office. 34 U.S.C. § 10109(e). OVW is participating in JustGrants pursuant to its authorities under the Violence Against Women Office Act, 34 U.S.C. §§ 10442-10445.

Applicants for, and recipients of federal funding from DOJ’s three grant-making components may include both individuals and organizations. Correspondingly, external users of JustGrants are individuals who may either be individual applicants and recipients, or representatives of organizations that are applicants and recipients. External users will use JustGrants to manage their grant or payment program lifecycle. This includes applying for, accepting, modifying, monitoring, reporting on, and closing out DOJ grant awards or payment programs. External users must register with the System for Award Management (SAM.gov) and the U.S. Department of Treasury’s Automated Standard Application for Payments (ASAP) to facilitate the grant or payment program lifecycle operations.

The JustGrants System is comprised of the Dynamic Case Management (DCM) and Data Management, Reporting, and Analytics (DMRA) systems. DCM serves as the main grant case management system and is built on a Pegasystems, Inc. cloud platform for governments. DMRA performs functions related to data reporting and analytics for DOJ’s grant management process, programmatic assessments, and data calls (examples include responses to FOIA requests, audits, and Congressional inquiries). Information maintained in JustGrants will come from a number of sources including, but not limited to: applicants, recipients, sub-recipients, registered SAM.GOV users, GRANTS.GOV, DOJ’s NexGen system, DOJ’s Grants Management System, DOJ’s Unified Financial Management System (UFMS), ASAP, and DOJ’s Identity, Credential, and Access Service Records System (DOJ DIAMD) (JUSTICE/DOJ-020).

2.2 *Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)*

Authority		Citation/Reference
X	Statute	28 U.S.C. § 530C 31 U.S.C. § 3512(b)-(c) 44 U.S.C. § 3101 34 U.S.C. § 10109(e) (OJP and COPS Office) 34 U.S.C. §§ 10442-10445 (OVW)
	Executive Order	
	Federal Regulation	
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 *Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are*

provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to “other” any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
<i>Example: Personal email address</i>	X	B, C and D	<i>Email addresses of members of the public (US and non-USPERs)</i>
Name	X	A, B, and C	<ul style="list-style-type: none"> • First name • Middle name • Last name
Date of birth or age			
Place of birth			
Gender			
Race, ethnicity or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)	X	C	<ul style="list-style-type: none"> • Tax Identification Number (TIN)
Driver’s license			
Alien registration number	X	C	<ul style="list-style-type: none"> • Applicants to the State Criminal Alien Assistance Program application will provide an alien identification number (A-number)
Passport number	X	C	<ul style="list-style-type: none"> • Passport numbers are often used as federal identifiers
Mother’s maiden name			
Vehicle identifiers			
Personal mailing address	X	A, B, and C	<ul style="list-style-type: none"> • May be collected for grantees, applicants, and others involved in the grant making process.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Personal e-mail address	X	A, B, and C	<ul style="list-style-type: none"> • May be collected for grantees, applicants, and others involved in the grant making process.
Personal phone number	X	A, B, and C	<ul style="list-style-type: none"> • May be collected for grantees, applicants, and others involved in the grant making process.
Medical records number			
Medical notes or other medical or health information			
Financial account information	X	C	<ul style="list-style-type: none"> • Bank account • Other financial information (e.g. income)
Applicant information	X	C	<ul style="list-style-type: none"> • Catalog of Federal Domestic Assistance (CFDA) Number • Congressional districts as an applicant identifier • SAM.gov registration number • Originating Agency (ORI) number • Unique inmate identifier number (if applicable) • Financial accounting identifier
Education records			
Military status or other information			
Employment status, history, or similar information	X	C	<ul style="list-style-type: none"> • Employer Identification Number (EIN) • Consultant or SME resumes
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A and B	<ul style="list-style-type: none"> • Consultant or fellow personnel records

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information	X	C	<ul style="list-style-type: none"> Dun and Bradstreet number (DUNS#) Vendor identification number
Location information, including continuous or intermittent location tracking capabilities			
<i>Biometric data:</i>			
- Photographs or photographic identifiers			
- Video containing biometric data			
- Fingerprints			
- Palm prints			
- Iris image			
- Dental profile			
- Voice recording/signatures			
- Scars, marks, tattoos			
- Vascular scan, e.g., palm or finger vein biometric data			
- DNA profiles			
- Other (specify)			
<i>System admin/audit data:</i>			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- User ID	X	A, B, and C	
- User passwords/codes	X	A, B, and C	
- IP address	X	A, B, and C	
- Date/time of access	X	A, B, and C	
- Queries run	X	A, B, and C	
- Content of files accessed/reviewed			
- Contents of files			
Other (please list the type of info and describe as completely as possible): Audit data identifying the user and date if changes are made to certain data fields.	X	A, B, and C	• Audit data

