Office of Justice Programs

Privacy Impact Assessment
for the
DOJ Peer Review Management System
(PRMS)

Issued by:
Maureen A. Henneberg

Approved by: Andrew J. McFarland
Senior Counsel, Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: January 16, 2025

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

Peer Review Management System (PRMS) is a web-based tool to manage the planning, selection, and assignment of peer reviewers as part of the merit review of DOJ's funding opportunities. Individuals (i.e., potential peer reviewers who may be members of the public or in the federal government) voluntarily enter their personally identifiable information (PII) via an online application (i.e., profile) to be considered for peer review assignments. Authorized DOJ users (i.e. DOJ program office and contract staff) can search these profiles to nominate and invite a peer reviewer to review and score DOJ funding opportunity applications. Authorized public users (i.e., those members of the public or federal government invited by a DOJ program office staff to serve as peer reviewer) may log into PRMS to review their profiles and obtain access to assigned peer review tasks.

The PRMS supports DOJ's overall grantmaking and research efforts toward fair, equitable, and objective funding decisions by providing a centralized directory for DOJ staff to obtain peer reviewers. DOJ peer reviewers consist of federal government staff or members of the public, who offer their expertise in merit reviewing and scoring OJP funding opportunities. The system achieves this purpose by having two main components, the Peer Reviewer Database (PRD) and the Peer Review Support System (PRSS).

The PRD maintains and disseminates profiles of peer reviewers and their electronic enrollment information. This component collects PII about individual peer reviewers who voluntarily complete a multi-step online application process to be assigned peer review as needed by DOJ. The PRD allows authorized DOJ users (DOJ program and contractor staff) to nominate and invite a peer reviewer for a peer review assignment. Authorized DOJ users can also review and evaluate work performed once a peer reviewer completes an assignment.

The PRSS maintains details of the peer review process necessary for authorized DOJ users to manage the peer review process, including application review criteria from funding opportunities, application data, and peer reviewer assignments. The PRSS also converts raw peer review scores into normalized scores or tiers, which are uploaded into OJP's grants management system for programmatic review.

This PIA is being conducted pursuant to the E-Government Act of 2002 because PRMS contains information in identifiable form about members of the public that is contained in an IT system.

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.

The Peer Review Management System (PRMS) supports DOJ's overall grantmaking and research efforts toward fair, equitable, and objective funding decisions by providing a centralized directory for DOJ staff to obtain peer reviewers. DOJ peer reviewers consist of federal government staff or members of the public, who offer their expertise in merit reviewing and scoring OJP funding opportunities.

As discussed above, DOJ relies on the Peer Review Management System (PRMS) to

accomplish its mission of providing timely, cost-effective, and reliable peer review service to DOJ, other Federal agencies, and the public at large.

The information collected consists of e-mail addresses, passwords, any number of choices for a security question to enable password recovery, resume title, name, employee type (OJP, Other Federal, or Other), education level, job category, race, cultural and ethnic identities, subject matter expertise, research expertise, business organization, organization unit, job title, phone number (home and business), address (home and business), and gender and sexual identities. This data is required to effectively provide peer review services. OJP may search for these individuals in PRMS with any individual characteristic (e.g., sex, gender, race, ethnic, or cultural identities) if it is justified and documented that this information is needed to meet the objective of the solicitation and will be conducive to a full and fair evaluation of the relevant applications.

The PRMS functionality does not (itself) determine suitability for participating in a peer review assignment. Rather, suitability is determined by comparing an individual user's input to the requirements of a particular peer review assignment. The PRMS provides DOJ with a centralized location to obtain eligible individuals who self-identify as experts in subject matter or respective field(s) of study to analyze programmatic and research peer review options, when needed, more efficiently.

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
Statute	34 U.S.C. §§10102(a), 10110, 10224; and 10226(b); 28 U.S.C. § 530C(a); 2 C.F.R. Part 2800 (adopting 2 C.F.R. Part 200, with some modifications), specifically, 2 C.F.R. § 200.205 (requiring awarding agency to design and execute a merit review process for applications) and § 200.204 (requirements for notices of funding opportunities); and Attorney General Order No. 1473-91 (Feb. 19, 1991)
Executive Order	E.O. 13985
Federal regulation	See above
Agreement, memorandum of understanding, or other documented arrangement	N/A
Other (summarize and provide copy of relevant portion)	N/A

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
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, & D* *Note for all categories below designated with a response of "D. Members of the Public – Non- USPERs," OJP does not recommend the use of non-US or non- domestic reviewers due to limited resources, however, PRMS currently includes information on non-USPER reviewers since reviewers are not screened by citizenship. OJP may be able to mitigate the acceptance of non-USPER reviewers in the future as PRMS is upgraded.	Names of peer reviewers, DOJ entities, and other Federal Government Employees.
Date of birth or age	X	C&D and possibly A&B if they were external prior to DOJ employment	Year of Birth (YOB) only. Self-reported.
Place of birth			
Gender	X	C&D and possibly A&B if they were external prior to DOJ employment	Self-reported.
Race, ethnicity, or citizenship	X	C&D and possibly A&B if they were external prior to DOJ employment	Exclude citizenship. Self-reported.
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			

(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
Vehicle identifiers			
Personal mailing address	X	C&D and possibly A&B if they were external prior to DOJ employment	Personal email, phone number, and address of peer reviewers, DOJ and other Federal Government employees
Personal e-mail address	X	C&D and possibly A&B if they were external prior to DOJ employment	Personal email, phone number, and address of peer reviewers, DOJ and other Federal Government employees
Personal phone number	X	C&D and possibly A&B if they were external prior to DOJ employment	Personal email, phone number, and address of peer reviewers, DOJ and other Federal Government employees
Medical records number			
Medical notes or other medical or health information	X	A, B, C, and D	PRMS does not currently collect this information; however, the system may collect certain information of this type in the future in order to allow OJP to properly comply with any request for legally required accommodations.
Financial account information			
Applicant information	X	C & D	Application information may include individuals who apply for fellowships as individuals. Self-reported.
Education records	X	C&D and possibly A&B if they were external reviewer prior to DOJ employment	References in resumes and institution/certificates/etc. Self-reported.
Military status or other information	X	C&D and possibly A&B if they were external reviewer prior to DOJ employment	
Employment status, history, or similar information	X	C&D and possibly A&B if they were external prior to DOJ employment	
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates	X	C&D and possibly A&B if they were external prior to DOJ employment	References in resumes and institution/certificates/etc. Self-reported.
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities	X	C&D and possibly A&B if they were external prior to DOJ employment, although highly unlikely	Self-Reported.
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C&D and possibly A&B if they were external prior to DOJ employment, although highly unlikely	Self-Reported.

(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
Juvenile criminal records information	X	C&D and possibly A&B if they were external prior to DOJ employment, although highly unlikely	Self-Reported.
Civil law enforcement information, e.g., allegations of civil law violations	X	C&D and possibly A&B if they were external prior to DOJ employment, although highly unlikely	Self-Reported.
Whistleblower, e.g., tip, complaint, or referral	X	C&D and possibly A&B if they were external prior to DOJ employment, although highly unlikely	Self-Reported.
Grand jury information	X	C&D and possibly A&B if they were external prior to DOJ employment, although highly unlikely	Self-Reported.
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information	X	A, B, C & D	Applicant funding amounts and project descriptions.
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **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)**			
System admin/audit data:			
- **User ID**	X	A, B, C, & D	User IDs and Passwords of peer reviewers, DOJ and other Federal Government Employees
- **User passwords/codes**	X	A, B, C, & D	User IDs and Passwords of peer reviewers, DOJ and other Federal Government Employees
- **IP address**	X	A, B, C, & D	User IDs and Passwords of peer reviewers, DOJ and other Federal Government Employees

(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
- **Date/time of access**	X	A, B, C, & D	User IDs and Passwords of peer reviewers, DOJ and other Federal Government Employees
- **Queries run**	X	A, B, C, and D*	User IDs and Passwords of peer reviewers, DOJ and other Federal Government Employees
- **Contents of files**	X	C&D and possibly A&B if they were external prior to DOJ employment, although highly unlikely	
Other (please list the type of info and describe as completely as possible):	X	C&D and possibly A&B if they were external prior to DOJ employment, although highly unlikely	Resumes may contain more information not covered here. Recovery data for forgotten passwords for peer reviewers, DOJ and other Federal Government employees.

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		Online	X
Phone		Email	X		
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	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			
	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.**
Within the Component	X	X	X	Peer Reviewers and authorized OJP staff receive information from PRMS to administratively manage DOJ peer reviews.
DOJ Components	X	X (for the Office on Violence Against Women (OVW)'s case)	X	Requests for information on peer reviews and other information in PRMS may be used for responding to data calls.
Federal entities	X	N/A	N/A	DOJ/OIG and/or OMB may request information from PRMS.
State, local, tribal gov't entities	X	N/A	N/A	Non-award letters are sent to entities with information from PRMS.
Public	N/A	N/A	X	This is limited to users of the system, who can only see their own profile.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	N/A	N/A	N/A	
Private sector			.	
Foreign governments	N/A	N/A	N/A	
Foreign entities	X	N/A	N/A	If an entity is defined as a peer reviewer, then this is treated the same as Public.
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 Audit and Risk Assessment Management (OAAM) team understands that PII is maintained in this system and would coordinate with OJP FOIA Team and OCIO staff

members to review and redact PII as needed prior to release to the public.