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax	X	Online	X
Phone		Email	X		
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Online	X
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify):					

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	X
Commercial data brokers					
Other (specify):					

Section 4: Information Sharing

4.1 *Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.*

Recipient	How information will be shared			Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.
	Case-by-case	Bulk transfer	Direct log-in access	
Within the Component	X	X	X	This includes sharing between program offices or staff and administrative offices or staff to support and continuously improve all aspects of the DOJ-grant management lifecycle.
DOJ Components	X	X	X	This includes direct log-in access and sharing by OVW, COPS, and OJP for routine grants management activities as described in Section 2.1, case-by-case sharing with the Justice Management Division (JMD) Senior Management Executives (SMEs) to assist in setting Departmental policy priorities, case-by-case sharing with the DOJ Office of the Inspector General (OIG) to assist in audits and investigations, and case-by case sharing with the Federal Bureau of Investigations (FBI), and U.S. Attorneys to assist in prosecutions and investigations.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct log-in access	Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.
Federal entities	X	X	X	This includes sharing from Grants.gov. or SAM.gov, DOJ's Unified Financial Management System (UFMS), Automated Standard Application for Payments (ASAP), and DOJ Identity, Credential, and Access Service Records System (DOJ ICAM) to facilitate the DOJ-grant management lifecycle by allowing for seamless integration with these other Federal systems and services. Interconnection Security Agreements (ISAs) are completed when required for information sharing with these external entities.
State, local, tribal gov't entities	X		X	Applicants and recipients registered in SAM.gov are provisioned general user roles and only have access to their own account and application information.
Public	X		X	Applicants and recipients registered in SAM.gov are provisioned general user roles and only have access to their own account and application information.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector	X		X	Applicants and recipients registered in SAM.gov are provisioned general user roles and only have access to their own account and application information.
Foreign governments				

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct log-in access	Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.
Foreign entities				
Other (specify):				

4.2 *If the information will be released to the public for “[Open Data](#)” purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.*

OJP will not release JustGrants data on data.gov.

Section 5: Notice, Consent, Access, and Amendment

5.1 *What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.*

A System of Records Notice (SORN) describing the JustGrants system of records will be published in the Federal Register prior to deployment of the JustGrants system in order to provide notice to the public. Additionally, OJP’s Office of the Chief Financial Officer’s Information Technology Security Division (ITSD) will provide a Privacy Act 552a(e)(3) notice for individuals submitting information to the system. Finally, OJP ITSD will work with the JustGrants team to deploy a notification page that provides users with a warning banner that meets DOJ notice requirements when users log on to the system.

What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

Users are presented with a link to the Privacy Act 552a(e)(3) notice. The notice complies with all subsection (e)(3) requirements, including stating that providing information in the JustGrants system is voluntary, and outlines the potential effects of not providing all or any part of the requested information for DOJ users as well as applicants for and recipients of grant funding. Users are therefore provided the information necessary to choose whether to consent to the collection and use of their information.

5.2 *What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive*

notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

JustGrants users can validate or modify personal information through the standard user interface. As provided in the JustGrants System of Records Notice (SORN), individuals seeking to contest or amend records must directly contact the applicable component’s FOIA Officer (COPS, OJP, or OVW). 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 in the SORN. 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. 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.

Section 6: Maintenance of Privacy and Security Controls

6.1 *The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).*

X	<p>The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):</p> <p>An ATO was issued and has been reauthorized until March 3, 2021.</p> <p>If an ATO has not been completed, but is underway, provide status or expected completion date:</p> <p>Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:</p> <p>POAMs related to the cloud platforms’ Federal Risk and Authorization Management Program (FedRAMP) packages are stored in the OMB Max Portal due to sensitivity.</p>
	<p>This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:</p>
X	<p>Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:</p>