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.

PRMS provides a link to the DOJ Privacy Policy on each page accessed by a user. OJP has added a Privacy Act (e)(3) Statement to the system.

5.2 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.

Individual peer reviewers voluntarily complete an online application to be assigned peer reviews as needed by DOJ. Therefore, the PII entered in the system by individual peer reviewers is all on a voluntary basis.

5.3 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.

As PRMS depends on information provided by individual peer reviewers when they voluntarily complete the online application to be assigned peer reviews as needed by DOJ, individuals have the ability to update or correct their profiles on their own. Individual peer reviews also may make a request to DOJ authorized users who have access to the system to update or correct their information. Users also can request access and amendment in accordance with the System of Records Notice and 28 C.F.R. § 16.46, "Requests for Amendment or Correction of Records."

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	**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)**: PRMS currently has an ATO date of 06/17/2025. **If an ATO has not been completed, but is underway, provide status or expected completion date:** **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:**
	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: N/A
X	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan**: PRMS is categorized as a Moderate impact system in accordance with guidance provided in FIPS 199 based on the type of information collected and stored to maintain the confidentiality, integrity, and availability of information in the system. The system categorization is documented in JCAM.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** An access control policy and mechanism has been implemented and is documented in the program system security plan. OJP has implemented IT security continuous monitoring, a critical part of the risk management process. In addition, DOJ/OJP monitors the monthly continuous monitoring submissions from Cloud Service Providers (CSPs) for all Cloud Service Offerings (CSOs) supporting PRMS in accordance with FedRAMP Continuous Monitoring requirements.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** An audit policy and mechanism has been implemented. This is documented in the program system security policy. Additionally, application audit logs are ingested by Splunk and reviewed in accordance with Department and Component policies and procedures.
X	**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**. This is governed by DOJ/OJP policy.
X	**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:** There is no additional training specific to this system. This is governed by DOJ/OJP policy.

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?

The system environment is hosted in the AWS GovCloud. Physical access is strictly restricted to System Administrators who are allowed privileged access to system components. The system virtual privacy cloud is integrated with Digital Identity and Access Management Directory (DIAMD), an identity and management system which prohibits logical access to the system environment. The environment audit logs are also integrated with OJP CCP audit log system – Splunk. In addition, a Splunk alert has been set up to ensure key stakeholders, such as the system owner, ISSM, and ISSO are notified of security events and incidents within the environment. Furthermore, OJP has issued the OJP IT Security Program instruction and additional SOPs that define various types of digital and/or non-digital media requiring restricted access and provides guidelines for the secure processing, transmission, and storage of OJP sensitive information.

The following PRMS controls have been implemented and confirmed:

- AC-06: Least Privilege - PRMS applications are defined and configured to provide access based on the principles of Least Privilege. Only approved privileged users are provided access to the PRMS platform with roles in the application based on the least privilege access needed to perform function.
- IA-02(1): Multi-Factor Authentication to Privileged Accounts - PRMS Admins who are a privileged user are authenticated using PIV to the workstation and RSA Token. Internal users will not be able to sign in outside of VPN (which enforces PIV to be used to sign in for VPN on GFE devices).
- RA-05: Vulnerability Monitoring and Scanning - Vulnerability scanning is covered in the Vulnerability Management Program (VMP) which conducts vulnerability scanning for all the information systems and hosted applications in accordance with the DOJ Vulnerability Management Plan (VMP). The scan results are reviewed monthly for remediations.

PRMS is hosted withing the OJP AWS Secure Cloud Network (SCN). The Secure Cloud Network protects the confidentiality and integrity of transmitted information. Privileged users manage the Windows, Linux, Database EC2 instances remotely over the Internet using SSH/RDP encrypted connections. Privileged users access the AWS console to manage the cloud infrastructure with a web browser through a port 443 TLS/SSL (https) with IAM login requiring multifactor authentication.
Each EC2 instances include an encrypted key pair to protect authentication information in transit.

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. __X__ 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:

OJP-020, Peer Review Management System, last published in full at 89 Fed. Reg. 93656 (Nov. 27, 2024), available at https://www.govinfo.gov/content/pkg/FR-2024-11-27/pdf/2024-27570.pdf.

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?

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. Records are stored in accordance with applicable executive and agency orders.

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 user's identification and authentication determined in development to ensure PII is stored and disseminated appropriately, and not made available outside of the reviewer or OJP, OVW, the Office of Community Oriented Policing (COPS), and DOJ. Data collection is minimized to only collect data voluntarily. Based upon the individual user's input and having a centralized location to obtain eligible individuals who self-identify as experts in subject matter or respective field(s) of study, OJP staff can streamline the location of subject matter experts desiring to serve as peer reviewers for OJP.