	DOJ/OJP Cybersecurity Standards and Continuous Monitoring: Testing of the AU-02, AU-03, AU-06, AU-12, AU-13 controls is underway for JustGrants. In addition, OCIO has been monitoring and tracking the known vulnerabilities for the system under OMB MAX FedRAMP Continuous Monitoring.
X	<p>Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:</p> <p>Audit logs are reviewed by OJP security operations in accordance with the auditing and accountability control family requirements as specified in the DOJ/OJP Cybersecurity Standards (unclassified security control matrix) are identified, implemented, and assessed as detailed in the Security Assessment Report within the DOJ Cyber Security Assessment and Management (CSAM) tool.</p>
X	<p>Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy.</p>
	<p>Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:</p> <p>No additional training specific to this system is provided.</p>

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

JustGrants uses technical controls through role-based privileges to limit users' access privileges. The system implements the principle of least privilege to ensure that only authorized internal users have access to sensitive data. External users are provisioned general user roles that only have access to their account information and application.

Internally, auditing features of the system enable the reconstruction or review of actions taken by an individual, including unauthorized modifications to applications information. The audit trail captures any changes to application data by DOJ personnel. Department users of JustGrants have access privileges based on the roles granted to them. These roles may allow them to modify, add or remove general users, or make modifications to the website itself. Access requests go through COPS, OJP, and OVW's account management process that includes obtaining the approval of the system owner as listed in the DOJ CSAM tool.

External users interact with JustGrants via web portals over HTTPS that provide confidentiality of sensitive data via secure communications that are encrypted in transit between web services, and restrictions against anonymous users. Again, external users are provisioned general user roles that allow access only to their account information and

application.

DOJ leverages the DOJ Strong Authentication Policy service. JustGrants receives the benefit of a FedRAMP compliant solution implementing necessary security controls at a FISMA Moderate level commensurate with the FIPS-199 Standards for Security Categorization of Federal Information and Information Systems requirements for a moderate security categorization and the guidance of NIST SP 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories. It also features user identification and password access controls.

Information is encrypted at rest and in transit within the JustGrants system. OJP's Application Programming Interface Management (API-M) secures the transmission of information between the JustGrants solution and the various internal (e.g. DMRA, DIAMD) and external (e.g. SAM.Gov, Grants.gov) components using encryption commensurate with the FIPS-199 requirements for a moderate security categorization. The DCM and DMRA components that store the JustGrants information at rest also implement encryption commensurate with the FIPS-199 requirements for a moderate security categorization.

Additionally, the information systems are categorized as Moderate B. This data categorization matches the overall system security categorization found in the system security plan, which is a part of this system's certification and accreditation package.

6.3 *Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)*

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.

Section 7: Privacy Act

7.1 *Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).*

No. Yes.

7.2 *Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or*

explain if a new SORN is being published:

COPS-003 COPS Management System: NexGen (CMS:NxG)

- 85 FR 3421 (1-21-2020)*

OJP-004 Grants Management Information System

- 53 FR 40526 (10-17-1988)*
- 66 FR 8425 (1-31-2001)
- 72 FR 3410 (1-25-2007) (rescinded by 82 FR 24147)
- 82 FR 24147 (5-25-2017)

A new SORN, Justice Grants System (JustGrants), JUSTICE/ OJP—016 is being published to more clearly notify the public about the information collected regarding this system.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***

The following controls have been put into place, each of which helps to reduce the distinct yet related risks of unauthorized disclosure, data breach, and receipt of data by an unauthorized recipient:

- Direct access to case data via JustGrants by members of the public and DOJ employees, as well as contractors, is limited by access controls that are commensurate with individuals' purpose of access.
- The system is designed to collect data only as needed for the awarding and administrative processing of grants, as well as the processing of payment programs, throughout the lifecycle of the program or activities involved.

- A DOJ background check is performed on all DOJ personnel, including employees and contractors, working on JustGrants. In addition to background checks, all DOJ personnel are required to complete annual computer security awareness training and sign “DOJ Cybersecurity and Privacy Rules of Behavior (ROB) for General Users,” which include rules for safeguarding identifiable information.
- Users of the system can only gain access to the data by a valid user ID and password. Access to the data in the system is further limited by the user’s assigned role within the system.
- Auditing features of JustGrants capture changes to application data by DOJ personal and enable the collection of information on such changes, which allows for the reconstruction or review of actions taken by an individual including unauthorized modifications to applications information.
- All communications between users and the system are protected by a secure communication protocol that provides confidentiality and integrity of the transmitted data. The system adheres to records retention schedules, which decreases the length of time information will be maintained, in accordance with such schedules.
- 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.
- The system leverages FedRAMP compliant cloud service infrastructure with security controls, including physical safeguards appropriate for a FISMA moderate system.